

BCC

Belgian Cost of Cybercrime: Measuring cost and impact of cybercrime in Belgium

Letizia Paoli, Elke Van Hellefont, Cedric Verstraete, Jonas Visschers (KU LEUVEN LINC) - Ralf De Wolf, Marijn Martens, Lieven De Marez, Pieter Verdegem, Evert Teerlinck (imec-mict-UGent) - Ping Chen, Christophe Huygens (KU LEUVEN DistriNet) - Thomas De Cnudde, Vincent Rijmen (KU LEUVEN COSIC) - Marie-Christine Janssens, Thomas Marquenie (KU LEUVEN, CiTiP)

Axis 4: Federal public strategies



NETWORK PROJECT

BCC

Belgian Cost of Cybercrime: Measuring cost and impact of cybercrime in Belgium

Contract - BR/132/A4/BCC

FINAL REPORT

PROMOTORS: Marie-Christine Janssens (KU LEUVEN CiTiP)
Lieven De Marez (imec-mict-UGent)
Wouter Joosen (KU LEUVEN DistriNet)
Vincent Rijmen (KU LEUVEN COSIC)

AUTHORS: Letizia Paoli, Elke Van Hellefont, Cedric Verstraete, Jonas Visschers (KU LEUVEN LINC)
Ralf De Wolf, Marijn Martens, Lieven De Marez, Pieter Verdegem, Evert Teerlinck (imec-mict-UGent)
Ping Chen, Christophe Huygens (KU LEUVEN DistriNet)
Thomas De Cnudde, Vincent Rijmen (KU LEUVEN COSIC)
Marie-Christine Janssens, Thomas Marquenie (KU LEUVEN, CiTiP)





Published in 2018 by the Belgian Science Policy Office
Avenue Louise 231
Louizalaan 231
B-1050 Brussels
Belgium
Tel: +32 (0)2 238 34 11 - Fax: +32 (0)2 230 59 12
<http://www.belspo.be>
<http://www.belspo.be/brain-be>

Contact person: Aziz NAJI
Tel: +32 (0)2 238 36 46

Neither the Belgian Science Policy nor any person acting on behalf of the Belgian Science Policy is responsible for the use which might be made of the following information. The authors are responsible for the content.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without indicating the reference :

P. Chen, Th. De Cnudde, Lieven De Marez, R. De Wolf, Ch. Huygens, M.-Ch. Janssens, M. Martens, Th. Marquenie, L. Paoli, Evert Teerlinck, E. Van Hellefont, , Pieter Verdegem, C. Verstraete, J. Visschers, ***Belgian Cost of Cybercrime: Measuring cost and impact of cybercrime in Belgium.*** Final Report. Brussels : Belgian Science Policy 2018 – 117 p. - BRAIN-be (Belgian Research Action through Interdisciplinary Networks)

TABLE OF CONTENTS

| | |
|----------------------------------------------------------------------------------------------------|-----|
| SUMMARY | 5 |
| ENGLISH..... | 5 |
| FRANCAIS | 8 |
| NEDERLANDS..... | 11 |
| 1. INTRODUCTION | 14 |
| 2. STATE OF THE ART AND OBJECTIVES | 15 |
| 3. METHODOLOGY | 16 |
| 3.1. CITIZENS..... | 16 |
| 3.1.1. <i>Surveys</i> | 16 |
| 3.1.2. <i>Samples</i> | 16 |
| 3.1.3. <i>Questionnaire survey 1</i> | 17 |
| 3.1.4. <i>Questionnaire survey 2</i> | 17 |
| 3.1.5. <i>Data Analysis</i> | 18 |
| 3.2. BUSINESSES..... | 19 |
| 3.2.1. <i>Security state assessment and cost modeling</i> | 19 |
| 3.2.2. <i>Surveys</i> | 19 |
| 3.2.2.1. <i>Questionnaire</i> | 20 |
| 3.2.2.2. <i>Sampling Procedures and Final Samples</i> | 23 |
| 3.2.2.3. <i>Data Analysis</i> | 24 |
| 3.3. GOVERNMENT..... | 24 |
| 3.3.1. <i>Survey</i> | 25 |
| 3.3.2. <i>Parliamentary Questions</i> | 25 |
| 3.3.3. <i>Interviews</i> | 26 |
| 3.3.3.1. <i>Topics</i> | 27 |
| 3.3.3.2. <i>Sampling and Data Collection</i> | 27 |
| 3.4. FORECASTING..... | 28 |
| 3.4.1 <i>The Problem of Cost Prediction</i> | 28 |
| 3.4.2 <i>Survey Considerations and Questions</i> | 28 |
| 4. SCIENTIFIC RESULTS AND RECOMMENDATIONS | 30 |
| 4.1. TYPOLOGIES..... | 30 |
| 4.1.1. <i>Citizens</i> | 30 |
| 4.1.1.1. <i>Cybercrime</i> | 30 |
| 4.1.1.2. <i>Impact, Harms and Costs of Cybercrime</i> | 32 |
| 4.1.2. <i>Businesses/Government</i> | 34 |
| 4.1.2.1. <i>Cybercrime</i> | 34 |
| 4.1.2.2. <i>Impact, Harms and Costs of Cybercrime</i> | 38 |
| 4.2. EMPIRICAL RESULTS..... | 40 |
| 4.2.1. <i>Citizens</i> | 40 |
| 4.2.1.1. <i>Victimisation, security measures and costs of cybercrime of the general population</i> | 40 |
| 4.2.1.2. <i>Conclusion</i> | 50 |
| 4.2.2. <i>Businesses</i> | 51 |
| 4.2.2.1 <i>Security State Assessment and Cost Modeling</i> | 51 |
| 4.2.2.2. <i>Surveys</i> | 72 |
| 4.2.3. <i>Government</i> | 87 |
| 4.2.3.1. <i>Analysis of Parliamentary Questions</i> | 87 |
| 4.2.3.2. <i>Selected interviews</i> | 94 |
| 4.2.4. <i>Forecast</i> | 96 |
| 4.3. POLICY RECOMMENDATIONS | 100 |
| 4.3.1. <i>General</i> | 100 |
| 4.3.2. <i>Citizens</i> | 102 |
| 4.3.3. <i>Businesses</i> | 103 |
| 4.3.4. <i>Government</i> | 104 |
| 5. DISSEMINATION AND VALORISATION | 107 |
| 6. PUBLICATIONS | 109 |
| 7. ACKNOWLEDGEMENTS | 110 |
| REFERENCES | 111 |
| LIST OF TABLES AND FIGURES | 116 |

SUMMARY

ENGLISH

Context: The research project Belgian Cost of Cybercrime (BCC) is as a four-year interdisciplinary research project on the cost and impact of cybercrime in Belgium. The BCC project started from the assumption that, while information technology has been offering unprecedented opportunities to the Belgian society and economy, it also created new opportunities for, and vulnerabilities to, crime. More in particular, cybercrime can cause serious harm to individual and corporate internet users and compromise communication, e-commerce, financial and other services that rely on digital information and infrastructure.

Objectives: The project aimed a) to assess the impact – in terms of costs or material harms and non-material harms - of cybercrime on three levels: Belgian individuals, Belgian companies and the Belgian government, b) to estimate the prevention and reaction costs of Belgian based individuals and businesses and the Belgian government, and c) to develop policy recommendations for Belgian and European policy-makers.

Methodology of the research:

Five teams of researchers at the KU Leuven and the University of Ghent have pooled their expertise in computer science (DistriNet and COSIC), criminology (LINC), communication sciences (imec-mict-UGent) and IT law (CiTiP) to perform the research amongst citizens, companies and government using a methodology adapted to the target group, as described hereafter.

At the outset, a literature review was performed in order to develop cybercrime models for citizens based in Belgium on the one hand and Belgian businesses and the Belgian government on the other hand. These models were used as framework for the different empirical studies that were subsequently undertaken.

To gain more insight in the impact of cybercrime on **Belgian citizens** two large-scale surveys were conducted, one in 2015 and one in 2017. Both surveys used the same theoretical framework and had a big overlap in questions to make cross comparison between 2015 and 2017 possible.

In order to gain insight in the impact of cybercrime on **Belgian businesses**, a two-fold strategy was followed. First, an investigation was launched to assess the state of security of Belgian businesses. Secondly, two survey waves were administered to Belgium based businesses. The results of these surveys were subsequently combined with the security assessments to come up with a cost model. The predictive capabilities of this model were then assessed.

As regards the assessment of the impact of cybercrime on **Belgian Governments**, a web survey has been designed to gather the necessary data from the different governments in Belgium (Federal, Flemish, Walloon, French-speaking community and Brussels government).

However, because the obtained data were too limited for a meaningful analysis, the research has shifted its focus towards (i) an analysis of the answers of the Belgian federal government to parliamentary questions concerning the impact of cybercrime and (ii) interviews with representatives of the federal government and two big Belgian cities.

Main conclusions:

Belgian citizens

In general, most Belgians seem to be aware of the dangers of the internet and are implementing quite a lot of security measures to protect themselves against cybercrime. This, however, doesn't mean that these security measures are implemented effectively. The combination of the reduction in victimization rate of malware and an increase of technical adaptive security measures taken, makes us believe that people in 2017 are better armed against cyber criminality than in 2015. The victimization of scams and hacking, however, hasn't changed in a significant way, despite the growing security measures that are used. Malware makes the most victims, while scams account for the highest direct monetary costs. More than 80% of the victims of any cybercrime (but scams) do not suffer from any direct monetary costs. In contrast, people pay most to protect themselves (=defense cost) against the cybercrimes that are least expensive in terms of direct costs (=malware). Opportunity costs are believed to be felt by every internet user except the most experienced optimistic internet users. Especially the pessimistic experienced internet user and the inexperienced internet user are missing out on opportunities the internet presents due to cybercrime. Subjective norm plays a big role into the intention towards protecting oneself against cybercrime, as does the perceived severity of a certain cybercrime and the perceived effectiveness of the protective measures.

Belgian Industry

(DistriNet): An essential element of cost assessment is modelling to predict (a subset) of the cost of cybercrime. The archetypical example in this case is the banking industry. This sector has Internet facing websites that are often attacked through various means resulting in monetary losses. The banking industry is unique since it is heavily regulated, and is legally required to keep a database of these losses. This is not the case for other industries. However, the individual case data is typically not disclosed – only the consolidated country data is available. To circumvent this limitation, country and sector wide variable measurements of web hygiene can be based on public web data. Secondly, this data can be correlated with loss numbers collected by industry survey to come up with an initial predictive model of these losses based on web hygiene.

(COSIC): Accurate cost prediction of cybercrime is complicated by several factors. Firstly, it is difficult to get accurate numbers for the current situation. IT Security companies tend to overestimate the costs. Victims do not always wish to report crimes; sometimes they don't even know that they have been victims. There are however significant investments in various types of countermeasures. At the moment, it appears that the cost for countermeasures is larger than the direct cost of cybercrime. Furthermore, the future cost of cybercrime can be

expected to grow exponentially. Currently, cyber criminals are often caught when they try to convert stolen digital goods into traditional cash or other real-world properties. With the proliferation of digital currencies and the increase of the digital market, the need for conversion will disappear, and hence also this opportunity to catch criminals. Secondly, the deployment of the Internet of Things will multiply the number of devices that can be attacked. The merger between cyber space and “meat space” will increase the opportunities for extortion. It is well known that exponential growth is difficult to predict accurately.

(LINC): Quite some Belgium businesses seem to be confronted with cybercrime: more than half of the businesses in our samples reported have been victims of at least one of the cybercrime types in the last 12 months. However, for the three cybercrime types for which we have substantial data (i.e. illegal access to IT systems, data/system interference and cyber extortion), only few incidents generated serious costs or harm. The monetary costs reported by the businesses were for all cybercrime types quite low. Concerning non-material harms, we see that businesses generally ranked harms to their internal operational activities higher than those to the other interest dimensions. Comparing the harm severity scores across the different cybercrimes, cyber extortion appears to be the most harmful of the three types for which we have substantial data. As for the overall impact of cybercrimes, our findings are more conservative than those reported by private security and consultancy companies; they appear to be higher than those of other academic studies.

Belgian Government

Although our data are rather limited, we found that federal government agencies have been confronted with cybercrime in the last couple of years. The costs and harms of cyber incidents turned out to be rather low, though. However, we also found indications for the fact that the federal government should further invest in cybersecurity, for example by stimulating the exchange of cyber security expertise between agencies and by increasing the cyber security budget.

Keywords: Cybercrime; Cybersecurity; Costs, Internet Security, impact, hacking

FRANCAIS

Contexte : Le projet 'Belgian Cost of Cybercrime (BCC)' est un projet de recherche interdisciplinaire s'étalant sur une durée de quatre ans, relatif aux coûts et impacts de la cybercriminalité en Belgique. Le projet BCC part du principe suivant : bien que les technologies de l'information ont créé des opportunités sans précédent, tant pour la société belge que son économie, elles ont également créé de nouveaux risques et vulnérabilités à l'égard du milieu criminel. De façon plus spécifique, la cybercriminalité peut occasionner des dégâts sévères aux utilisateurs (particuliers et entreprises) et peut compromettre la communication, le e-commerce, les services financiers et autres, dépendants de données informatisées ainsi que de l'infrastructure.

Objectifs : Le projet a pour objectif a) d'évaluer l'impact – en termes de coûts ou dommages matériels et non-matériels – de la cybercriminalité à trois niveaux : individus belges, entreprises belges ; gouvernement belge, b) d'estimer les coûts de prévention et de réaction engendrés par les individus, entreprises, et le gouvernement belge, et c) de développer des recommandations à destination du législateur Belge et Européen.

Méthodologie de la recherche :

Cinq équipes de chercheurs au sein de la KU Leuven et de l'Université de Gand ont partagé leur expertise en sciences informatiques (DistriNet and COSIC), criminologie (LINC), sciences de la communication (imec-mict-UGent), et droit des technologies de l'information (CiTiP). Elles ont mené des recherches à l'égard des individus, entreprises, et gouvernement selon une méthodologie adaptée au groupe cible, telle que décrite ci-après.

Dès l'origine, un examen des sources pertinentes a été réalisé afin de développer des modèles de cybercriminalité visant les citoyens basés en Belgique d'une part, et concernant les entreprises belges ainsi que le gouvernement belge d'autre part. Ces modèles ont été utilisés en tant que cadre de référence pour les différentes études de nature empirique qui ont été menées par la suite.

Afin de mieux comprendre l'impact de la cybercriminalité sur les **citoyens Belges**, deux grands sondages ont été réalisés, l'un en 2015, l'autre en 2017. Les deux sondages ont utilisé le même cadre de référence, et les questions s'entrecroisaient afin de permettre une comparaison transversale entre 2015 et 2017.

Afin de mieux comprendre l'impact de la cybercriminalité sur les **entreprises belges**, une stratégie à deux niveaux a été suivie. D'abord, une enquête a été ouverte afin d'évaluer l'état de la sécurité des entreprises belges. Dans un second temps, deux vagues de sondages ont été envoyées aux entreprises basées en Belgique. Les résultats de ces sondages ont par la suite été combinés avec l'évaluation de la sécurité pour élaborer à un modèle de coûts. Les potentialités prédictives de ce modèle ont par la suite été évaluées.

Concernant l'examen de l'impact de la cybercriminalité sur les **gouvernements belges**, un sondage en ligne a été conçu afin de collecter les données nécessaires de la part des divers gouvernements en Belgique (Fédéral, Flamand, Wallon, Communauté française, Région de Bruxelles-Capitale). Cependant, puisque les données obtenues étaient trop limitées pour une analyse significative, les chercheurs ont déplacé leur attention vers (i) une analyse des réponses du gouvernement fédéral belge aux questions parlementaires relatives à l'impact

de la cybercriminalité et (ii) des interviews avec des représentants du gouvernement fédéral et de deux grandes villes belges.

Principales conclusions :

Citoyens Belges

En général, la plupart des Belges semblent être au courant des dangers de l'internet et mettent en place toute une série de mesures de sécurité pour se protéger contre la cybercriminalité. Ceci ne veut toutefois pas dire que ces mesures de sécurité sont implémentées de manière efficace.

La combinaison de la réduction du taux de victimisation des malwares et de l'augmentation de mesures de sécurité adaptées à la technique nous font croire que les individus, en 2017, sont mieux armés contre la cybercriminalité qu'en 2015. Le nombre de victimes des fraudes et de hacking n'a toutefois pas changé de manière significative, malgré l'augmentation des mesures de sécurité.

Les malwares touchent le plus de victimes, tandis que les fraudes entraînent les plus importants coûts sur un aspect pécuniaire. Plus de 80% des victimes de cybercriminalité (à l'exception des fraudes) ne souffrent pas de conséquences financières directes. Il est à noter que les individus payent le plus pour se protéger eux-mêmes (defense cost) d'une catégorie de cybercriminalité qui entraîne les coûts directs les plus bas (malware)

Les coûts d'opportunité sont supposés être perçus par chaque consommateur à l'exception des utilisateurs les plus expérimentés et optimistes de l'internet. Ce sont les utilisateurs expérimentés mais pessimistes cette fois ainsi que les utilisateurs inexpérimentés qui manquent le plus d'opportunités sur internet à cause de la cybercriminalité.

Les normes subjectives jouent un rôle important dans l'intention de se protéger contre la cybercriminalité ; ainsi qu'en ce qui concerne la perception de la gravité de certains actes de cybercriminalité, et de l'efficacité perçue des mesures de protection.

Industrie belge

(DistriNet) Un élément essentiel lors de l'examen des coûts est la création d'un modèle permettant de prédire un sous-ensemble du coût de la cybercriminalité. L'exemple typique est celui du secteur bancaire. Les sites internet des fournisseurs de services bancaires sont fréquemment attaqués, par le biais de différents moyens, ce qui résulte en des pertes de nature pécuniaires. Le secteur bancaire est unique en ce qu'il est très réglementé. Il existe également une obligation légale de tenir un registre qui recense ces pertes. Tel n'est pas le cas pour les autres secteurs. Toutefois, les cas individuels sont peu fréquemment divulgués – ce sont uniquement les données consolidées pour l'intégralité du pays qui sont communiquées. Afin de contourner ces limites, des mesures par pays et par secteur sont réalisées visant la hygiène du web; des données étant accessibles publiquement ? Deuxièmement, ces données peuvent être corrélées avec le nombre des pertes collectées par des sondages réalisés dans le secteur afin de parvenir à un modèle prédictif initial de ces pertes, modèle basé sur l'hygiène du web.

(COSIC) Des prévisions précises des coûts de la cybercriminalité sont délicates à anticiper à la suite de plusieurs facteurs. Premièrement, il est difficile d'obtenir des numéros fiables pour

la situation actuelle. Les entreprises de sécurité informatique ont tendance à surestimer les coûts. Les victimes ne souhaitent pas toujours porter plainte ; parfois même elles ne savent pas qu'elles ont été des victimes. Il existe cependant des investissements significatifs pour une série de contre-mesures. Il apparaît pour l'instant que le coût de ces contre-mesures est plus important que le coût direct émanant de la cybercriminalité. De plus, les coûts de la cybercriminalité vont probablement augmenter de façon exponentielle. À l'heure actuelle, les cybercriminels sont souvent pris la main dans le sac lorsqu'ils essaient de convertir des biens digitaux volés en cash traditionnel, ou en des biens susceptibles d'être appréhendés. Avec le développement des monnaies virtuelles ainsi que du marché digital, ce besoin de conversion va disparaître, et avec lui cette opportunité d'attraper les criminels. Deuxièmement, le développement de l'internet des choses (Internet of Things) va démultiplier le nombre d'appareils susceptibles d'être attaqués. La fusion entre le cyber espace et le 'meat space' va augmenter les cas d'extorsion. Il est bien connu que la croissance exponentielle est difficile de prédire de façon correcte.

(LINC) Il existe toute une série d'entreprises belges qui sont confrontées avec le problème de cybercriminalité. Plus de la moitié des entreprises de notre échantillon a mentionné avoir été victime d'au moins une sorte de phénomène cybercriminel au cours des 12 derniers mois.

Cependant, pour les trois types de cybercriminalité au sujet desquels nous avons des données substantielles (accès illégal aux systèmes informatiques ; pannes de systèmes informatiques ; extorsion via l'internet), ce sont uniquement quelques éléments qui ont occasionné des coûts ou dommages importants. Les coûts de nature pécuniaire communiqués par les entreprises étaient assez faibles, et ceci concernant tous les types de cybercriminalité. Concernant les dommages de nature non-matérielle, nous avons constaté que les entreprises estiment en général leurs dommages causés à leurs activités opérationnelles à l'intérieur de bien plus grande importance que pour les autres domaines.

En comparant l'importance des dégâts des différentes catégories de cybercriminalité, nous avons constaté que, hors des trois types de cybercriminalité examinés, c'est l'extorsion via l'internet qui cause le plus de dommages. Concernant l'impact de la cybercriminalité en général, nos constats sont plus modérés que ceux des entreprises de sécurité privée et bureaux de consultances, mais plus prononcés que ceux des autres études provenant du monde académique.

Gouvernement Belge

Bien que les données dont nous disposons sont assez limitées, il a été constaté que les instances étatiques au niveau fédéral ont été confrontées les dernières années avec des questions relatives à la cybercriminalité. Les coûts et dommages de ces cyber-incidents étaient relativement bas. Cependant, nous avons également trouvé des indications relatives au fait que l'autorité fédérale doit dans le futur continuer d'investir dans la cyber-sécurité, par exemple en favorisant et stimulant l'échange d'expertise entre les différentes instances et en augmentant le budget relatif à la cyber-sécurité.

Mots clés: Cybercriminalité; cyber-sécurité; coûts; sécurité sur internet ; impact, hacking

NEDERLANDS

Context: Het onderzoeksproject 'Belgian Cost of Cybercrime' (BCC) is een vierjarig interdisciplinair onderzoeksproject over de kosten en impact van cybercriminaliteit in België. Het BCC-project gaat uit van de veronderstelling dat, hoewel informatietechnologie ongekende mogelijkheden biedt voor de Belgische samenleving en economie, het ook nieuwe kansen en kwetsbaarheden voor criminaliteit creëerde. Meer in het bijzonder kan cybercriminaliteit ernstige schade toebrengen aan individuele en commerciële internetgebruikers en kan het de communicatie, elektronische handel, financiële en andere diensten die afhankelijk zijn van digitale informatie en infrastructuur ernstig compromitteren.

Doelstellingen: Het project had volgende doelstellingen: a) het beoordelen van de impact - in termen van kosten of materiële schade en immateriële schade - van cybercriminaliteit op drie niveaus: Belgische individuen, Belgische bedrijven en de Belgische overheid, b) het maken van een inschatting van de preventie- en reactiekosten die cybercriminaliteit voor Belgische particulieren en bedrijven en de Belgische overheid met zich meebrengt, en c) het opstellen van aanbevelingen voor Belgische en Europese beleidsmakers.

Methodologie van het onderzoek

Vijf teams van onderzoekers aan de KU Leuven en de Universiteit van Gent bundelden hun expertise in informatica (DistriNet en COSIC), criminologie (LINC), communicatiewetenschappen (imec-mict-UGent) en IT-recht (CiTiP) om het onderzoek uit te voeren bij burgers, bedrijven en overheid. Er werd gebruik gemaakt van een methodologie aangepast aan de doelgroep, zoals hierna beschreven.

Vooraf werd een literatuuronderzoek uitgevoerd om cybercrime-modellen te ontwikkelen voor, enerzijds, burgers in België en, anderzijds, Belgische bedrijven en de Belgische overheid. Deze modellen werden gebruikt als kader voor de verschillende empirische studies die vervolgens werden uitgevoerd.

Om meer inzicht te krijgen in de impact van cybercriminaliteit op **Belgische burgers** werden twee grootschalige enquêtes uitgevoerd in respectievelijk 2015 en 2017. Beide onderzoeken gebruikten hetzelfde theoretische kader en grotendeels dezelfde vragen om een vergelijking tussen de resultaten bekomen in 2015 en 2017 mogelijk te maken.

Om inzicht te krijgen in de impact van cybercriminaliteit op **Belgische bedrijven**, werd een tweevoudige strategie gevolgd. Eerst werd een onderzoek gestart om de veiligheidstoestand van Belgische bedrijven te beoordelen. Daarna werden twee enquête-rondes gevoerd bij in België gevestigde bedrijven. De resultaten van deze enquêtes werden vervolgens gecombineerd met de beoordelingen op het vlak van veiligheid om hieruit een kostenmodel af te leiden en voorstellen. Tenslotte werden de voorspellende mogelijkheden van dit model beoordeeld.

Met betrekking tot de beoordeling van de impact van cybercriminaliteit op de **Belgische overheid**, werd een web-enquête ontworpen om de nodige gegevens te verzamelen van de

verschillende overheden in België (federale, Vlaamse, Waalse, Franstalige gemeenschap en de Brusselse overheid). Omdat de verkregen gegevens echter te beperkt waren voor een zinvolle analyse, is het onderzoek verschoven naar (i) een analyse van de antwoorden van de Belgische federale overheid op parlementaire vragen over de impact van cybercriminaliteit en (ii) interviews met vertegenwoordigers van de federale overheid en twee grote Belgische steden.

Belangrijkste conclusies

Belgische burgers

In het algemeen geven de resultaten aan dat de meeste Belgen zich bewust zijn van de gevaren van internet en passen ze vrij veel beveiligingsmaatregelen toe om zichzelf tegen cybercriminaliteit te beschermen. Dit betekent echter niet dat deze beveiligingsmaatregelen op een efficiënte wijze worden geïmplementeerd. De combinatie van de vermindering van het aantal slachtoffers van malware en de toename van de technisch aangepaste beveiligingsmaatregelen, ondersteunt de stelling dat mensen in 2017 beter gewapend zijn tegen cybercriminaliteit dan in 2015. Niettemin, en ondanks de groeiende beveiligingsmaatregelen die worden gebruikt, is de ratio van het aantal slachtoffers van oplichting en hacking niet significant gewijzigd. Malware maakt de meeste slachtoffers, terwijl oplichting de hoogste directe monetaire kosten met zich meebrengt. Meer dan 80% van de slachtoffers van cybercriminaliteit (behalve oplichting) ondervinden geen directe monetaire kosten. Burgers betalen daarentegen het meest om zichzelf te beschermen (= verdedigingskosten) voor cybercriminaliteit die het minst duur is in termen van directe kosten (= malware). Zogenaamde opportunitetskosten worden blijkbaar gevoeld door elke internetgebruiker, behalve de meest ervaren optimistische internetgebruikers. Vooral de categorieën van de 'pessimistische ervaren internetgebruiker' en de 'onervaren internetgebruiker' missen kansen die het internet hen biedt als gevolg van cybercriminaliteit. De subjectieve norm speelt een grote rol bij de beslissing om zichzelf te beschermen tegen cybercriminaliteit. Verder geldt dit ook voor de waargenomen ernst van een bepaalde cybercriminaliteit en de waargenomen effectiviteit van de beschermende maatregelen.

Belgische industrie

(DistriNet): Een essentieel element van kostenbeoordeling is modellering om (een deelverzameling) van de kosten van cybercriminaliteit te voorspellen. Het archetypische voorbeeld in dit geval is de banksector. Het bankwezen heeft websites die op het internet zijn gericht en die vaak op verschillende manieren worden aangevallen, waardoor geld verloren gaat. Het bankwezen vormt een uniek onderzoeksobject omdat het sterk gereguleerd is en wettelijk verplicht is om een databank van deze verliezen bij te houden. Dit is niet het geval voor andere industrieën. De individuele casusgegevens worden namelijk meestal niet bekendgemaakt - alleen de geconsolideerde gegevens per land zijn beschikbaar. Om aan deze beperking te remediëren, kunnen land- en sector brede variabele metingen van web hygiëne worden uitgevoerd op openbare webgegevens. Ten tweede kunnen deze gegevens worden gecorreleerd met verliescijfers die verzameld worden via een industrie-enquête. Op die wijze kan een initieel voorspellend model voor deze verliezen op basis van web hygiëne worden opgesteld.

(COSIC) : Het maken van een nauwkeurige voorspelling van de kosten van cybercriminaliteit wordt gecompliceerd door verschillende factoren. Ten eerste is het moeilijk om nauwkeurige cijfers te krijgen. IT-beveiligingsbedrijven hebben de neiging om de kosten te overschatten en slachtoffers willen niet altijd misdaden melden; soms weten ze niet eens dat ze slachtoffer zijn geweest. Er worden niettemin aanzienlijke investeringen gedaan in verschillende soorten beveiligingsmaatregelen. Uit het onderzoek blijkt dat de kosten voor beveiligingsmaatregelen hoger zijn dan de directe kosten van cybercriminaliteit. Bovendien kan worden verwacht dat de toekomstige kosten van cybercriminaliteit exponentieel zullen toenemen. Momenteel worden cybercriminelen vaak betrapt wanneer ze gestolen digitale goederen proberen om te zetten in traditioneel contant geld of andere fysieke goederen. Met de toename van digitale valuta's en de expansie van de digitale markt, zal de behoefte aan deze conversie verdwijnen en daarmee ook de mogelijkheid om criminelen te vatten. Ten tweede zal de ontwikkeling van het 'internet der dingen' het aantal apparaten dat kan worden aangevallen exponentieel doen toenemen. De fusie tussen 'cyberspace' en 'meat space' zal de kansen op afpersing vergroten. Zoals algemeen bekend is het moeilijk om een exponentiële groei nauwkeurig te voorspellen.

(LINC): (LINC): Heel wat Belgische bedrijven lijken geconfronteerd te worden met cybercriminaliteit: meer dan de helft van de bedrijven in onze steekproeven gaf aan geconfronteerd te zijn geweest met minstens een type van cybercriminaliteit in de laatste 12 maanden. Echter, voor de drie types van cybercriminaliteit waarvoor we substantiële data verzameld hebben (i.c. ongeautoriseerde toegang tot ICT-systemen, ICT-storingen en cyberafpersing) bleken slechts weinig incidenten ernstige kosten of schade met zich mee te brengen. De geldelijke kosten gerapporteerd door bedrijven waren voor alle types van cybercriminaliteit relatief laag. Wat de niet-materiële schade betreft, werd gevonden dat bedrijven de schade aan hun dagelijkse interne werkzaamheden hoger inschatten dan de schade aan de andere *interest dimensions*. Wanneer we de ernst van de schade van de verschillende types van cybercriminaliteit vergelijken, zien we dat, van de drie types waarvoor we substantiële data verzameld hebben, cyberafpersing het meest schadelijk was. Wat de totale impact van cybercriminaliteit betreft, zijn onze bevindingen gematigder dan die van private beveiligingsbedrijven en consultancybedrijven, maar meer uitgesproken dan die van andere academische studies.

Belgische overheid

Hoewel onze data eerder beperkt zijn, werd toch vastgesteld dat federale overheidsinstanties met cybercriminaliteit te maken hebben gekregen in de afgelopen jaren. De kosten en schaden van deze cyberincidenten waren wel relatief laag. Echter, er werden ook indicaties gevonden voor het feit dat de federale overheid verder dient te investeren in cybersecurity, bijvoorbeeld door de uitwisseling van expertise rond cybersecurity tussen instanties te stimuleren en het budget voor cybersecurity te verhogen.

Kernwoorden: Cybercriminaliteit; Cyberveiligheid; Kosten, Internetveiligheid, impact, hacking

1. INTRODUCTION

Information technology has revolutionized our daily lives, offering unprecedented opportunities to the Belgian society and economy, but also creating new opportunities for, and vulnerabilities to, crime. More in particular, cybercrime – that is, crime using or targeting computer or networks – can cause serious harm to individual and corporate internet users and compromise communication, e-commerce, financial and other services that rely on digital information and infrastructure. A report released in February 2018 has put a number on it: worldwide cybercrime costs an estimated \$600 billion USD a year, an increase with \$ 100 billion USD compared to 2014 (CSIS 2018).

On the national level, it is important that Belgian competent authorities can make informed decisions to protect internet users as well as the overall society and economy from cyber threats. In order to allow them to do so, research centres from the Universities of Leuven and Ghent have conceived the present research project Belgian Cost of Cybercrime (BCC) which consequently obtained funding from the BELSP0 – the Belgian Service Science Policy Office.

The BCC project aimed at systematically investigating and assessing the impact (i.e., costs or harms to material interests and non-material harms) of cybercrime on three levels: society, industry and government. Five teams of researchers at the KU Leuven and the University of Ghent have pooled their expertise in computer science (DistriNet and COSIC), criminology (LINC), communication sciences (imec-mict-UGent) and IT law (CiTiP), to jointly perform this research project under the coordination of the latter. Besides the intense collaboration between these academic research groups, the project has benefitted from the co-operation by industry players as well as government agencies.

The project started in December 2013 and ended in August 2018.

2. STATE OF THE ART AND OBJECTIVES

Despite growing fears and alarmist scenarios, the impact of cybercrime had not yet been systematically investigated and no research on the topic had been carried out in Belgium at the start of the project. It is this knowledge gap that the BCC project intended to address. In particular, drawing on multidisciplinary expertise in computer science (DistriNet, COSIC), criminology (LINC), communication sciences (imec-mict-UGent) and IT law (CiTiP), the project aimed at:

- Assessing the impact (i.e., costs or harms to material interests and non-material harms) of cybercrime on Belgian individuals and companies and the Belgian government;
- Estimating the prevention and reaction costs of Belgian based individuals and companies and the Belgian government;
- Developing policy recommendations for Belgian (and European) policy-makers.

3. METHODOLOGY

First, we conducted a literature review in order to develop cybercrime models for citizens based in Belgium on the one hand and Belgian businesses and the Belgian government on the other hand. These models were used as framework for the different empirical studies undertaken within this project. In the following paragraphs, we discuss more in depth the methodologies employed for the empirical studies conducted among citizens, businesses and government entities, as well as the methodology employed for the forecasting of the impact of cybercrime.

3.1. Citizens

To gain more insight in the impact of cybercrime on Belgian citizens two large-scale surveys were conducted, one in 2015 and one in 2017. Both surveys used the same theoretical framework and had a big overlap in questions to make cross comparison between 2015 and 2017 possible. In what follows we will explain more in depth in how we conducted these surveys.

3.1.1. Surveys

The first wave of the survey was conducted in 2015 and tried to demystify the victimization of cybercrime, the financial impact of cybercrime and the risk perception of cybercrime. On a theoretical level, the research used the Protection Motivation Theory (PMT) as a guiding framework to help understand the risk perception of cybercrime.

The second wave, which was conducted in 2017, had the goal to measure the same concepts and compare them with the 2015 insights. The concepts put forward in the first wave were minimally adjusted and improved in the second wave to accommodate insights from the previous wave and other timely research. Furthermore, in both waves, clusters were made to discover who is most vulnerable for and impacted by cybercrime. The comparison between the two waves in terms of clusters as well as general insights, resulted in recommendations for cybercrime risk communication.

3.1.2. Samples

Data for the first wave was collected using a non-random-internet sample utilizing a quota sampling method to target respondents with certain demographic characteristics to make the sample representative for age, gender and residence for the active Belgian internet population. After data-cleaning on incompletes, a control variable and inconsistent answer patterns our sample consisted of 1033 Belgians. The entire sample was recruited out of the panel of a professional research company.

The second wave used the same internet sampling method and used the same (although updated) demographic characteristics to make the sample representative for age, gender and residence. Of the initial 2132 responses, 1181 were retained after data cleaning and validation. Next to cleaning on incompletes, a control variable and inconsistent answer

patterns, in the second wave, we also cleaned on a credible time frame. This way we could ensure our respondents were paying attention during the survey.

3.1.3. Questionnaire survey 1

The first survey started with demographic questions and various questions to gain insights in the internet use patterns of the respondents. They include variables concerning what devices were available to the respondents, how long they use the internet and what kind of activities they do online. These questions were followed by questions concerning the perceived safety of the different activities they do online.

Next, some questions concerning the different cybercrimes (e.g. viruses) were asked. Firstly, we measured the perceived seriousness (ranging from not serious at all to very serious) and perceived general occurrence (Never – All the time) of these cybercrimes.

Furthermore, we measured if the respondent was victimized over the last 12 months by one of these cybercrimes. The respondents who indicated they were victimized by a certain cybercrime received questions concerning the financial cost that accompanied the incident, how many times they were victimized last year, what device was infected, if the incident was reported and what activity they were doing online. Furthermore, more qualitative and open questions were asked concerning the incident.

Next, questions concerning the security measures someone takes to protect themselves against some specific cybercrimes were asked. These questions included adaptive (e.g. a virus scanner) and maladaptive security measures (e.g. using less internet) and were divided between the different cybercrimes. These questions together with the questions concerning the online activity were used to cluster our sample.

Lastly, questions were asked concerning the process individuals go through in deciding which security behaviors to exercise when faced with cybercrime threats using the variables of the PMT-model. The PMT divides in two cognitive mediating processes to the attitude towards behavior, namely threat appraisal and coping appraisal. Threat appraisal is the cognitive process by which an individual evaluates the severity of the threat (=perceived severity) and the likelihood of being victimized by a certain threat (=perceived vulnerability) (Jansen et al., 2016). Coping appraisal is the cognitive process that answers the question if an individual feels him-/herself able to perform a certain security behavior (= Self-efficacy) and the question if this security behavior is effectivity to protect the individual against harm (=Response efficacy) (Jansen et al., 2016). All these concepts were asked in the questionnaire of the first wave.

For a full overview of the questions used in the first wave, we refer to D3.1.1.

3.1.4. Questionnaire survey 2

In the second wave we followed the same rationale as in the first wave but adjusted some measures. We kept the questions concerning demographics, online activity, victimization and security measures the same as these are used to cluster our sample and we wanted to make

a comparison between wave one and two. We did however update some variables (e.g. the social media examples given) to make the questionnaire up to date.

Furthermore, we adjusted the questions about the cybercrime cost to include four types of cost. Namely; direct monetary cost (e.g. a ransom as a result of a scam), direct non-monetary cost (e.g. privacy), opportunity costs (e.g. Not being able to enjoy the benefits of online banking because someone is scared to do so) and defense costs (e.g. the cost someone pays for their anti-virus program).

In line with the first wave, direct monetary cost was measured using an open question and was only visible for people who were victimized by a certain cybercrime.

To measure the direct non-monetary costs, we used the operationalization of the harm assessment framework (Greenfield & Paoli, 2013; Paoli et al., 2017). The direct non-monetary costs included in our study are three-fold: daily activities, privacy and reputation. Harm was operationalized as a 6-point scale going from “harmless” to “catastrophic”. We included the option “does not apply” to prevent bias. These questions were also only visible to those who stated they were victimized in a previous answer.

Opportunity costs were measured using three techniques. Firstly, we have the direct questions that measured opportunity costs against online banking, online shopping and the use of social network sites (Eurostat, 2016). Secondly, we have the maladaptive security measures who implicate opportunity costs (Chou & Sun, 2017; Crossler & Bélanger, 2014; Jansen & van Schaik, 2017). Finally, we calculated the correlation between the frequency of use of a certain activity and its perceived security. These questions were asked to all respondents and not only those who stated to be a victim.

Defense costs were operationalized as direct costs with an open question (Verdegem et al., 2015). This question was also visible for all respondents (and thus not only the victims).

Furthermore, we added questions about respondents’ awareness of cybercrimes and security measures. After we’ve measured the respondents’ awareness, we educated them into what the definitions were of the different cybercrimes. It was necessary that the respondents were sure what the different cybercrimes meant as we questioned the different variables of the PMT for the different cybercrimes.

For a full overview of the questions used in the second wave we refer to D3.1.2.

3.1.5. Data Analysis

For our analysis we used SPSS 22 in the first wave and SPSS 24 & AMOS 22 in the second wave. To answer the different research questions, we used descriptive and comparative analysis (χ^2 -test, Mann-Whitney, Kruskal-Wallis, Wilcoxon, One-Way Anova, t-tests, spearman correlation) depending on the levels of data. Some analysis are done only on the victims of cybercrime, these analysis are exclusively explorative of nature and do not possess the power to be extrapolated to the Belgian population.

In the second wave, we created a SEM-model to answer the question concerning the predictors of the public's intention to adopt security measures. Here, we analyzed the PMT-model and compared this between malware, scams and cybercrime in general. Furthermore, we ran a SEM-model for the model for different relevant clusters to get a better insight.

For all analyses, we have checked the assumptions, there were no violations found except when explicitly stated in the analysis. We used a significance level of .05

3.2. Businesses

In order to gain insight in the impact of cybercrime on Belgian businesses, a two- fold strategy was followed. First, an investigation was launched to assess the state of security of Belgian businesses. Secondly, two survey waves were administered to Belgium based businesses. The results of these surveys were subsequently combined with the security assessments to come up with a cost model. The predictive capabilities of this model were then assessed.

3.2.1. Security state assessment and cost modeling

The ultimate aim of the data collection among businesses was to model and predict a subset of the cost of cybercrime, in this case the effective losses incurred by businesses through cybercrime. The archetypical example in this case is the banking industry. Banking has internet facing websites that are often attacked through various means resulting in monetary losses. The banking industry is unique since it is heavily regulated, and is legally required to keep a database of these losses. This is not the case for other industries. However, the individual case data is typically not disclosed; only the consolidated country data is available. In a first body of work, we performed country and sector wide variable measurements of web hygiene. Secondly, we correlated these measurements with the data of two survey waves (see below) to come up with a predictive model of the losses based on web hygiene.

In a nutshell, first we collected web hygiene parameters for Belgium and Europe. To assess the evolution thereof, we then focused on a (long term) longitudinal study of the problem. Finally, we built the model for losses using these technical internet-observable variables and business parameters obtained through surveys as input and as such provided a loss estimate.

3.2.2. Surveys

A second strategy that we adopted to obtain data from Belgian businesses, was the administration of two survey waves, one between June and August 2016 and one between November 2017 and February 2018. In this paragraph, we first discuss the questionnaire that was used, followed by a description of the sampling procedures adopted and the final samples obtained. We conclude this paragraph with a short overview of the procedures that were used to analyze the data.

3.2.2.1. Questionnaire

In both waves, we operationalized the key concepts in a questionnaire, which we have administered via a web-based survey. In the first part, we have asked several general questions to enable the categorization of the businesses according to, inter alia, their size and economic sector. In both waves, the bulk of the questionnaire was structured on the basis of the cybercrime typology (see results section). For each type of cybercrime, the questionnaire followed a similar format and entailed five (sets of) questions to fulfil the study objectives.

The first question asked the respondents how often their business had been confronted with the selected cybercrime type in the past 12 months. The eight possible answers—ranging from never to hundreds of times a day—served to direct respondents to the next set of questions. If the answer was never, the survey immediately proceeded to the fifth set of questions. In the case of single (once) or multiple victimization (a few times up to a hundreds of times a day), respondents were expected to answer the following sets of questions for this incident. In the case of multiple victimization, we asked the respondents to distinguish in the following sets of questions between the last and the most serious incident for all types. As illegal access to IT systems occurs much more frequently than the others (e.g., Clough, 2015; Wall, 2007), we asked the respondents to consider also all the “illegal access to IT systems” incidents that occurred during the past 12 months together.

The second set of questions entailed a specification of the incident. We started with a question to specify the incident. In the case of cyber extortion, for instance, respondents were invited to specify whether the incident could be best categorized as a demand for money (1) to avert or stop an attack; (2) to unblock systems or data, or (3) to avoid confidential or compromising data from disclosure—items that correspond to the three above-mentioned subtypes of cyber extortion, i.e., request of protection money, ransomware campaigns and requests of hush money. In the second wave, we added also a question focusing on the moment the incident was discovered (ranging from within an hour after the incident to a year after the incident or later). In this wave, we also asked whether judicial authorities, the Federal Cyber Emergency Team (CERT), the network administrator or other authorities had been informed of the incident and how long the business had experienced the negative consequences of the incident (ranging from less than an hour to more than two months).

The third and fourth sets of questions focused on the costs and non-material harms of cybercrime, respectively. To investigate the staff costs, in the first wave we asked the respondents to indicate the total amount of staff time that was needed to respond to/neutralize the incident. Possible answers ranged from less than an hour to more than 2 working months. By multiplying these figures with the earlier collected data on average personnel cost per hour of the businesses’ IT staff, we could thus estimate the personnel costs generated by cybercrime for the businesses that did not outsource such tasks to external consultants. In the first wave, we also asked the respondents to specify which portion of the staff time has been outsourced to external consultants or companies to

respond to each incident. In the second wave, we improved the questions concerning the personnel costs and asked the respondents to indicate whether business (IT) employees and/or external (IT) consultants or businesses were responsible for neutralizing the incident. If respondents indicated that business employees were responsible, we asked them to estimate the number of man hours spent by these employees on neutralizing the incident; by multiplying this number by the average salary of an IT employee of the business (as questioned in the first part), we obtained an estimate of the internal staff costs of the incident. If the respondents stated that external consultants or businesses were responsible for the neutralization, we asked them to estimate the amount of money spent on the outsourcing of the incident neutralization. Combining internal staff costs and outsourcing costs, we obtained an accurate estimate of the total staff costs spent by the business on the neutralization of cybercrime incidents. In both waves, for the five other costs we asked the respondents to estimate the amount of money spent or lost because of the incident. The possible answers ranged from less than €1.000, to more than €20.000 for internet fraud, and from nothing to more than €200.000, for the four other types of cybercrime.

Following Greenfield and Paoli (2013), we conceptualize other harms as harms to the business's functional integrity, reputation and "privacy." We further split functional integrity into two subcategories: internal operational activities, and services to customers. All these harms cannot fully be expressed in monetary terms. It is difficult to put a dollar or euro value on some harms, such as those to privacy. For others, it might be conceptually possible, but the data to do so might be insufficient. These problems are also discussed in the cybercrime literature: both Klahr et al. (2016: 39) and the NCSC (2016: 19) admit that it is very hard to estimate the full economic impact of security breaches. Klahr et al. (2016: 39-40), in particular, note that "it is very uncommon for businesses to have ongoing monitoring of the financial cost of cyber security breaches, with just five per cent of firms saying they do this."

To avoid these problems, in both waves we have asked the respondents to assess the severity of the harms to the four interest dimensions on the basis of a six-point scale, including the categories of no harm, marginal, moderate, serious, grave, and catastrophic. In the second wave, we also asked the respondents to use the same scale to assess the severity of the overall harms to material support, which we described as financial impact in the questionnaire. This helped us to get an idea of the relative weight of the material costs reported above vis-à-vis the non-material harm. To help the respondents clearly understand the meaning of our ratings, in both waves we gave them some guidelines. In the first wave, the following text was used: "In assessing the severity of a harm please consider the ability of your business to fulfil its mission in the mid and long-term (thus six months or longer) as a benchmark:

- A "catastrophic" harm would be a harm that prevents your business from fulfilling its mission for six months or longer;
- At the opposite end, a "marginal" harm is a harm that affects only lightly and/or shortly your business's ability to fulfil its mission;
- Given this long-term perspective, an incident that shuts down all business's services for one day or two would be "serious" or "grave" but not "catastrophic";

- “Not applicable” means that this type of cyber incident cannot (according to you) have an effect upon the item being asked.”

In the second wave, we slightly revised and simplified the text: “In assessing the severity of a harm please consider the ability of your business to fulfil its mission in the mid and long-term (thus six months or longer) as a benchmark:

- "Catastrophic" harm means that the business was prevented from fulfilling its mission for six months or longer;
- "Marginal" harm means that the business's ability to fulfil its mission was affected only shortly;
- “No harm” means that the business's ability to fulfil its mission was not affected.

The fifth set of questions of the core part of the survey invited the respondents to assess the risk of (another) victimization for each of the five cybercrime types in the next 12 months on a 4-point scale ranging from very unlikely to very likely. The sixth part included some more general questions about cybercrime and had to be filled out by all respondents. In this part, we for example asked the respondents to assess the harm of cybercrime in general for all businesses within their sector in the previous 12 months and this for the four interest dimensions of non-material harm as well as financial interests (see above).

The final part of the first-wave questionnaire focused on the measures businesses take to prevent cybercrime. We asked respondents whether their businesses had acquired the following tools to protect the company's computers and electronic data in the past 12 months: (a) an anti-spam filter, (b) anti-phishing software, (c) anti-cryptolocker software, (d) automatic back software, (e) anti-virus software, (f) a software firewall and (g) a hardware firewall. Next, we asked the respondents to indicate how often their business performed the following procedures to prevent cybercrime: (a) updating the anti-virus software, (b) updating the operating system of computers, (c) updating the operating system of mobile devices, (d) updating the internet browser, (e) updating the general software and (f) making a backup of essential business data. Answers could range from yearly to always, with a separate answer possibility if the employees managed the procedure themselves. The last question of this part concerned insurance: specifically, we asked the respondents whether their business had an insurance against cybercrime, and if so, how much it had to pay for this insurance on a yearly basis. The possible answers here ranged from less than €500 to more than €100.000.

In the second-wave questionnaire, the questions on preventive measures were placed right after the general questions and were slightly revised. For the first subset of questions, we asked whether the businesses have—thus no longer if they had bought in the previous 12 months—the same tools mentioned in the first wave, i.e.: (a) an anti-spam filter, (b) anti-phishing software, (c) anti-cryptolocker software, (d) automatic back software, (e) anti-virus software, (f) a software firewall and (g) a hardware firewall. The question regarding procedural prevention and insurance remained unchanged. Departing from the previous questionnaire, in the second wave we added two questions on training, asking respondents whether their business organizes training for their employees to prevent and/or detect

cybercrime and how many of their employees participate in training organized by other organizations or institutions. The possible answers for this question were no one, a minority, half, a majority and all.

3.2.2.2. Sampling Procedures and Final Samples

The target population of the surveys consisted of all the businesses based in Belgium. For the first wave, we constructed a sampling frame of 9,249 business representatives based on information provided by the Federation of Enterprises in Belgium (FEB), the largest business consortium in Belgium representing more than 50.000 small, medium and large businesses based in Belgium, and by the sector federations Comeos and Febelfin. These two federations represent sectors considered particularly vulnerable to cybercrime, i.e., commerce and services as well as banks, stock markets, credit and investment businesses, respectively. For the second wave, we used a list of 10,479 business representatives provided by the FEB as sampling frame.

We sent letters of invitation via an automatically generated email to all members of the sampling frame using the email addresses they had listed with the federations. With the mail, the business representatives also received a unique code to access and resume the survey on LimeSurvey, an online survey software program. The first survey was distributed in three languages, Dutch, French and English and ran from June to August 2016—a period during which we sent three reminders (early July, late July, Mid-August), whereas the second survey was only distributed in Dutch and French, the two main languages in Belgium, and ran from the end of November 2017 to the beginning of February 2018—a period during which we sent three reminders (mid-December, and beginning and end of January).

The number of non-contacts was high: 1,198 business representatives in the first wave and 1,513 business representatives in the second wave could not be reached, due to undeliverable emails, unavailable mailboxes, or expired e-mail addresses. Of the business representatives who are expected to have received the e-mail, 310 (first wave) and 277 (second wave) filled out the questionnaire in such a way that their record could be retained for statistical analysis, which brings the valid response rates at 3.4% and 2.6%, respectively. These rates are not much lower than the response rate of the CSI (2011) study (6.4%) but much lower than the response rate achieved by Klahr et al. (34% in 2016 and 27% in 2017), the only two other studies that are explicit about it.

For both waves, the majority of the businesses that took part in the survey have their headquarters in Flanders (first wave: 61.9%; second wave: 66.4%). Further, the Brussels region accounts for 20.8% (first wave) and 21.2% (second wave) of the samples, and Wallonia for 13.7% (first wave) and 11.3% (second wave). The number of businesses whose headquarters is outside Belgium is considerably lower, amounting to 3.6% (first wave) and 1.1% (second wave) of the samples. By comparing these figures with the official data about the location of businesses and persons liable for VAT (FOD Economie, 2016), we note that the percentage of the Flanders-based businesses taking part in the surveys corresponds more or less to the percentage of businesses and persons liable for VAT located in Flanders

(60.4%). In our samples, there is instead an overrepresentation of the Brussels-based businesses, as they effectively count only for 11.1%, and an underrepresentation of those based in Wallonia, which are in reality about a quarter of the Belgian businesses and persons liable for VAT (26.6%).

The businesses taking part in the survey belong to many different economic sectors, but many sectors, and the related sector federations, are only represented once or twice in our samples. The sectors most strongly represented in both samples are technology (represented by the sector federation Agoria; first wave: 22.6%; second wave: 21.8%) and chemical and life sciences (represented by the sector federation Essenscia; first wave: 10%; second wave: 7.5%), In the first wave, commerce and services (represented by the sector federation Comeos; 9.6%) was also strongly represented and in the second one, credit and investment (represented by the sector federation Febelfin; 7.1%) and textiles, woodworking and furniture (represented by the sector federation Fedustria; 7.1%). Due to the low number of representatives of many sector federations, we could not make the analysis of the incidence or impact of cybercrime per sector.

As for the size of the businesses, we distinguish between small, medium and large businesses, based on staff headcount, following the standard classification of the European Commission (2003). This defines businesses with less than 50 staff as small, those with a staff between 50 and 249 as medium, and those with more 250 or more staff as large. In our samples, around half of the businesses are small (first wave: 51.5%; second wave: 50%), the rest of the sample being almost equally distributed amongst medium (first wave: 22%; second wave: 21%), or large (first wave: 26.6%; second wave: 29%) businesses. Comparing these figures with the data of the Belgian Ministry of the Economy (FOD Economie, 2016) on all the businesses and persons liable for VAT, we notice that our final sample does not reflect the distribution of Belgian businesses based on size. Specifically, large businesses are underrepresented, and small businesses are overrepresented in our final samples.

3.2.2.3. Data Analysis

We used SPSS Statistics 24.0 (2016) to analyze the data of both waves. For each wave, we conducted descriptive analyses on all variables, which, as already mentioned, constitute the bulk of our results section. In addition, we used t-test to investigate whether the incidences, the perceived victimization risk and the costs and no-material harms were significantly different in the two waves. For all the analyses, we have used the standard significance level of .05.

3.3. Government

Initially, we designed a web survey to gather the necessary data for the government. However, the obtained data were too limited for meaningful analyses. Hence, we decided to shift the focus of our research to (i) an analysis of the answers of the Belgian federal government to parliamentary questions concerning the impact of cybercrime and (ii) interviews with representatives of the federal government and two big Belgian cities.

3.3.1. Survey

A web survey similar to the survey for the businesses was designed to gather the necessary data for the government. The target population of this survey consisted of all IT employees working for government organizations in Belgium (i.e. federal, regional as well as local organizations). Since an appropriate sampling frame for these population units was unavailable, we used a convenience sample, implying that the obtained sample consists of participants that could (easily) be reached by the researchers (Bijleveld, 2009).

In order to get access to potential participants, we contacted representatives of following governments or institutions with a request for participation in the study:

- Federal government
- Flemish government
- Walloon government
- French-speaking community government
- Brussels government
- IT organization of Flemish provinces and cities
- IT organization of Walloon provinces and cities

However, only the federal government, the Walloon government, the Brussels government and the IT organization of Flemish provinces and cities were willing to participate in the study. Hence, the survey could only be distributed (via our contact persons or directly) among IT employees of these three governments and among IT employees of the Flemish provinces and cities. More concretely, the IT employees were sent the link to access and resume the survey on LimeSurvey. The survey was distributed in Dutch and French, the two main languages in Belgium, and ran from June to August 2017.

Although extra efforts were made to increase the response (i.e. reminders and calls to potential participants), only four people completed (entirely or partially) the questionnaire. Hence, the data gathered via the survey were too limited to perform meaningful analyses.

3.3.2. Parliamentary Questions

We analyzed a set of eighteen responses given by the Belgian federal ministers and state secretaries to a parliamentary question. This question probed into the cybercrime situation as experienced by the Belgian federal government in 2015 and it was posed by parliamentarian Nele Lijnen in early 2016.

The question under discussion was retrieved, together with the subsequent responses, from the Belgian Chamber of Representatives' website (www.dekamer.be) by using the predefined EUROVOC-descriptor 'Computercriminaliteit' as a search term. Using this EUROVOC-descriptor, we obtained a list of questions sent to more than 160 addressees during the period between 2010 and 2016 – however, the same question was often sent to

multiple addressees and not all questions yielded a response. At the time of the data collection, the question under discussion was the only parliamentary attempt that was elaborate and profound enough to make a systematic analysis possible and which suited our needs. It provided the researchers with the opportunity to take a timeframe into consideration of exactly one calendar year (i.e., 2015), thereby adhering to the methodology used in our earlier study on cybercrime. This way, this analysis would enable a cautious comparison between the cybercrime victimizations in 2015 and 2017, albeit not without paying strict attention to issues such as differences in the wording of questions. Other questions that were retrieved by using the descriptor mentioned above but weren't considered eligible for analysis, took a timeframe into consideration that was too broad for a meaningful and accurate analysis (e.g., cyber incidents from 2010 to 2014), or were related to topics that fell beyond the specific scope of the present research project (e.g., phishing mails that were sent to the general population, proposed changes to the legislation, priorities of and investments in the Federal Computer Crime Unit, the cyber defense capacity of the Ministry of Defense, etc.).

The question consisted of seven sub-questions probing federal public services on (1) the number of times their administrations were victimized by cybercriminals, (2) the nature and impact of these incidents (e.g. loss of data or sabotage of an IT system), (3) evolutions in the complexity, professionalism, etc. of the attacks, (4) the preventative measures aimed at controlling cybercrime that were in place at the time, (5) the number of times legal action was taken in the wake of an attack and the outcome, (6) their assessment of how realistic a scenario was in which their victimization went unnoticed and (7) the relationship (and the impact thereof) between their administrations and the – then newly established – Centre for Cybersecurity Belgium (CCB).

The answers to the question under discussion were organized and analyzed using the QDA-software package NVivo (v.11). The ultimate focus was on the clustering of information obtained from the respondents' answers to the question under discussion around a number of concepts of interest – or so-called 'sensitizing topics'. These were the same concepts that were of central importance in the surveys (cf. supra). This resulted in the creation of four clustered categories, namely "Number of incidents", "Further specification of the incident(s)", "Cost(s) related to the incident(s)" and "Harm(s) related to the incident(s)". In an attempt to group the relevant information into one of these predefined categories, some coding phases could be discerned which bear close resemblance to some of those identified by Strauss and Corbin (1990) in their elaboration of Grounded Theory-methodology, i.e. axial coding and selective coding.

3.3.3. Interviews

In this part, we briefly present the interview research design. We start with a description of the topics that were discussed with the interviewees and then continue with the sampling, data collection and data analysis.

3.3.3.1. *Topics*

To collect the data, we administered semi-structured, in-depth interviews. Hence, we made use of a topic list, containing the topics that should definitely be discussed with the interviewees. The topics were split into two sections: cybersecurity and cybercrime. In the first section, we asked the interviewee about the importance of cybersecurity for the organization and how this importance has evolved over time. Next, we asked the interviewee to describe the cybersecurity structure within the organization. Here, we asked the interviewee whether the organization had its own IT employees and/or they made use of external IT consultants and businesses. In addition, we focused on the technical and organizational cybersecurity measures the organization implements and the cybersecurity training the organization offers to its employees. For the cybercrime section, we used the five cybercrimes we identified in our typology as a guideline. First, we asked the interviewee to indicate the extent to which the organization has been confronted with cybercrime and to describe the cyber incidents the organization had encountered. We also focused on the way the organization dealt with cyber incidents. More concretely, we asked the interviewee to indicate who was responsible for resolving such incidents, as well as to indicate the people or entities that were informed of cyber incidents (e.g. judicial authorities, CERT etc.). Secondly, we asked the interviewee to assess the total harm of cyber incidents on the organization, as well as to assess the material harm (or costs) and non-material harm separately. For the latter, we made a distinction between the harm to services to citizens, internal operational activities of the organization, reputation, and privacy (see also typology for public and private entities). To conclude the interview, we asked the respondents to describe the expected evolution in the organizations' confrontation with cybercrime for the coming years, as well as to indicate which measures they deem necessary to counter future cyber incidents.

3.3.3.2. *Sampling and Data Collection*

From the population of Belgian government organizations, we selected both federal, regional as well as local organizations in order to obtain insights about the situation at the different government levels. More concretely, we approached the federal government, the Flemish government and three cities, two of which are located in Flanders and one of which is located in Wallonia. No answer was received from the Flemish government and the Walloon city. Hence, interviews were only administered for the federal government and the two Flemish cities.

The interviews were administered face-to-face. Interviewees participated on a voluntary basis and were informed that their answers would be treated confidentially. Each interview took approximately one hour and was recorded on a voice recorder. Afterwards, detailed summaries were made of the interview, which were then sent to the interviewees to verify whether the interviewer had understood everything correctly and to allow the interviewees to add things that they thought had to be added.

3.4. Forecasting

We first provide a caveat on cost forecasting for cybercrime. We proceed the design considerations for the survey questions.

3.4.1 The Problem of Cost Prediction

The current impact of cybercrime is limited by a number of factors that will change in the near future. The most important changes are:

1. Since the cyber world is still quite separated from the “real” world, cybercriminals still need to convert their cyber gains into exchangeable goods like cash. Often this conversion process can be used to track and catch cyber criminals. With the proliferation of digital currencies and the increase of the digital market, the need for conversion will decrease.
2. The deployment of the Internet of Things will multiply the number of devices that can be attacked by cyber criminals. The merger of “meat space” and cyber space will increase the opportunities for extortion.

Consequently, while the current situation might give the impression that investments in cyber security are too high compared to the costs of cyber criminality, the expected increase in the latter might quickly change this situation in a few years, if the industry and the society do not prepare. Furthermore, many cybercrimes lead to losses that are difficult to measure (e.g. reputation, loss of opportunity) and cybercrimes are often not detected because of the complexity of the cyberworld. These factors add to the complexity of the forecasting.

3.4.2 Survey Considerations and Questions

The survey questions were composed with the following considerations in mind:

1. In order to keep the response rate high, the survey was kept short. This was the foremost consideration.
2. Since not all potential respondents are security specialists, the questions were made intelligible also by people who are not specialists.
3. Since IT security is a sensitive issue, we asked for data that companies are willing to share.

After several discussions with other members of the consortium, this resulted in the following 6 questions.

1. *How is the effectiveness of your security program evaluated?*
The possible answers are: *Penetration testing by ICT personnel in your company, Penetration testing by external consultants/company, By Vulnerability assessment, Not, By Risk Assessment, Others.*
2. *What IT or security certifications does your company have? Are there any that the company is pursuing within a time frame of two years?*

3. *Does your company have an insurance to protect itself from cybercrime and if yes how much does your company pay for it?*
The possible answers are: *No insurance, Less than € 500, Between € 501 and € 1,000, Between € 1,001 and € 2,000, Between € 2,001 and € 5,000, Between € 5,001 and € 10,000, Between € 10,001 and € 20,000, Between € 20,001 and € 50,000, Between € 50,001 and € 100,000, More than € 100,000.*
4. *Has your company in the last 12 months acquired any of the following tools to protect the company computers and electronic data? Indicate all that apply.*
The possible answers are: *Anti-spam filter, Anti-phishing software, Anti-cryptolocker software, Automatic data back-up software, Anti-virus software, Software Firewall, Hardware Firewall, Others.*
5. *How many man-hours per week does your company invest in the prevention of cybercrime?*
The possible answers are: *None, Less than 1, Between 1 and 10, Between 11 and 50, More than 51.*
6. *What does your company do to keep itself updated in the prevention of cybercrime?*
The questions is answered separately for following prevention methods: *Update anti-virus software, Update OS of computers, Update OS of mobile devices, Update Browser, Update General Software, Back-up of essential company data.* The possible answers are: *Managed by employee, Weekly, Monthly, Yearly, Always (i.e. every time update is available).*

4. SCIENTIFIC RESULTS AND RECOMMENDATIONS

In this part, we first discuss the scientific results of the project. We make a distinction between the typologies we developed (discussed in the first paragraph) and the results of our empirical studies (discussed in the second paragraph). In the final paragraph, we discuss the recommendations that arise from the results of our studies.

4.1. Typologies

In this paragraph, we discuss the cybercrime and impact typologies we developed throughout the project. First, we focus on the way cybercrime and impact are conceptualized for citizens. Secondly, we shift our attention to the conceptualization of cybercrime and impact for businesses and government organizations.

4.1.1. Citizens

4.1.1.1. Cybercrime

In academia and beyond there is no consensus about the concept of cybercrime and what it entails. Holt and Bossler (2015) claim that the difficulty of defining cybercrime lies in the multidisciplinary context in which cybercrime resides. Some adopt the conceptualization in the justice system as a baseline to define cybercrime (Stratton, Powell, & Cameron, 2017). Others define cybercrime after their real-life counterpart (e.g. cyberstalking is defined as stalking in an online environment) (Reyns, Randa, & Henson, 2016). Still others refer to the technical components of a specific threat when defining cybercrime (Van der Hulst & Neve, 2008).

Cybercrime that might target public and private entities, however, differs to a great extent from cybercrime that might target private individuals/citizens.

To conceptualize cybercrime for the general public, we aim to include all the above-described components in an overall definition to be holistic and all-encompassing (WP1):

“Cybercrime comprises all computer-mediated activities, committed over electronic communication networks and information systems in an electronic environment, which are either illegal or considered illicit by certain parties and which can be conducted through all global electronic networks and media. These activities affect society as a whole due to their cost for and impact on individuals, industry and the government. They are directed against the confidentiality, integrity and availability of automated processes/resources and focused on interfering with or affecting the operation of computer systems/systems that maintain automated processes.”

Computer-mediated activities are commonly divided into computer-assisted crimes and computer-dependent crimes, with the first being crimes that use the computer as a tool to do an already existing crime, and the second being a crime where the computer is the target (Europol, 2017). This division is widely accepted by policymakers and researchers (Li, 2016;

Riek, Böhme, & Moore, 2016; Stabek, Watters, & Layton, 2010; Tsakalidis & Vergidis, 2017; Van der Hulst & Neve, 2008).

We followed the approach of Anderson et al. (2013) and Holt and Bossler (2015) to divide and categorize cybercrime in different cyber threats. Over the two waves we fine-tuned this classification based on the results of the first wave, new insights of the Internet Organized Crime Threat Assessment and more recent research (Europol, 2017; Rens, 2015).

In our typology, we distinguish four types of cyber threats:

- A. Malware
- B. Scams
- C. Hacking
- D. Monitoring

Malware and hacking are both considered computer-dependent crimes, whereas monitoring and scams are considered computer-assisted crimes (Li, 2016, Riek, Böhme, & Moore, 2016; Stabek, Watters, & Layton, 2010; Tsakalidis & Vergidis, 2017; Van der Hulst & Neve, 2008).

Our typology is neither exhaustive nor mutually exclusive but does include most encountered cybercrimes.

Malware

Malware is described as one of the key threats of cyber-dependent crimes (Interpol, 2017). The two dominant malware threats are defined as ransomware and information stealers. We define malware as the umbrella term for software that alters the normal functioning of a device (Dang-Pham & Pittayachawan, 2015). Malware thus includes trojans, worms and viruses where technical knowledge is needed to deploy and delete (Bergmann, Dreißigacker, von Skarczynski, & Wollinger, 2018). In line with Chawla and Chouhan (2014), we perceive malware to be a “technical” type of cybercrime .

Malware is defined as the malicious software that affects the normal functioning of your device.

E.g. virus, worms, Trojan horses, adware, botnets, ransomware...

Scams

Scams are described as misleading actions to obtain information or money. On a large scale, end users are deceived and impersonation is used to obtain a target’s information (Anderson et al., 2013; Lastdrager, 2014). Scams rely on human error and social engineering to reveal sensitive information from the victims (Aike, Mahon, Haughton, O’Neill, & O’Carrol, 2016; Rao & Ali, 2015). Recognizing something as a scam is seen as one of the biggest defense mechanisms to protect oneself against it (Albladi & Weir, 2018). Contrary to malware, we perceive scams to be a “social” type of cybercrime (Chawla & Chouhan, 2014). Our line of

thought is strengthened by the research of Alsharnouby, Alaca, and Chiasson (2015), who found no correlation between technical proficiency and the ability to detect scams.

Scams are defined as an action whereby information or money is obtained by misleading a victim using information technologies.

E.g. via mail, false websites...

Hacking

Hacking is defined as unlawful or unauthorised access (Martellini, Abaimov, Gaycken, & Wilson, 2017; Verdegem, Teerlinck, & Vermote, 2015) and is linked to the key threat “data breaches” and “network attacks” by the Internet Organised Crime Threat Assessment (Europol, 2017).

Hacking is defined as obtaining unauthorized access to a computer or internet account.

E.g. Facebook, mail....

Monitoring

In our typology of cybercrime, we also include activities that are considered illicit. Therefore monitoring was taken into account as a cybercrime even as this is not always the case from a legal point of view. In line with others we argue that the activity of monitoring in some occasions can be considered unethical and/or illicit (Dinev, Hart, & Mullen, 2008; Froomkin, 2015; Lyon, 2014; Verdegem et al., 2015).

Monitoring is defined as collecting data from a victim by the government or a private company.

E.g. checking internet usage, reading e-mails... .

4.1.1.2. Impact, Harms and Costs of Cybercrime

It is important to have a general understanding of what one should understand as costs connected to cybercrime (Agrafiotis et al., 2016). In a systematic literature review of more than twenty studies that estimated the cost of cybercrime Wickramasekera, Wright, Eley, Murray and Tubeuf (2015) found no consensus about what should and should not be counted as a cost of cybercrime. Evidently, the measured costs were different across the studies. Anderson et al. (2013) differentiate between direct, indirect and defence costs.

Anderson et al. (2012) division of the different costs was originally made to measure the total cost of cybercrime in response to the request of the UK Ministry of Defence to debunk overestimations of costs. After the study, they explicitly chose not to add up the different costs as this would show an opaque, context-free figure deemed meaningless (Anderson et al., 2013).

In contrast to the approach of Anderson et al. (2013), Paoli, Visschers, Verstraete and van Hellefont (2017) do not have the intention to quantify every cost of cybercrime. Harm is the

direct non- quantifiable cost used in the framework of Greenfield and Paoli (2013) and is widely used as a concept by legislators of the EU.

The costs also differ depending on the perspective one adopts; the victim, government and society. (Wickramasekera et al., 2015). Greenfield and Paoli (2013) distinguish four perspectives or potential “bearers of harm”, namely; individuals, private-sector entities, the government and the social and physical environment (Greenfield & Paoli, 2013). Every bearer has its own relevant “interest dimensions” where harm could be experienced. In this study, we measure the costs through the viewpoint of the victims. For individuals, this is functional integrity, material support, reputation and privacy and autonomy. We combined the categorization of Anderson et al. (2012) and Greenfield and Paoli (2013) of these direct costs.

Lagazio, Sherif and Cushman (2014) proposed indirect costs as opportunity costs in their research. Additionally, a recent news release operationalized indirect costs as the opportunities someone lost because of security concerns (Eurostat, 2016).

We combine the classifications of Anderson et al. (2013), Paoli et al. (2017) and Lagazio et al. (2014) and differentiate between direct costs, opportunity costs and defence costs. Direct costs, however, are split into the direct monetary and direct non-monetary costs. Direct non-monetary costs are described using the harm assessment framework with the absence of material support as interest dimension (as this is seen as a direct monetary cost in this research). Under opportunity costs, we see the indirect costs as proposed by Lagazio, Sherif and Cushman (2014) and Eurostat (2016). Defence costs are the last category (see Anderson et al. (2013). Contrary to the research on the impact of cybercrime on Belgian businesses, we believe that citizens are able to estimate their spending on defence against cybercrime as their expenses are not bundled as in businesses (Paoli et al., 2017). Indirect costs and defence costs are reported to be surprisingly high for cybercrime, which makes them of special interest (Anderson et al., 2013). We do believe however it is important to make a clear separation between the direct, indirect and defence cost to retain a transparent view of the costs.

In sum we include three types of costs for citizens, namely direct, indirect and defence costs. Direct costs are divided into direct monetary and direct non-monetary costs.

Direct costs are the monetary equivalent of losses, damages, or other suffering felt by the victim as a consequence of a cybercrime. **Direct monetary costs** are the financial direct costs. **Direct non-monetary costs** are the non-financial direct costs, considered as harm.

Indirect costs are described as the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, these include loss of trust and loss of opportunity.

Defence costs are the monetary equivalent of prevention efforts.

4.1.2. Businesses/Government

4.1.2.1. Cybercrime

Following the approach adopted by legal texts, policy documents and other studies (e.g., UNODC, 2013), the present project does not define cybercrime per se, but rather identifies specific acts that constitute cybercrime. Unlike most other studies on the cost and impact of cybercrime, we have developed a “technology-neutral” typology of cybercrime, i.e., a typology that is independent of the specific techniques used by cybercriminals. The typology largely draws from the Council of Europe’s Convention on Cybercrime, and the Belgian criminal law concerning cybercrime, but also incorporates the insights from the academic literature on the topic. The typology entails five types of cybercrime that might target public and private entities:

- A. Illegal access to IT systems
- B. Cyber espionage
- C. Data or system interference
- D. Cyber extortion
- E. Internet fraud

The first three types belong to the category of “computer-integrity crimes” (Gordon & Ford, 2006: 14) and the latter two to the category of “computer-assisted crimes” (Wall, 2007: 50). Our conceptualization of the three computer-integrity crimes is based upon the Council of Europe’s Convention and Belgian cybercrime law. In fact, the incidents of illegal access to IT systems, cyber espionage and data/system interference, correspond, respectively, to the offences of “illegal access” (art. 2), “illegal interference” (art. 4) and “data” and “system interference” (art. 5-6) in the Convention. The type “cyber extortion” has no direct correspondence in the Convention; it is rather the cyber version of a standard offence in Belgian and other national criminal laws. The last type, “internet fraud,” draws from the offence of computer-related fraud defined by the Convention (art. 8) as well as two other more traditional types of fraud that frequently occur online.

Illegal Access to IT Systems

This first type is comprised of illegal access to IT systems. The generic term “IT system” exemplifies the technology-neutral way in which the survey is drafted. Following the Council of Europe’s 2001 convention, an IT system is conceived as “any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data”.

Illegal access to an IT system can be achieved in many different ways, for example through the use of hackertools, such as exploit kits, Trojan horses, backdoors, password sniffers and the like (e.g., Bernaards et al., 2012: 27-34; ENISA, 2016: 19-21). In addition, cybercriminals can also avail themselves of specific techniques in order to “socially engineer” log-in information out of unsuspecting users. Supporting techniques include (spear)phishing, password guessing or even checking discarded documents retrieved from the waste disposal (e.g., Bernaards et al., 2012; Leukfeldt, Domenie & Stol, 2009; Van der Hulst & Neve, 2008;

Wall, 2007). The Council of Europe's 2001 Convention also compels the parties to criminalize acts of legitimate users of the IT system (e.g., employees, hired consultants etc.) who exceed their access privileges, considering them as instances of illegal access. This obligation has, for example, been introduced in Belgian Penal Code with Art. 550bis. Illegal access can also occur by exploiting known vulnerabilities in the security – ranging from zero-day vulnerabilities to accessing an unprotected WiFi-network of a public or private entity (e.g., Centraal Planbureau, 2016; Verizon, 2016).

Cyber Espionage

Cyber espionage presupposes illegal access to an IT system (Verizon, 2016: 52), regardless of the technique employed. The close link between the two types was also acknowledged by the Belgian criminal (cyber) act of 2000: the Belgian legislator, in fact, has criminalized this offence, by simply adding an extra paragraph (art. 550bis, §3, of the Belgian Penal Code) to the article concerning illegal access to an IT system. When the espionage attempt is successful, this results in the theft of confidential and protected information that for one reason or another is important for the entity (ENISA, 2016: 39). Just as was the case with the conceptualization of an "IT system," our conceptualization of "data" also has a technology-neutral character. Following the Council of Europe's 2001 convention, data is understood here as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function."

Cyber espionage is nowadays a common cybercrime (e.g., Europol, 2016; Gemalto, 2016). Several types of data can be targeted, but they all have in common that they are in one way or another of high value to motivated cybercriminals, whether these are malicious insiders, or outsiders, hacktivists, or hostile nation states (Europol, 2016: 36; Gemalto, 2016: 6; Wall, 2007: 94-101). According to ENISA (2016: 39) identity information is the most frequently targeted and breached type of data (50%), followed by, financial access credentials (over 20%), confidential data, or data on intellectual property (over 10%), and user credentials (over 10%).

Given the great variety of data types stored in the IT systems of public and private entities, we have used generic categories for the data that might constitute the primary object of the attack. For private entities, these include a) bulk business data (e.g., details of customers or employees and financial details of the organization); b) data on high-value intellectual property (e.g., R&D outputs and product prototypes); c) data containing tactical corporate information (e.g., contract bid prices and documents describing business processes or strategies), and d) the residual category "other" (see Detica, 2011: 9 and Deloitte, 2016: 12). On the other hand, for public entities, these include a) publicly available data about individuals, b) non-publicly available data about individuals, c) confidential data about individuals, d) other publicly available data, e) other non-publicly available data and f) other confidential data. Non-publicly available data can be accessed by the data subject and his or her delegates; for confidential data this is not the case.

Data/System Interference

The third type of computer-integrity crimes consists of data or system interference. This can be achieved through a myriad of specific techniques (e.g., viruses, worms, cryptoware, (D)Dos-attacks performed by botnets etc.; e.g., Bernaards et al., 2012; Leukfeldt et al., 2009; Van der Hulst & Neve, 2008) but can be classified under two broad categories: data interference (e.g., Van der Hulst & Neve, 2008: 71-73) and system interference (e.g., Van der Hulst & Neve, 2008: 73-77). Both categories are criminalized under Belgian IT law by means of an article referring to the offence of IT sabotage (Art. 550ter of the Belgian Penal Code).

In line with the Council of Europe's 2001 convention, an interference - as defined in this study - refers to the intentional "damaging, deletion, deterioration, alteration or suppression of computer data without right" and/or to the "serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data". In practice, most interferences are provoked by malware infections, but they can also result from malicious actions of persons or groups that first gained illegal access to the IT system. Data interferences are mainly caused by (i.e., Distributed denial-of-service) attacks or by spamming. In both cases, the IT system becomes overloaded by the massive quantity of data (requests) sent (Van der Hulst & Neve, 2008: 19). In the case of data interferences, the negative impact can vary heavily depending on both their intensity and duration (Centraal Planbureau, 2016: 49).

Cyber Extortion

Over the last few years, the number of companies victimized by ransomware has been on the rise drastically (ENISA, 2016: 45; Europol, 2016: 17; Munnichs, Kouw & Kool, 2017: 15; Van Leiden, Appelman, Van Ham & Ferwerda, 2014: 41). A system can become infected with this type of "crimeware" through multiple techniques, ranging from infected email attachments or links to other types of malware (Domenie, Leukfeldt, van Wilsem, Jansen & Stol, 2013: 39; Verizon, 2016: 46). The malware encrypts data stored in the IT system, making the data (or even the entire system) inaccessible or unusable to authorized users (Centraal Planbureau, 2016: 35; Verizon, 2016: 46). Recovery from this kind of infections is by and large not possible, since the data can only be "freed" when the user enters a cryptographic key that only can be obtained via the cybercriminal responsible for the infection (Munnichs et al., 2017: 15). While private persons often seem to be rarely inclined to pay a ransom of a few hundred euros (Centraal Planbureau, 2016: 35), some sources suggest that public and private entities generally show a greater willingness to pay to restore their operational integrity and/or protect their reputation (Munnichs et al., 2017: 15). According to some sources (e.g., Centraal Planbureau, 2016: 38) ransomware-campaigns have become a very lucrative form of cybercrime, not only because of their low cost and the low detection rate, but also because the extortionists can vary the ransom depending on the importance of the data for the entity.

In addition to the demand for a ransom, two other types of extortion are also prevalent in cyberspace. First, cybercriminals may (attempt to) extract “hush money” from public or private entities. This may happen after the entity in question has become the victim of a data breach and the extortionists subsequently threaten to make the stolen data public (De Cuyper & Weijters, 2016: 7; NCSC, 2016: 38). Second, public or private entities may receive requests to pay protection money. Entities that are highly dependent on IT systems for their daily operations can prove attractive targets for this kind of extortion (Van Leiden et al., 2014). Cybercriminals can, for example, conduct a relatively small data breach or a (D)DOS-attack on the website, and inform the owner that a more devastating attack can be averted by paying the requested protection money (Munnichs et al., 2017: 20; Van Leiden et al., 2007: 40).

These forms of cybercrime show great resemblance with the more classic forms of extortion that are performed in the offline world. Therefore, they can be regarded as instances of computer-assisted crime that can be prosecuted by means of the ordinary criminal law (e.g., in Belgium, art. 470 Penal Code). The demand for protection money for example, has been taking place since time immemorial and has long been one of the favorite types of extortion for Italian mafia organizations (Leukfeldt et al., 2009: 102).

Internet Fraud

The last type, internet fraud, is also a computer-assisted crime and we have conceptualized it in terms of three specific types of fraud: fraud with internet banking, advance fee fraud and auction fraud. The first subtype of fraud exemplifies computer-related fraud as defined in the Council of Europe’s Convention (2001, art. 8), as it is a special case of fraud committed through “any input, alteration, deletion or suppression of computer data” (emphasis added). It can also be prosecuted under Belgian IT law by means of the article referring to computer fraud (i.e., art. 504quater of the Belgian Penal Code). In accordance with the Council of Europe’s 2001 convention the Belgian legislator created a new offence that criminalized, among other things, the intentional input of computer data into an IT system “with fraudulent or dishonest intent or procuring, without right, an economic benefit for oneself or for another person.”

The other two are covered by the traditional offence of fraud in national criminal laws (e.g., in Belgium, art. 496 Penal Code). Although, for Levi (2017: 5), “there is very little significant fraud that is not at least cyber-assisted in the late modern era,” we have chosen to focus on these two specific types, because they are, according to the literature, the most frequent types of fraud that affect public and private entities (e.g., Domenie et al., 2013: 62-64; Leukfeldt et al., 2009: 75; Levi & Burrows, 2008). Advance fee fraud typically involves promising the victim a large sum of money in return for a small up-front payment; if a victim makes the payment, the fraudster either invents a series of further fees for the victim, or simply disappears (Wall, 2007: 90). Auction fraud occurs when certain commodities or services are purchased and paid online but are either never delivered or are of a lower quality than the advertisement postulated (Domenie et al., 2013: 44; Van der Hulst & Neve, 2008: 56).

In addition to these three general types of internet fraud, we identify four types of internet fraud that are specific for government agencies, namely online benefit fraud, electronic embezzlement, online procurement fraud and online tax fraud (Button et al., 2009; Levi, 2008; Levi & Burrows, 2008; Levi et al., 2017). Online benefit fraud refers to various kinds of fraud upon the social security system, ranging from widespread ‘working and drawing’ by seasonal employees via housing benefit frauds to the more common failure to notify officials of changes in circumstances that disentitle claimants to benefits. Electronic embezzlement concerns frauds against public entities by staff, ranging from junior clerical staff to directors and officers. It normally involves accounts manipulation or the construction of false invoices. Online procurement fraud refers to fraud in the purchasing process (e.g., abuse of inside information in the construction of tenders). Bills sent out to public entities fraudulently claiming that they have ordered a placing in a business directory or similar scheme are also included. Finally, online tax fraud involves the failure to pay direct taxes, indirect taxes and excise taxes, when the payment occurs via the internet. Direct tax fraud encompasses income tax and corporation tax fraud, ranging from individuals failing to declare income from minor skilled work to large schemes involving corporate manipulation. Indirect tax fraud refers to VAT-fraud and excise tax fraud to alcohol and tobacco and motor oil tax evasion. Some tax frauds also arise at the local or regional government level, in relation to municipal taxes or the cadastral income.

4.1.2.2. Impact, Harms and Costs of Cybercrime

We understand the impact of cybercrime as the overall harm of cybercrime, that is, the “sum” of the material harms, or costs, and the non-material harms of cybercrime. We draw on Greenfield and Paoli’s (2013) harm assessment framework, to conceptualize harm—and thus impact itself. Specifically, we understand harm as a violation of stakeholders’ legitimate interests (see Feinberg, 1984), thus recognizing that the dominant political morality and the underlying socio-economic conditions play a role in establishing which interests are regarded as legitimate. Following Greenfield and Paoli (2013), we further assume that public and private entities experience harms as damages to one or more “interest dimensions” (von Hirsch & Jareborg, 1991: 19). These dimensions consist of functional integrity, material support, reputation, and privacy, of which only the harms to material support can be monetized and thus are costs. Following Greenfield and Paoli (2013), who build on von Hirsch and Jareborg (1991) and Sen (1987), we treat these interest dimensions as representing capabilities or pathways for achieving a certain quality of life, referred to as “institutional mission” (Greenfield & Paoli, 2013), in the case of public and private entities. Below we identify the harms to material support, or costs and subsequently consider the harms to the other interest dimensions.

We speak of harm to material support, or costs, when an entity suffers a material loss, such as damages to its infrastructure or remediation costs. In particular, we distinguish between personnel and other costs. For the personnel costs, we consider the internal and external costs. As for the other costs, we identify five categories: (1) hard- and software replacement; (2) value of other lost or damaged assets (e.g., data files); (3) money paid to offender; (4) fines and compensation payments, and (5) revenue lost. We note that not all the five costs are relevant for our five types of cybercrime. The fourth type of cost, money paid to the

offender, for example, is only relevant for cyber extortion: it consists of ransom, “protection money”, or “hush money”, the latter being a sum paid to buy the “silence” of cybercriminals after these have stolen confidential data from a business.

As for the non-material harms, our definitions are as follows. First, we consider functional integrity, as synonym of operational integrity. Given the centrality of this interest dimension, we have split harms to functional integrity in two, and further distinguish between “the provision of services to (potential) customers (private entities) or citizens (public entities)” and the entity’s “internal operational activities.” Damage to public and private entities can occur under a variety of circumstances, including those involving an employee, official or representative’s participation in a criminal activity. In this respect as well, we follow Greenfield and Paoli, (2013) who argue that such entities experience at least some reputational loss whenever rule- or lawbreaking leaves the impression that they are weak. Finally, public or private entities may also suffer a loss of “privacy.” This results from illegal access to, and possible misuse of, the entity’s premises, IT systems, or sensitive proprietary information, which might render the entity less able to pursue its institutional interests.

By identifying only the harms to material support as costs, we draw a clear line between those harms that can be monetized from those that cannot. Following Greenfield and Paoli (2013), we regard some harms—such as the harms to individuals’ dignity or harms to individuals’ and entities’ reputation and privacy—as inherently unquantifiable. We recognize that other interest dimensions, such as the functional integrity of an entity, can at least in principle and partially be measured through monetary indicators (e.g., stock exchange price), but realize that this data is not available for all entities nor is it possible to separate the impact on it of each single cybercrime. The clear distinction between costs and other harms gives us, as Greenfield and Paoli (2013: 874) argue, “the freedom of employing alternative means of analysis and formally incorporating qualitative insights; we do not, so to speak, leave any credible information on the table.” Hence, we give a full conceptualization of impact and avoid the opposed dangers of neglecting the harms that cannot be monetized and of embarking in wacky assumptions to monetize all harms.

Following Greenfield and Paoli (2013), we also set relevant bounds on our assessment. In particular, we exclude the costs incurred by public or private entities to protect themselves from crime. There are three reasons for this decision. First, in most cases public and private entities, do not assess the threat of each criminal activity separately, making it impossible to identify, let alone estimate, the costs of efforts to prevent each particular activity. Second, prevention costs are not solely a function of the inherent “toxicity” of crime itself, but are also a function of the perceptions of entities. A business, for example, might incur security expenses, for three reasons: an internal desire to hedge risks, the demand from employees and customers for particular protections, and government regulation mandating certain security measures (Jackson, Dixon & Greenfield, 2007: 34–35). Lastly, prevention costs are often bundled together with general compliance and technological systems, hence it would be very difficult to disentangle them empirically from the costs of these other activities (Levi & Burrows, 2008: 310).

Along the same lines, we exclude law enforcement costs. If we were to include them, the criminal activities that are already most heavily prioritized by law enforcement agencies – as reflected in the agencies’ funding and expenditures – would likely appear to be more harmful than other activities that have been less heavily prioritized. We do, however, consider remediation and replacement costs, such as the costs incurred by a business to respond to a cyber incident, or to repair and substitute assets damaged or stolen by criminals, including increases in insurance premiums that might result from repair or replacement.

4.2. Empirical Results

In this paragraph, we discuss the results of our empirical studies. First we discuss the results with regards to the Belgian citizens, continuing with the results with regards to the Belgian businesses. We conclude this paragraph with a discussion of the results with regards to the Belgian federal government¹.

4.2.1. Citizens

The results for Belgian citizens of 2017 are divided in a more descriptive section where victimization rates, protective behavior and the different costs of cybercrime are discussed and a more in depth analytical section where different typologies of internet users, their security-related behavior, the evolution between 2015 -2017 and the predictors of protective behavior (PMT) are included. The results of the first section are included in this final report. For the in-depth results of the first wave and for the more in-depth analysis of the other sections of the second wave we refer to D3.1.1 & D3.1.2, where all results are discussed in depth.

4.2.1.1. Victimization, security measures and costs of cybercrime of the general population

In a first section we aim to answer the first research question: “What is the state of the general Belgian population in terms of victimisation, security measures and costs of cybercrime?”

¹ As the project was aimed particularly at the Belgian federal government, we only focus on this body here.

• **Online activities: activities undertaken & activity security**

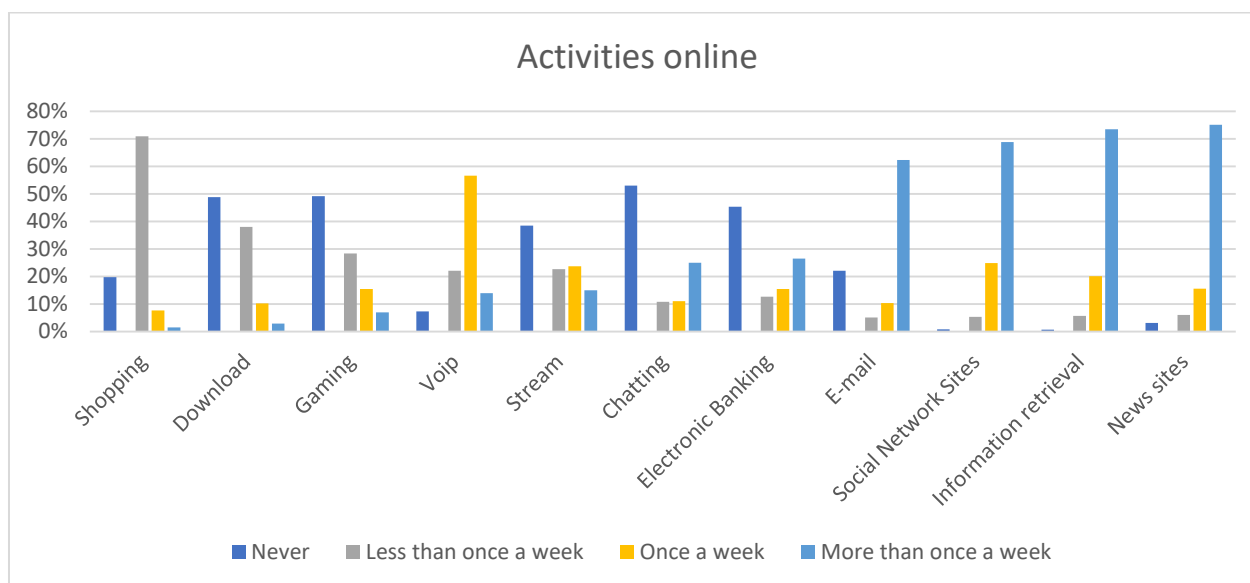


Table 1 Total sample: Online activities

Considering the activities one performs online, we see a big difference between the frequencies of these activities (see Table 1). In our sample, the respondents score the lowest on online shopping. Moreover, many activities we included in this study are (almost) never performed. (e.g. Chatting, gaming, downloading, electronic banking). Checking E-mails, activity on Social Network Sites and retrieving information or consulting news sites are the most popular.

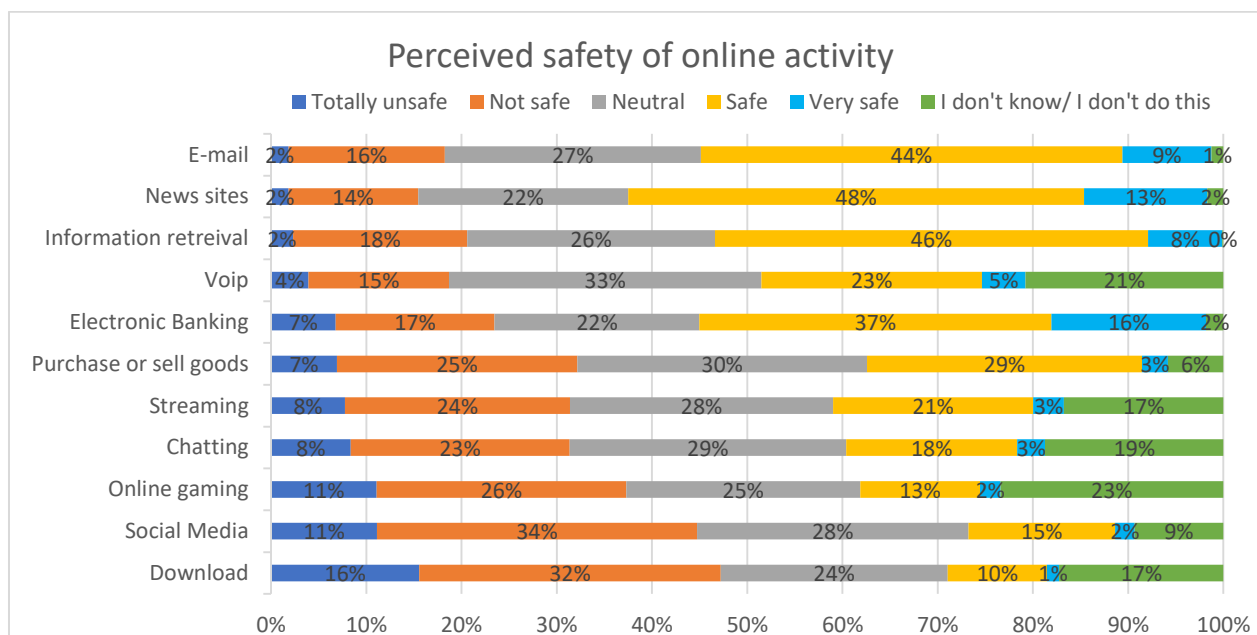


Table 2 Total sample: perceived security of online activities

If we take a look at the perceived security of a certain activity, we can conclude that downloading is seen as the least safe activity (with most people stating it is totally unsafe) followed by social media, online gaming, chatting and streaming (see table 2). Interestingly is

that for every activity at least 15% state that they find that activity “not safe” or less safe. In other words, every activity online is seen as somewhat unsafe by more than one in seven people. More than half (57.0%) of the people who do or at least know downloading, perceive it as “not safe” or less safe. Almost half of the people who use or at least know social network sites (49.3%) and online gaming (48.7%) also perceive it as “not safe” or less safe. Less than 20% of the population perceive Downloading, Social media or online gaming as “safe” or safer.

Furthermore, we can conclude that there is a big fraction of the population perceiving electronic banking (16.24%), visiting news sites (12.92%) and e-mail (9.35%) as very safe. It is also important to note that for some activities there is quite a big group of the respondents that didn't know or didn't perform the activity.

Less than 20% of the people perceive downloading, social media use or online games as at least safe

- ***Correlations between online activity and perceived safety***

After a two-tailed Spearman correlation between the perceived security of an activity and its frequency of use, we find that there are quite a few activities where this correlation is significant. Six of the activities have a significant correlation that is higher than .200 (see table 3). Hence, the higher their frequency of doing an online activity, the higher the perceived safety of that particular activity. Only for email and downloading this relation is not significant.

| Activity | Correlation coefficient | p |
|------------------------|-------------------------|------|
| Information retrieval | .077** | <.01 |
| News sites | .125** | <.01 |
| E-mail | .042 | .054 |
| Electronic Banking | .122** | <.01 |
| Online gaming | .356** | <.01 |
| Social Media | .266** | <.01 |
| Chatting | .308** | <.01 |
| VoIP | .274** | <.01 |
| Purchase or sell goods | .227** | <.01 |
| Download | .052 | .094 |
| Streaming | .287** | <.01 |

Table 3 Total sample: Correlations between online activity & perceived safety

This correlation could indicate opportunity costs as people who perceive a certain activity as less safe are performing this activity less often. Surprisingly this correlation is less strong for activities that are perceived safer like information retrieval, visiting news sites and electronic banking (cfr. Supra). Downloading and email, however, is not following this trend.

- **Security measures**

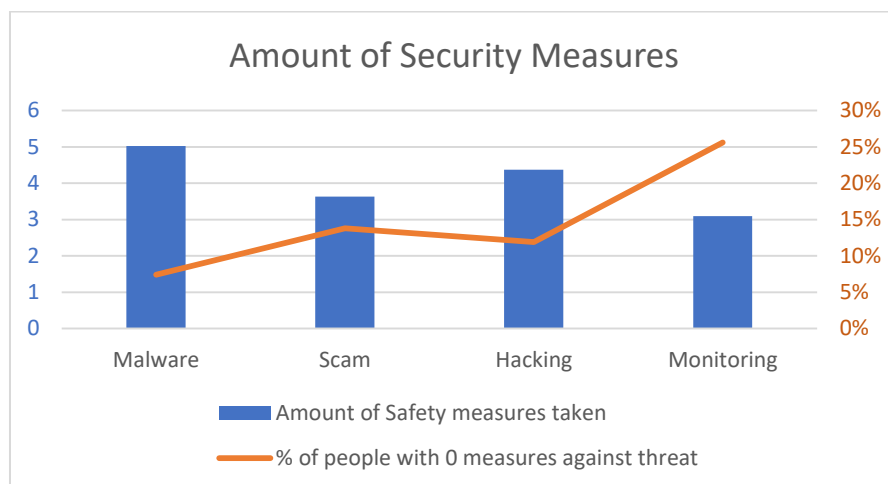


Table 4 Total sample: Amount of security measures taken

Analysing the number of security measures one takes we see that the most measures are taken against malware and hacking (see table 4). It is important to note that even with the lowest average amount of security measures being 3.09 security measures, there are for every cybercrime between 7.4% and 25.6% that do not implement any of the proposed measures as a security measure. This makes them especially vulnerable to cybercrime. Interestingly more than one in four people do not take any security measure against monitoring, they do however averagely use more than three security measures to protect themselves against monitoring.

More than one in four people does not take any security measures against monitoring

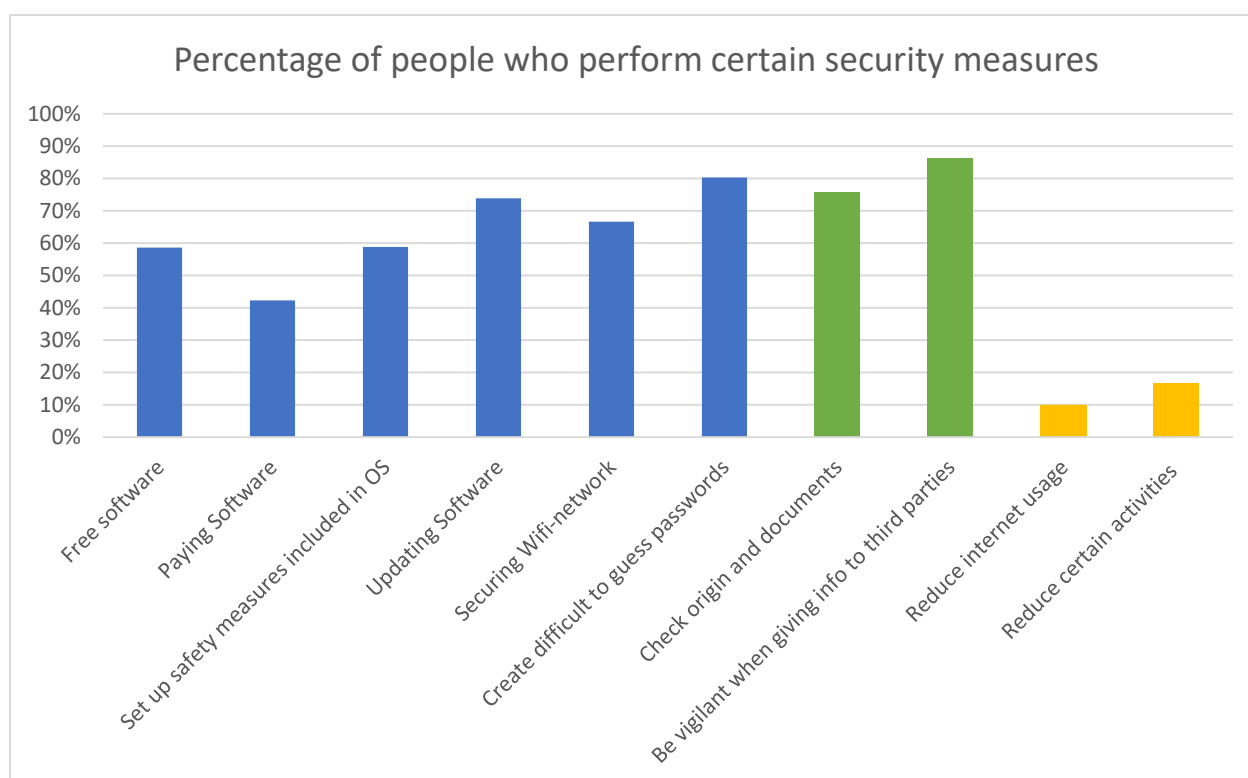


Table 5 Total sample: percentage of people who perform certain security measures

Almost 10% (9.7%) is reducing their internet usage and 16.5% is reducing or stopping certain activities online, these security measures are described as maladaptive and incorporate opportunity costs (yellow bars). In comparison with the other security measures this is much lower, but still more than one in ten Belgians are implementing a maladaptive security measure of any kind (see table 5).

More than one in ten people implement maladaptive security

Most people protect themselves by using social adaptive security measures such as checking the origin and documents before opening and being vigilant when giving info to third parties.

It is however impossible to know if these social securities measured (green bars) are applied in an effective way. This is dependent on the knowledge and skills of the person implementing these social adaptive security measures. If this is not the case, these social adaptive security measures will, of course, have no impact on the defence people have against cybercrime.

For every adaptive technical security measure (blue bars) - besides paying for software (42,3%) - the majority of people is using them. This means that less than 50% is willing to pay for their security measures. The recent trend of including security measures in operating systems for free is thus a good evolution and should continue.

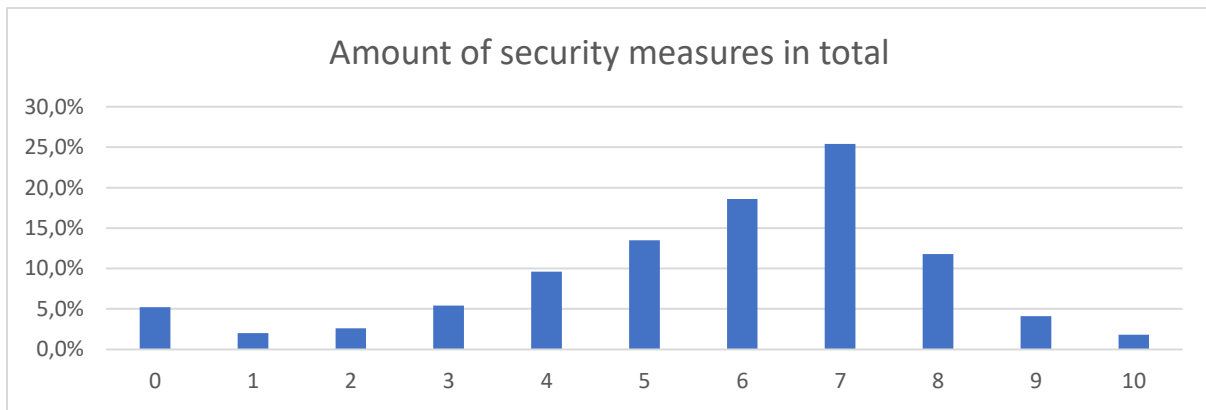


Table 6 Total sample: amount of security measures in total

With 84% of the people using four or more security measures and more than half using six or more security measures, most people are taking security seriously (see table 6). There are however still 5.2% of the people who take no security measures whatsoever and more than 10% implementing two or fewer security measures.

More than 5% of the people implements no security measures

- **Victimisation**

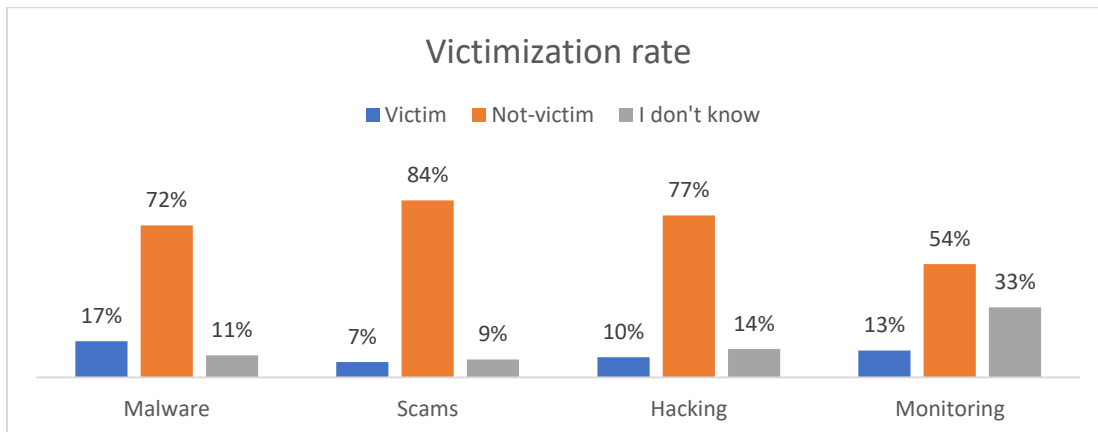


Table 7 Total sample: victimisation rate

With 17%, **malware** caused for the most victims the last 12 months (see table 7). People were least confronted with **scams**. The data also shows how most people are uncertain about **monitoring**. A total of 33% did not know if they were monitored or not by third parties.

Most victims were caused by malware in 2017

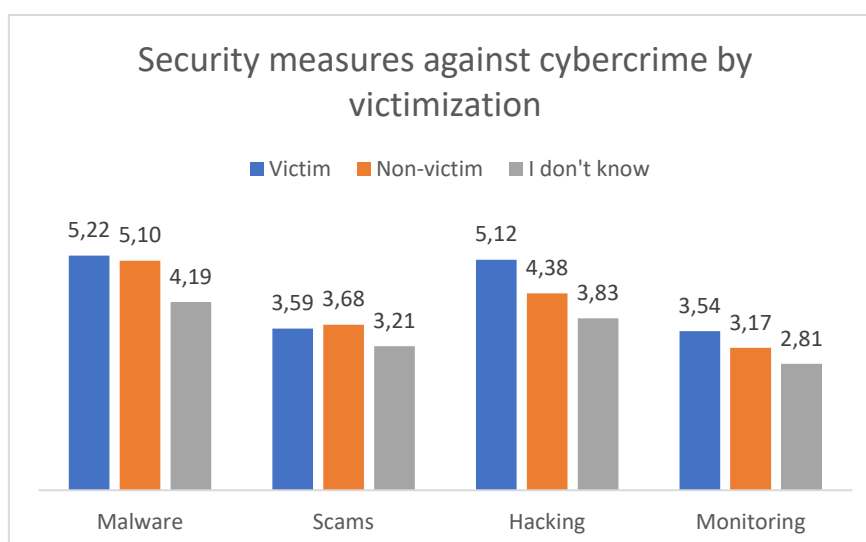


Table 8 Total sample: security measures taken against cybercrime by victimisation

A one-way Anova shows a difference between victims, non-victims and those who do not know if they are victimized by **Malware** considering their amount of security measures. ($F(2)=9.068$ $p<.001$) A post hoc analysis using Scheffe further indicates no significant difference between the victims and the non-victims. There is, however, a significant difference between the victims ($M=5.2215$ $SD=2.28135$) and the unknowing ($M=4.1884$ $SD=2.92571$) ($p<.01$) and the non-victims ($M=5.1025$ $SD=2.36944$) and the unknowing

Those who do not know if they were victimized implemented less security measures, this is true for three of four cybercrimes

($p<.001$) (see table 8).

There is no significant difference in security measures for **scams** between victims, non-victims and unknowing ($F(2)=1.769$, $p=.171$).

For **Hacking** there is a significant difference between all the groups ($F(2)=8.895$, $p<.001$) with the post hoc analysis using Scheffe showing that the victims are having significantly more security measures in place ($M=5.1239$ $SD=2.52641$) followed by the non-victims ($M=4.3752$ $SD=2.54037$) and then the unknowing ($M=3.8253$ $SD=2.59582$)².

For **monitoring** the one-way Anova with a post hoc using Scheffe also shows a significant difference between the victims ($M=3.5407$ $SD=2.66390$) and the unknowing ($M=2.8110$ $SD=2.57896$) ($p<.05$) ($F(2)=4.876$, $p<.01$), where the unknowing implement fewer security measures than the victims.

² Victims vs non-victims ($p<.05$), Victims vs unknowing ($p<.001$), non-victims vs unknowing ($p<.05$)

In three of the four cybercrimes the respondents who stated they didn't know if they were victimized implemented significantly fewer security measures than at least one other group. This makes this unaware group especially vulnerable.

- **Cybercrime Cost (RQ3)**

- Direct monetary cost³

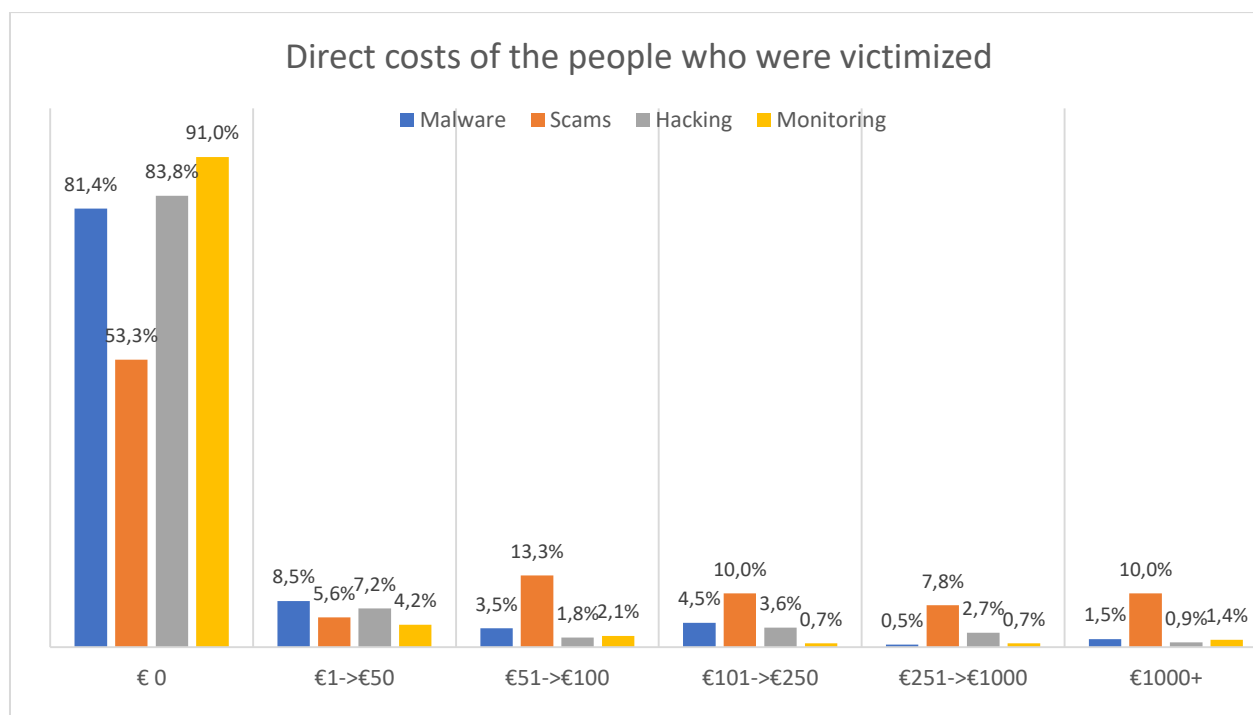


Table 9 Total sample: direct monetary costs by cybercrime

If we take a look at the monetary costs that are the direct consequence of a certain cybercrime, we can conclude that scams are the costliest of cybercrimes. More than 80% of the victims of malware, hacking or monitoring paid €0 as direct costs. 46.7% of the victims of scams, however, reported a direct cost of more than €0. 10% of the victims of scams even reported a loss of more than €1000. More than 25% of the victims of scams reported a loss of more than €100 (see table 9).

More than 80% of the victims of malware, hacking or monitoring paid €0 as a direct cost

³ Averages are not being reported because the amount of respondents that paid direct costs is too low, with only 37 for malware, only 42 for scams, 18 for hacking and 13 for monitoring and because some outliers would influence the average too much.

In comparison, just 18.6% of the victims of malware, 16.2% of the victims of hacking and 9% of the victims of monitoring reported a direct loss of any amount.

Of the victims of malware, only 6.5% stated a bigger loss than €100. Of the victims of hacking, this is 7.2%, of the victims of monitoring this is 2.8%.

- Direct non-monetary cost

No significant differences were found when comparing the sumscales (malware: $\alpha=.886$, scams: $\alpha=.915$, hacking: $\alpha=.872$, monitoring: $\alpha=.841$) of the harm against daily activities, privacy and reputation for malware (M=2.6783 SD=1.32443), scams (M=2.5991 SD=1.42012), hacking (M=2.8775 SD=1.41128) or monitoring (M=2.5809 SD=1.30074). This means that the harm done by a cybercrime is perceived equally harmful for the different cybercrimes.

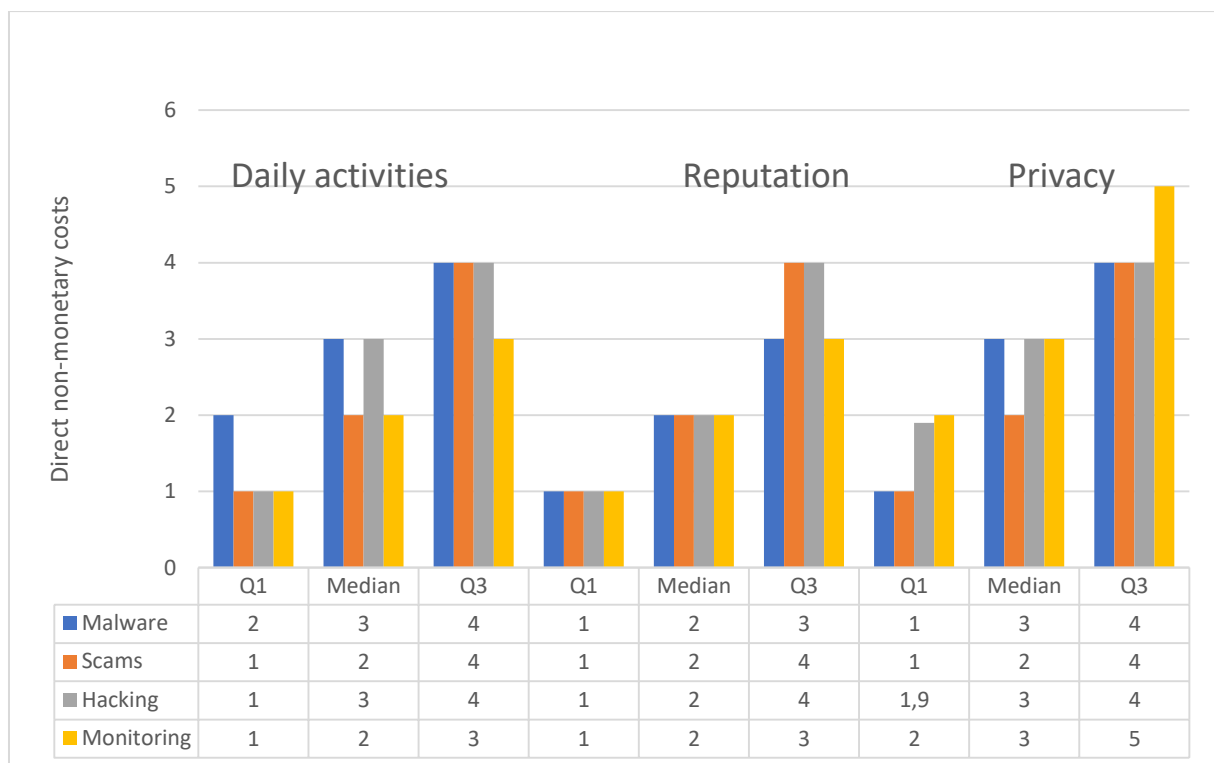


Table 10 Total sample: direct non-monetary cost by cybercrime (1=harmless, 2=insignificant, 3=moderate, 4=serious, 5=grave, 6=catastrophic)

More than 50% of the victims of malware and more than half of the victims of hacking state that their **daily activities** were moderately or more harmed by the cybercrime (see table 10). On the other hand just more than 25% of the victims of monitoring state that monitoring has moderately harmed or worse their daily activities. If we look at **reputation** we see for more than 25% of the victims of scams or hacking this incident was perceived as a considerably harmful or worse for their reputation.

50% of all but the victims of scams state that they perceived the harm to their **privacy** as moderate or higher. For more than 25% of the victims of monitoring, this was even

considered serious, for the other crimes more than 25% of the victims considered the incident as considerably harmful to their privacy.

- Opportunity cost

If we look at the direct questions about opportunity costs, 5.9% of the sample agrees that they reduced or stopped the use of electronic banking because of the threat of cybercrime. For online shopping, this is a higher 10.4% and for social network sites, this is 9%.

If we look at the maladaptive security measures, we can see that 9.7% of the sample is reducing or stopping internet use as a security measure, even 16.5% of the population reduce or stop certain activities online as a security measure.

The correlations between the perceived security of a certain activity and its frequency of use shows us that there is quite a big opportunity cost as electronic banking ($r=.122$, $p<.001$), social network sites ($r=.266$, $p<.001$) and purchasing goods online ($r=.227$, $p<.001$) have a significant correlation, this combined with the direct questions about these activities makes us believe that people experience opportunity costs for these activities. Furthermore other activities such as online gaming ($r=.356$, $p<.001$), chatting ($r=.308$, $p<.001$), VoIP ($r=.274$, $p<.001$) or streaming ($r=.287$, $p<.001$) have an even stronger relationship between their frequency and perceived security.

The combination of these three methods gives us the insight that there is quite a big opportunity cost that people experience as a result of cybercrime.

- Defense cost

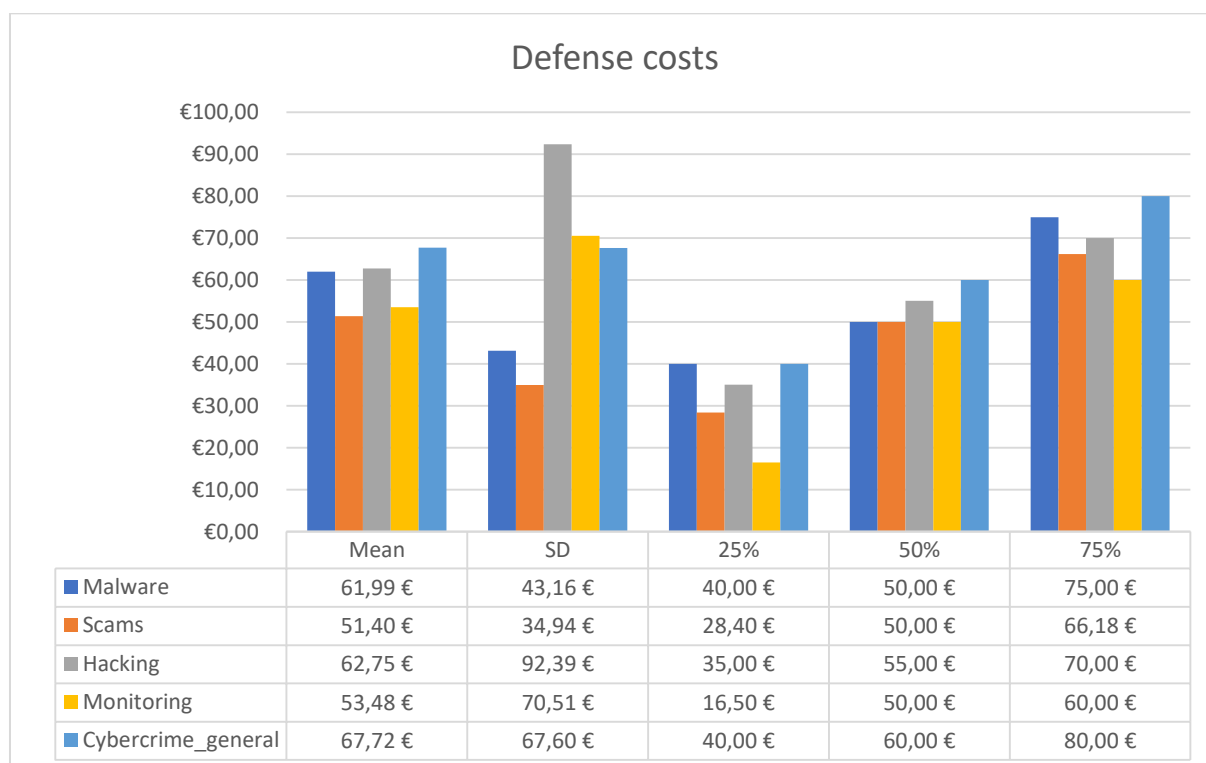




Table 11 Total sample: defence costs

If we compare the defence costs of the different cybercrimes we can see that malware (M=€61.99 SD=€43,16) and hacking (M=€62.75 SD=€92.39) are considered the most expensive (see table 11). Interestingly the median of all crimes is around €50. Which means that if someone pays for a defence against cybercrime, approximately half of them pay less than €50 and half of them pay more than €50, independent of the cybercrime. The costs of cybercrime in general are not much higher than the cost of the cybercrimes separately. It is likely that when people defend themselves against one crime, they also defend themselves against other crimes with this action.

4.2.1.2. Conclusion

In general, people are using the internet the most for information linked activities such as



 *Scams made the least victims but cause the highest direct financial costs* 

checking their emails, retrieving information, searching news websites and social networking.

There is a clear positive relationship between the frequency of the different activities one performs online and the perceived security of those activities. Furthermore, we can conclude that people develop different measures to protect themselves, not to say that these measures are adequate or effective. In general, most people were confronted with malware, followed by monitoring, hacking and then scams. Scams, however, caused for the highest direct financial cost linked to it.

Victims of hacking employ more security measures than non-victims. It is, however, difficult to know if they were victimized and as a result implemented more security measures or if they were victimized despite the security measures. Furthermore, it is important to conclude that in almost all cybercrimes the people who didn't know if they were victimized implemented fewer security measures compared to victims and non-victims.

Most victims do not experience direct costs as a consequence of an incident. Scams are the costliest of cybercrimes if it comes to direct costs. Almost half of the victims of scams state they've suffered direct monetary loss. Besides direct costs, there are many Belgian citizens who experience opportunity costs to some extent. These opportunity costs are felt in their online behaviour linked to the perceived safety of these activities but also in the maladaptive coping mechanisms implemented by more than one in ten people. Belgians spend most money defending themselves against malware and hacking. These are, however, not the

 *There are many Belgian citizens who experience opportunity costs* 

cybercrimes with the highest direct costs. They are not stacking costs for different cybercrimes as most people pay money just once to defend themselves against all cybercrimes.

4.2.2. Businesses

In this paragraph, we first present the results of our hygiene measurements and the cost model based on these measurements and the survey results. Secondly, we give a more detailed overview of the results of the two survey waves administered to Belgium based businesses.

4.2.2.1 Security State Assessment and Cost Modeling

Web Protection Mechanisms

As the web rapidly expands and gets deeply integrated into our society, it is important to ensure the security of web applications. While individual users can learn to avoid some web attacks through security awareness education, the main responsibility of offering web protection should rest on the shoulder of website owners.

In general, business owners have three main motivations to ensure their websites' security: (1) to defend critical data assets from attacks (an unprotected website might lead to severe data breaches); (2) to build trust with customers (a well-protected website makes its user feel being cared and concerned); and (3) to comply with legal requirements (some countries have strict data protection law, such as the General Data Protection Regulation (GDPR) in the European Union (European Parliament and the Council of the European Union, 2016), which requires websites to protect individuals' private data.

Web attacks are constantly evolving, and there are no silver bullets. To protect web applications, website owners can adopt a risk-based approach, i.e., to treat cyber-attacks as always-present risks and manage the risks properly. As part of their risk management, websites owners can implement known security mechanisms, and regularly assess their security posture. While this cannot completely avoid attacks, it minimizes attack surface and alleviates the consequences when attacks occur. Moreover, since some security mechanisms are visible from the client side, they provide reassurance to customers.

This section introduces several security mechanisms that websites owners can adopt to protect their web applications. While these security mechanisms are implemented by a web server, they require a client (conformant browser) to enforce it, thus they are referred as client-side security mechanisms/features in this report.

- **HTTPS Support**

HTTPS protocol is the standard solution for securing web traffic, which can thwart the eavesdropping and MITM attacks (Rescorla, 2000). It guarantees the confidentiality and integrity of web communications by adding the security capabilities of SSL/TLS to HTTP. The original SSL (Secure Sockets Layer) protocol was developed by Netscape for its Netscape Navigator browser in 1994. In 1996, Internet Engineering Task Force (IETF), an internet standards organization, took over the responsibility for the protocol. IETF later renamed SSL to TLS (Transport Layer Security) which was formally specified in Dierks and Allen (1999).

When a web application uses HTTPS, the connection between a web browser and a web server is secured by TLS. A message transmitted over HTTPS is encrypted and its integrity is validated with a message authentication code. In addition to the confidentiality and integrity, TLS can also authenticate the identity of the communicating parties by using public-key cryptography. In practice, HTTPS only provides website authenticity with the CA/B (Certificate Authority/Browser) trust model, and the user is authenticated with other mechanisms.

Since HTTP provides no security guarantees, website operators are strongly recommended to adopt HTTPS. While HTTPS has long existed as a standard solution, the adoption of it has been slow. Besides the performance overhead of SSL/TLS, the complexity of HTTPS deployment also deterred its adoption. However, these concerns have been largely addressed by recent improvements such as the support of HTTP/2 (Belshe & Peon, 2015) and the free SSL/TLS certificates provided by Let's Encrypt (www.letsencrypt.org/). And web browsers are holding non-secure sites more accountable, for example, Google Chrome (from version 56) displays a “Not Secure” warning for pages served over HTTP. These efforts have speeded up the HTTPS adoption in recent years. To correctly deploy HTTPS, web developers can follow the best practices recommended by OWASP ([www.owasp.org/index.php/Transport Layer Protection Cheat Sheet](http://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet)).

- HTTP Strict-Transport-Security

HTTP Strict Transport Security (HSTS; Hodges, Jackson & Barth, 2012) is a web security policy mechanism which helps websites to prevent SSL-stripping attacks (Marlinspike, 2009). The HSTS Policy is sent by the server to the browser via an HTTPS response header field named *Strict-Transport-Security*. It specifies a period of time during which the user's browser is instructed that all requests to that website need to be sent over HTTPS, regardless of what a user requests.

To implement an HSTS policy, a web server supplies a *Strict-Transport-Security* header over an HTTPS connection (HSTS headers sent over HTTP are ignored). The header sets a max-age (specified in seconds) during which a browser can only interact with the website by using secure HTTPS connections. For example, *Strict-Transport-Security: max-age=3600* instructs a browser to use only HTTPS for future requests for an hour (3600 seconds). The HSTS header can also specify an optional parameter *includeSubDomains* to include all of the site's subdomains as well.

When a conformant browser receives an HSTS header from a website, it will automatically turn any insecure HTTP links to that website into secure HTTPS links during the specified time frame. The browser will update the expiration time whenever it receives an HSTS header, so web applications can prevent the timeout from expiring by always sending HSTS headers. Additionally, modern browsers typically maintain an “HSTS preloaded list”, which is a list of known HSTS-enabled sites that are hardcoded into the browser as being HTTPS only. Google Chrome also offers an “HSTS Preload List Submission” service (<https://hstspreload.org>), which allows a website to use *preload* parameter in an HSTS header to submit itself to Chrome's “HSTS preloaded list”.

- Public Key Pinning and Certificate Transparency

Public Key Pinning and certificate transparency are two approaches that aim to address the issue of fraudulent SSL/TLS certificates used in MITM attacks.

Public Key Pinning allows websites to specify trusted public keys in an HTTP response header named *Public-Key-Pins* (Evans, Palmer & Sleevi, 2015). It tells a web browser to associate a set of specific cryptographic public keys with a certain website for a given time. During that validity time, the browser only accepts a server with one or more of those specified public keys. Thus, even if an attacker compromises a CA to forge a certificate, he cannot use the forged certificate to impersonate the website's server.

The idea of Public Key Pinning was originally started at Google in 2011, as an effort to protect its web services from MITM attacks (www.blog.chromium.org/2011/06/new-chromium-security-features-june.html). The approach was called static pinning, in which Google hardcoded some whitelisted public keys in Chrome. Google later expanded the idea into dynamic pinning, which was standardized as Public Key Pinning Extension for HTTP (HPKP) in 2015 [Evans et al. 2015]. However, it turned out that HPKP was difficult to implement and maintain (www.blog.qualys.com/ssllabs/2016/09/06/is-http-public-key-pinning-dead) and it can be abused by attackers (www.scotthelme.co.uk/using-security-features-to-do-bad-things/).

There are two main security issues with HPKP: HPKP Suicide and RansomPKP. HPKP Suicide refers to the situation where an HPKP-enabled website loses the pinned public keys. The keys might be accidentally deleted, or stolen in a hack incident. Consequently, browsers that have stored the site's HPKP policy will not be able to connect the site until the HPKP policy expires. The second issue, RansomPKP, happens in a web server breach scenario. When an attacker gains control of the server, he can set malicious HPKP headers such as pinning the attacker's keys. It will take a lot of time and effort for a website to recover if its HPKP is abused.

With these issues exist, and no support from other browsers (IE/Edge and Safari), Google Chrome plans to abandon HPKP in 2018 (www.groups.google.com/a/chromium.org/forum/#!msg/blink-dev/he9tr7p3rZ8/eNMwKPmUBAAJ), and turns to another approach called Certificate Transparency. Certificate Transparency (CT) (www.certificate-transparency.org/) is an open framework for monitoring and auditing SSL/TLS certificates in nearly real time. It requires certificate authorities to publish all issued certificates in public CT Logs. This allows quick detection of any mis-issued certificates.

A website can use an HTTP response header called *Expect-CT* to enforce Certificate Transparency. The *Expect-CT* header instructs a browser to expect a valid Signed Certificate Timestamps (SCTs) to be served when connecting to the website. By combining *Expect-CT* with active monitoring of CT logs, website operators can proactively detect fraudulent SSL/TLS certificates. Certificate Transparency and *Expect-CT* are still under the drafting process by IETF, and there is no support from other browsers as of October 2017. But starting from April 2018, Google Chrome will require Certificate Transparency for all newly issued, publicly trusted certificates.

Since Public Key Pinning (HPKP) is phasing out, and Certificate Transparency (CT) is proposed to achieve similar goals, these two approaches (HPKP/CT) are being treated as a single security feature in this report.

- HttpOnly and Secure Cookies

HttpOnly and Secure Cookies are cookies set with the *HttpOnly* and *Secure* attributes. These two flags can be used to protect session cookies and prevent session hijacking.

First introduced in Internet Explorer 6 SP1 in 2002, the *HttpOnly* attribute is designed to mitigate the risk of malicious client-side scripts accessing sensitive cookie values. Cookies are accessible to JavaScript code by default, which allows attackers to steal the cookies via an XSS attack. Using the *HttpOnly* attribute in a *Set-Cookie* header restrict the access of that cookie to the HTTP(S) protocol, making it inaccessible to client-side JavaScript (Barth, 2011).

The purpose of the *Secure* flag is to prevent cookies from being observed by unauthorised parties due to the transmission of a cookie in clear text. Although the traffic between a web server and a browser is encrypted when using HTTPS, the cookies stored in the browser are not, by default, limited to an HTTPS context. Thus, an active network attacker can intercept any outbound HTTP request from the browser and redirect that request to the same website over HTTP in order to reveal the cookies (Barth, 2011). By setting the *Secure* attribute, the scope of a cookie is limited to secure channels, thus *stopping* browsers from sending cookies over unencrypted HTTP requests.

The *HttpOnly* and *Secure* attributes are set via a *Set-Cookie* HTTP response header. For example, this header *Set-Cookie: OSID=5wRhE...; path=/; domain=mail.google.com; Secure; HttpOnly* sets a cookie named *OSID* with both flags enabled. A browser records this information as part of cookie data in its storage system, as shown in figure 1.

Figure 1. Example of HttpOnly and Secure Cookies stored in a browser

| Storage | Name | Value | Domain | Path | Expires... | Size | HTTP | Secure |
|-------------------------|---------|-------|----------------|------|------------|------|------|--------|
| ▶ Local Storage | HSID | AJ... | .google.com | / | 2019-0... | 21 | ✓ | |
| ▶ Session Storage | SSID | A6... | .google.com | / | 2019-0... | 21 | ✓ | ✓ |
| IndexedDB | SID | PA... | .google.com | / | 2027-1... | 74 | | |
| Web SQL | SAPI... | H-... | .google.com | / | 2019-0... | 41 | | ✓ |
| ▼ Cookies | OTZ | 41... | plus.google... | / | 2017-1... | 33 | | ✓ |
| https://mail.google.com | OSID | 5w... | mail.google... | / | 2019-0... | 75 | ✓ | ✓ |
| | NID | 11... | .google.com | / | 2018-0... | 278 | ✓ | |

- Content Type Options

When a web server sends a resource to a browser, it can use the *Content-Type* header to indicate the media type of the resource. The content type is specified as a MIME (Multipurpose Internet Mail Extensions) type, which is a way to identify different Internet resources. If a server does not provide the *Content-Type* header or the specified MIME type is ambiguous, some browsers such as Internet Explorer will use a detection algorithm to determine the content type, which is called MIME sniffing. However, this MIME-sniffing

feature can be abused by attackers to disguises a particular file type as something else, which might give them the opportunity to perform cross-site scripting attacks.

In order to disable MIME sniffing, thus reducing exposure to attacks, Microsoft introduced the *X-Content-Type-Options* (XCTO) header (www.blogs.msdn.microsoft.com/ie/2008/07/02/ie8-security-part-v-comprehensive-protection/). A website can send this header with “nosniff” value (*X-Content-Type-Options: nosniff*) to tell a browser not to sniff MIME type and instead follow the value specified in the Content-Type header. The *X-Content-Type-Options* header is supported by most browsers including Chrome, Firefox, IE/Edge.

- Content Security Policy

Content Security Policy (CSP; West, Barth & Veditz, 2016) is a security policy that helps to mitigate several types of attacks, including cross-site scripting (XSS), clickjacking and data injection attacks. CSP provides a standard method for website owners to declare approved origins of content that browsers should be allowed to load on that website. It can be used to cover many different type of web resources, such as JavaScript, CSS, images, HTML frames, audio and video files, and other embeddable objects.

CSP was originally proposed and implemented by Mozilla Firefox in 2010 (Stamm, Sterne & Markham, 2010), in order to help websites to prevent XSS attacks. It was quickly adopted by other web browsers and has been published as a W3C recommendation in 2014 (West et al., 2016). As of 2017, new version of CSP is being developed under W3C to include more features (West, 2016).

To enable CSP, a web server can send the *Content-Security-Policy* header. Alternatively, a CSP policy can also be specified in a <meta> element. The primary use of CSP is to mitigate XSS attacks. To achieve this goal, a website can send a CSP header that looks like listing 1.

Listing 1. Preventing XSS with a CSP policy

```
Content-Security-Policy: default-src 'self'; img-src *; \
script-src trusted.example.com;
```

In the above example, the policy specifies that 1) the default trusted origin is the website itself (via *default-src* directive); 2) images can be loaded from anywhere (via *img-src* directive); 3) executable script is only allowed from trusted.example.com (via *script-src* directive). Hence, whenever a requested resource originates from a source that is not defined in the CSP, it will simply not be loaded. For example, even if an attacker is able to inject malicious JavaScript in the webpage, the injected code will not be executed, as it is not from the specified trusted origin.

With more than 20 different directives, CSP is very versatile and flexible. Besides specifying trusted origin for various content types, a website can also use CSP to guarantee secure communication. For example, the *upgrade-insecure-requests* directive instructs a browser to upgrade HTTP links to HTTPS links; the *block-all-mixed-content* directive prevents loading HTTP-served content in an HTTPS page.

- X-Frame-Options

X-Frame-Options (XFO; Ross & Gondrom, 2013) is an HTTP response header designed to mitigate Clickjacking attacks. In a Clickjacking attack, the attacker redresses the user interface of website A with transparent layers, and then trick the user into clicking on a button on an embed page from website B when they were intending to click on the same place of the overlaying page from website A.

To stop Clickjacking attacks, a website can use the *X-Frame-Options* header to tell a browser whether a certain page is allowed to be embedded in a frame. There are three possible directives for this header: *DENY*, *SAMEORIGIN*, and *ALLOW-FROM*. If the header is set to *DENY*, then the browser will prevent the page from rendering when embedded within a frame. On the other hand, if *SAMEORIGIN* directive is specified, then the page is only allowed to be embedded in other pages from the same domain. The *ALLOW-FROM* directive is used to specify a trusted origin that can embed the page.

The function of *X-Frame-Options* has been integrated in the CSP version 2 (West et al., 2016) with the *frame-ancestors* directive. Thus, a website can also use CSP to prevent clickjacking attacks. Setting *frame-ancestors: none* in CSP has the same effect as *X-Frame-Options: DENY*. And *frame-ancestors: self* is similar to *X-Frame-Options: SAMEORIGIN*.

Large-scale Web Crawling Approach

To assess a website's security, a conventional approach is actively searching for vulnerabilities. This typically requires internal penetration testing and source code reviewing, hence it is time and labour consuming. Many small and medium-sized enterprises (SMEs) do not have the incentive and resources to conduct such an assessment. While there also exists automated external active scanning for weaknesses, it is often intrusive and has ethical issues.

This research used an alternative approach to analyse web application security. Instead of looking for vulnerabilities, an assessor can check the presence of defence mechanisms. To defend against attackers, website operators can utilize a wide range of defence mechanisms, both at the server-side, as well as the client-side of their web applications. From a security-metrics standpoint, the presence or absence of these mechanisms can be used as a security indicator of any given website. In particular, this approach focuses on the discovery of client-side security mechanisms (as described earlier). By adopting those client-side security mechanisms, a large number of security issues encountered by businesses can be remedied, or at least vastly reduced.

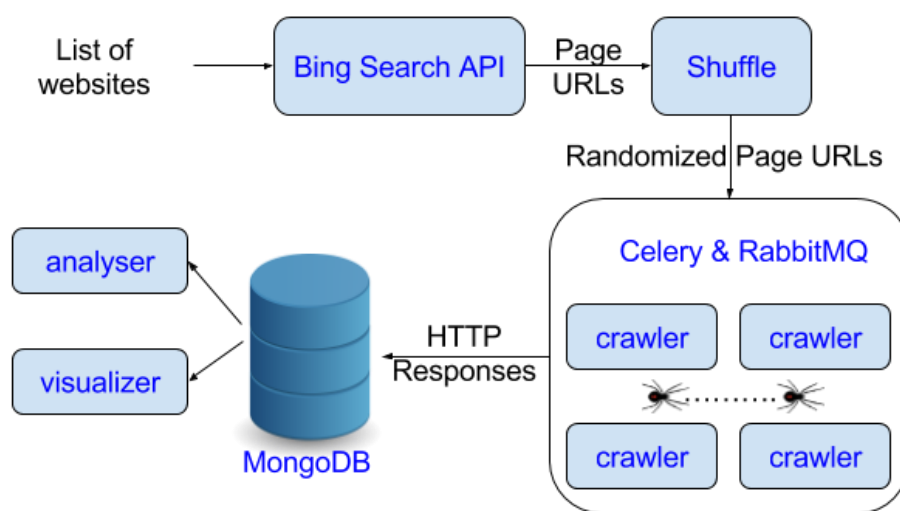
Assessing websites security through defensive security feature analysis has two main advantages:

1. Non-intrusiveness: since client-side security mechanisms can be detected from client side, the assessment can be carried out simply by visiting webpages in a browser, which does not cause any harm to the assessed website.

2. Automated efficiency: with a customized web crawler that mimics a normal browser's behaviour, the analysis process can be automated. This automation brings efficiency to the assessment.

This non-intrusive and automated approach can be applied on a large scale to assess the security of a large number of websites belonging to a country, or a specific industry sector. The steps of the web crawling approach are illustrated in figure 2. Using this approach, we could crawl 1 million webpages within 2 days, with 50 networked machines.

Figure 2. Large-scale web crawling approach



We began with a set of websites to be assessed. Since the analysis was based on the security features that can be found in webpages, we first needed to find enough webpages for each given website. To achieve this, Bing Web Search API (www.azure.microsoft.com/en-us/services/cognitive-services/bing-web-search-api/) was used to obtain popular webpages from a domain. The popular webpages found by Bing Search is a good representative of a website, as people typically enters a website through search engines. The presence or absence of defensive mechanisms on these popular webpages can largely reflect the website's security.

More specifically, we used the *site:domain* operator with Bing Web Search API to obtain a set of popular page URLs for a domain. For instance, a single search for *site:facebook.com* in Bing would return a set of 50 webpages belonging to *facebook.com*. Ideally, we got as many pages as possible for a website, since a larger sample size would be more representative. However, modern websites often serve dynamic pages, generating webpages based on the parameters in URL, which results some very correlated page URLs. For example, although <http://example.com?id=1> and <http://example.com?id=2> are different, they are produced by the same sever-side logic, thus having the same security features. In other words, the representativeness is not fully determined by the size of URLs set.

In our experiment, we typically obtained up to 200 page urls for a website, in order to have a reasonable representative sample size. Optionally, one can measure the similarity between URLs to filter out correlated URLs, which can reduce the sample size yet retain the same level of representativeness, making the lateral crawling phase faster.

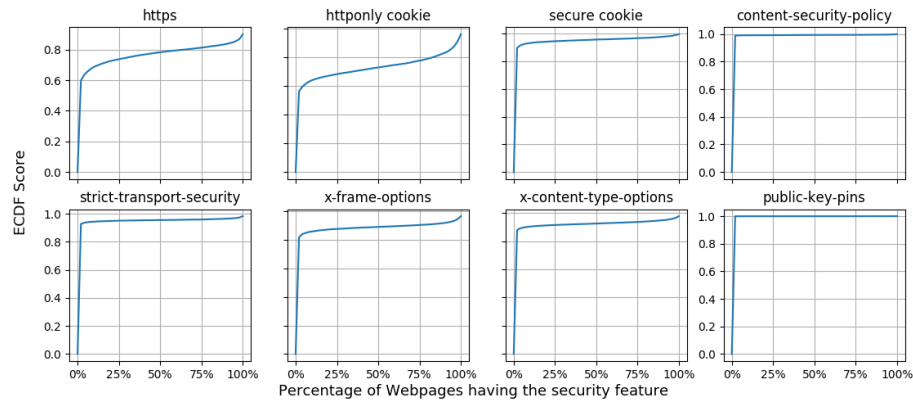
After page URLs of all websites were obtained, the pages were visited with a crawler. To avoid hurting the performance of websites, the URLs of all websites were randomly shuffled before feeding to the crawlers. The crawlers were built on top of a headless scriptable browser, such as HtmlUnit (www.htmlunit.sourceforge.net/) and PhantomJS (www.phantomjs.org/). By loading webpages in a headless browser with an appropriately set user-agent, we mimicked the behaviour of a regular user visiting a website with a normal browser.

To efficiently crawl millions of webpages within a reasonable period of time, we distributed the work across multiple threads or machines. Celery (www.celeryproject.org/), a Python library, was used to manage such a distributed task queue, where it uses a broker such as RabbitMQ (www.rabbitmq.com) to accept crawling tasks. A crawling task is simply using a crawler to visit a webpage, and receive HTTP responses. The results obtained by crawlers were all stored into a database (MongoDB; www.mongodb.com/), which could be accessed by an analyser program for data processing or a visualizer program for data visualization.

Web Security Scoring

In order to compare the security level among different websites, and among countries and businesses verticals, we developed a web security scoring system that gives quantitative scores for each website. The proposed scoring system was built upon the assessment of defensive security features introduced in the previous sections.

For each security feature, we first computed an empirical cumulative distribution function (ECDF) for all EU websites. The ECDF was computed based on the percentage of webpages having that feature on a particular website, as shown in figure 3. The ECDF score reflected how well a website was doing compared to websites in the EU dataset. For instance, if a website had a score 0.61 for the feature HTTPS, it means the website outperformed 61% of the websites in the EU dataset (i.e. by having a higher percentage of pages over HTTPS). Websites with no pages found to have a security feature were given a zero ECDF score for that feature.

Figure 3. ECDFs for each security feature

By applying the ECDFs to each website and each feature, we obtained eight security features scores per website. In our study, we grouped these features into three categories:

- **Category 1: Secure Communication.** This category included four features that contributed to secure communication between a server and a browser: HTTPS support, Secure Cookies, HTTP Strict Transport Security (HSTS), and Public Key Pinning or Certificate Transparency (HPKP/CT).
- **Category 2: XSS Mitigation.** This category included three features that can be used to mitigate XSS attacks: HTTPOnly Cookies, X-Content-Type-Options (XCTO), and Content Security Policy (CSP).
- **Category 3: Secure Framing.** This category had one feature, i.e., X-Frame-Options (XFO) to enable secure framing.

For each category, we calculated a weighted security score. The weight given to each feature reflected the relative importance and maturity of the feature in each category. The more fundamental and matured feature got relatively higher weights. In particular, the following weights were used to calculate the three subscores:

- **Secure Communication Score:** this subscore was measured by applying a weighted average of the HTTPS, HSTS, Secure Cookies and HPKP/CT usage.

$$\begin{aligned} \text{SecureCommunicationScore} &= \frac{45}{100} \times \text{HTTPS} + \frac{25}{100} \times \text{SecureCookies} + \frac{20}{100} \times \text{HSTS} + \frac{10}{100} \times \text{HPKP} \end{aligned}$$

- **XSS Mitigation Score:** this subscore was measured by applying a weighted average of the HttpOnly Cookies, XCTO, and CSP usage.

$$\text{XSSMitigationScore} = \frac{50}{100} \times \text{HttpOnlyCookies} + \frac{30}{100} \times \text{XCTO} + \frac{20}{100} \times \text{CSP}$$

- **Secure Framing Score:** this subscore was measured by the XFO usage.

$$\text{SecureFraming} = \frac{100}{100} \times \text{XFO}$$

And then for each (group of) website(s), we defined an overall security score (*OverallScore*) as a weighted average of these three scores:

$$\text{OverallScore} = \frac{40}{100} \times \text{SecureCommunicationScore} + \frac{40}{100} \times \text{XSSMitigationScore} + \frac{20}{100} \times \text{SecureFramingScore}$$

Longitudinal Study of Web Security

This section gives an overview of the adoption of client-side security mechanisms on the web, and provide a state-of-practice reference model of web security for website operators. To achieve this, we crawled more than 18,000 European websites in a four-year period. With the gathered data, we analysed the evolution of the usage of client-side security mechanisms, and used a security scoring system to compare a website to its peers (based on business vertical or popularity), in order to provide a web security baseline for website operators.

To study the security posture of the European web, the popular websites from the 28 member states in the EU were chosen to represent the European web. For each EU country, we selected the top 1,000 websites ending with the corresponding ccTLD (country code top-level domain) from Alexa's list of the top 1 million sites (www.s3.amazonaws.com/alexastatic/top-1m.csv.zip). As a result, we obtained a set of 23,050 European websites.

We then used the crawling approach to collect data from these websites in a four-year's timeframe. We removed the websites with less than 50 successfully crawled pages from our dataset. As a result, we obtained a dataset of 20,157 websites in 2013, 18,074 websites in 2015, and 14,984 websites in 2017, as shown in table 12. The number of websites decreased over time because some websites disappeared and some websites changed domain names.

Table 12 Overview of European web dataset for longitudinal study

| Time | # of sites | # of pages | avg. # of pages/site |
|------------|------------|------------|----------------------|
| Sept. 2013 | 20,147 | 3,499,080 | 174 |
| Sept. 2015 | 18,074 | 2,992,395 | 166 |
| Sept. 2017 | 14,984 | 2,266,338 | 151 |

Table 13 gives an overview on the use of security features on the European web over four years. It clearly illustrates that the web security on the European web did improve, as each of the security features had been adopted in 2017 by a larger fraction of websites than in 2013. One can also observe that the pace of improvement accelerated over time; in the last two years security features were adopted much faster.

Table 13. Overview of the use of security features on the European web

| Security feature | % of websites | | |
|------------------|---------------|------------|------------|
| | Sept. 2013 | Sept. 2015 | Sept. 2017 |
| HTTPS Support | 22.96% | 33.29% | 71.97% |
| Secure Cookies | 5.86% | 7.56% | 25.01% |
| HSTS | 0.49% | 4.30% | 19.82% |
| HttpOnly Cookies | 36.52% | 43.86% | 54.89% |
| XCTO | 2.24% | 6.82% | 24.43% |
| CSP | 0.05% | 0.43% | 5.71% |
| XFO | 4.80% | 14.93% | 32.08% |

We then assessed the extent to which the security of a particular website did improve over time, by measuring for each website if it adopted more security features over time or not. Since none of the websites had all seven security features enabled in 2013, there was space for improvement for all the websites.

By doing this, we found that more websites improved from 2015 to 2017 than between 2013 and 2015. There were 8,685 websites that adopted more security features by 2017 than by 2015, while the number of improved websites from 2013 to 2015 was 5,756. And by 2017, there were 377 websites that had all seven security features enabled.

- Websites that adopted more security features

In this section, we investigate the relationship between the adoption of security features in a website and its popularity (measured by its Alexa global rank, www.s3.amazonaws.com/alexastatic/top-1m.csv.zip) and sector (derived from McAfee's TrustedSource Web Database, www.trustedsource.org/en/feedback/url). We expected that higher ranked popular website and websites belonging to critical sectors such as finance and online shopping, had more incentive to adopt security features in order to protect their asset, compared to the less-known or less- valuable websites.

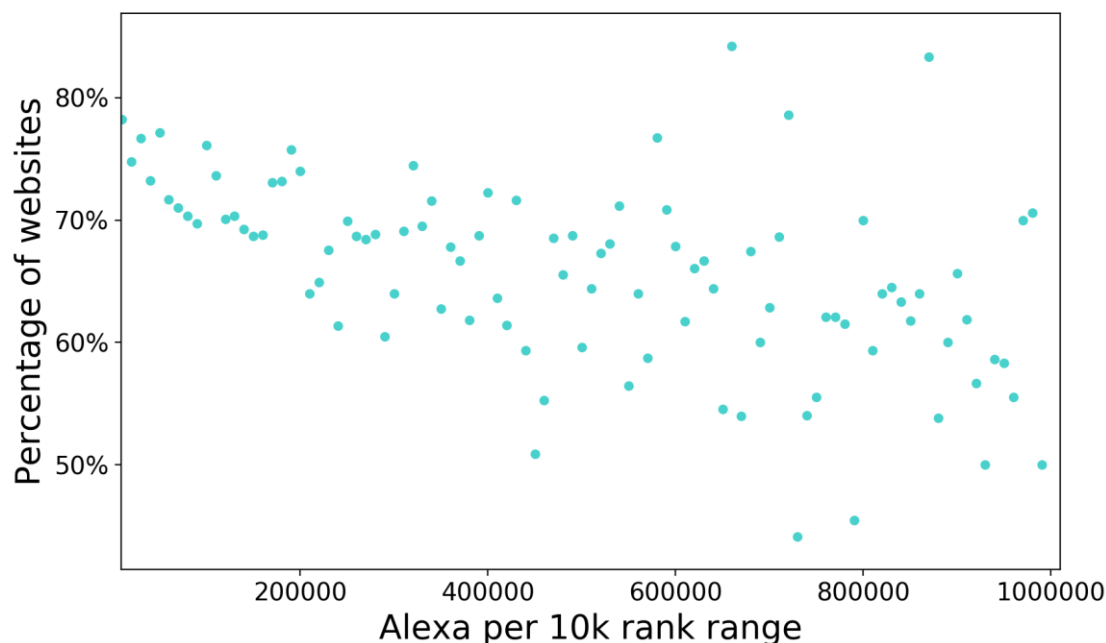
To confirm this hypothesis, we first used Point-biserial correlation to study the correlation between the adoption of security features in a website and its Alexa rank. We compared the three datasets in pairs to study the websites that adopted more security features over different time periods. As shown in table 14, all the correlation coefficients were negative, with p-value less than 5% (hence a negative correlation). It confirmed our hypothesis that higher ranked websites tend to adopt more security features.

Table 14. Correlation between the adoption of security features in a website and its Alexa rank

| datasets | coefficient | p-value |
|--------------|-------------|-----------------------|
| 2013 vs 2015 | -0.076 | 3.1×10^{-29} |
| 2015 vs 2017 | -0.089 | 7.4×10^{-27} |
| 2013 vs 2017 | -0.098 | 3.2×10^{-32} |

To better illustrate this correlation, per 10,000 Alexa ranks, we calculated the percentage of websites belonging to that rank range, which adopted more security features in 2017 versus 2013. As shown in figure 4, we can observe a downtrend for the percentage of websites that adopted more security features over the Alexa ranks.

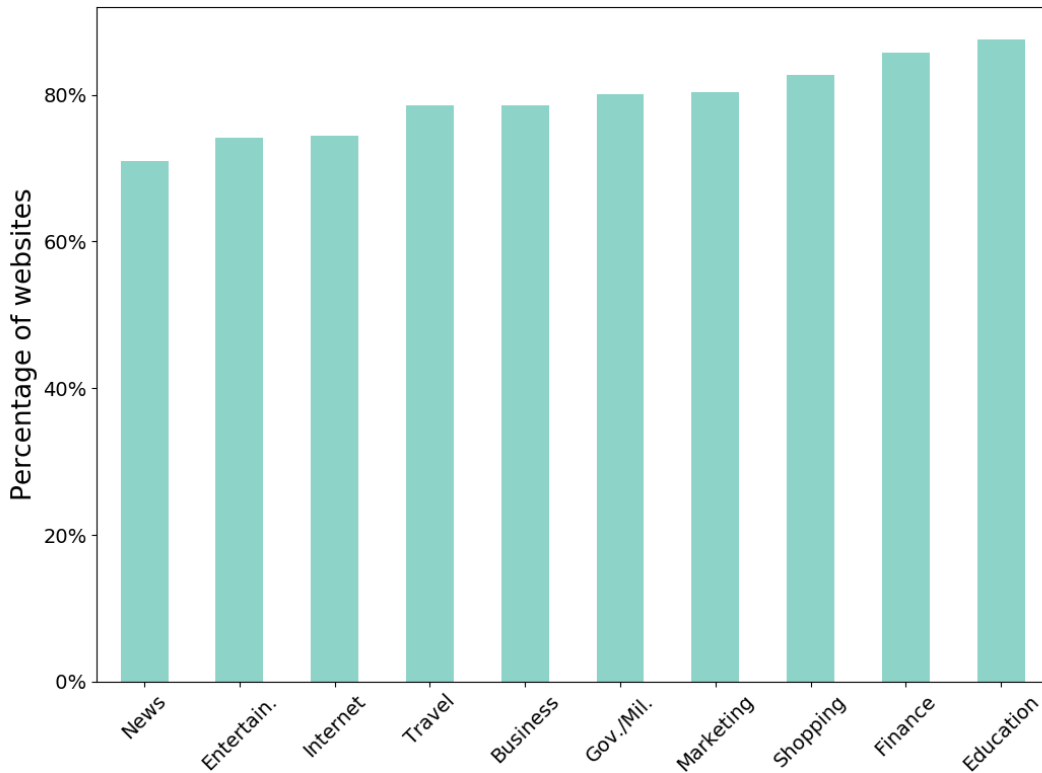
Figure 4. Percentage of websites that adopted more security features in 2017 versus 2013, plotted per 10k Alexa ranks



As for the relationship between the adoption of security features in a website and its sector, we calculated the percentage of websites that adopted more security features in each sector.

Figure 5 shows the top 10 sectors that had larger percentages of websites adopting more security features over time. It comes as no surprise that Education and Finance were the best two performing categories. Since educational and financial organizations handle a lot sensitive personal data (students' profiles, financial transactions), they have more incentives to adopt security features for protection. In addition, among the 377 websites that had all seven security features enabled in 2017, 72 sites were from the Education sector, accounting for 10% educational websites, and 63 sites were from the Finance sector, accounting for 11% financial websites.

Figure 5. Percentage of websites that adopted more security features in 2017 versus 2013, grouped per business vertical



- EU Web Security Score, in terms of website popularity

To assess the web security score in terms of website popularity, the websites were grouped per 10,000 Alexa ranks, and the average score was calculated for websites that belonged to that rank range. Figure 6 shows the average *OverallScore* for per 10k Alexa ranks.

Figure 6. Average overall security score for per 10k Alexa ranks

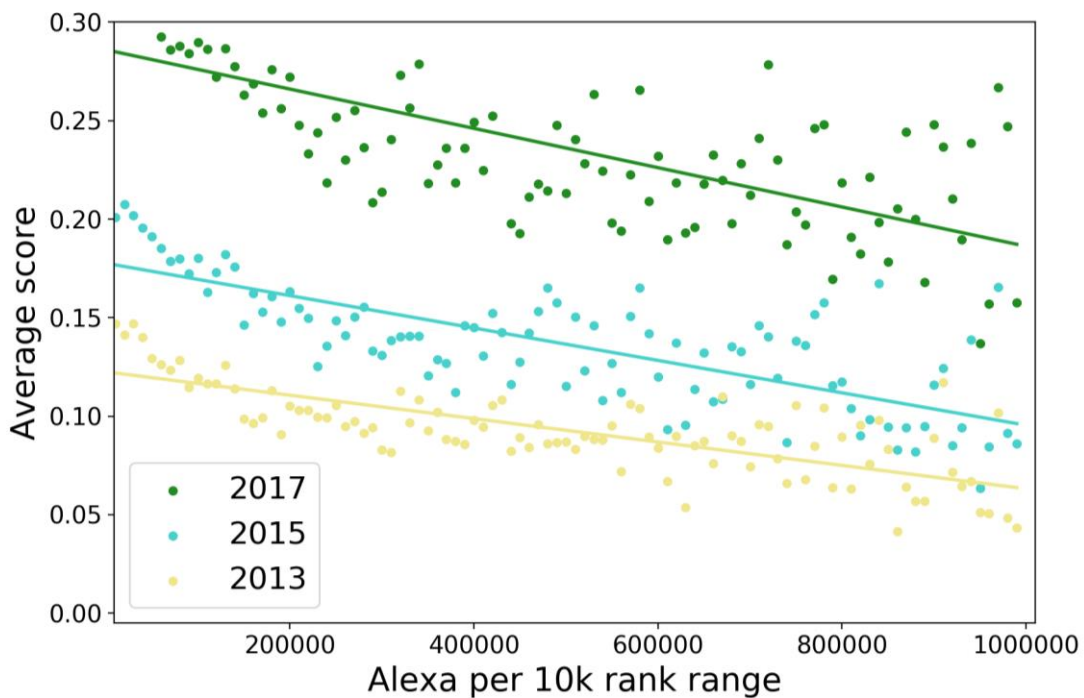


Figure 6 indicates that higher ranked websites tend to have higher security scores. To confirm this assumption, Spearman's rank correlation coefficient was used to assert the correlation between the *OverallScore* in a website and its Alexa rank (as listed in table 15).

Table 15. Correlation between the security score of a website and its Alexa rank

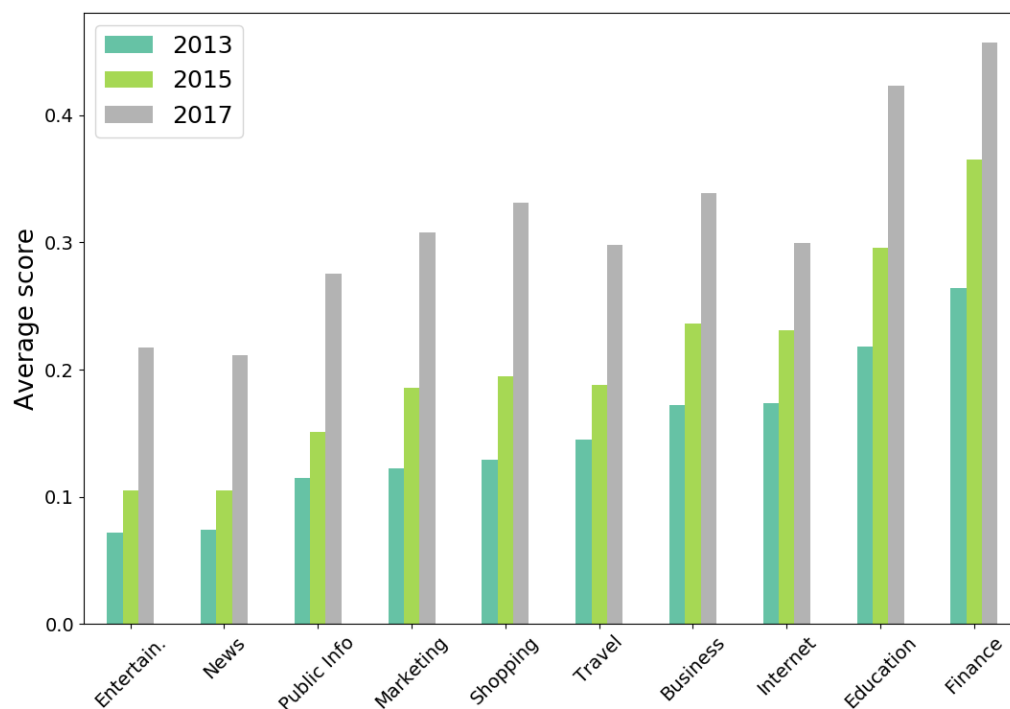
| datasets | coefficient | p-value |
|------------|-------------|------------------------|
| Sept. 2017 | -0.18 | 1.1×10^{-108} |
| Sept. 2015 | -0.15 | 2.9×10^{-86} |
| Sept. 2013 | -0.14 | 5.4×10^{-95} |

As expected, there was a negative correlation between the *OverallScore* in a website and its Alexa rank (see table 15), and this correlation held for all three sub scores. This correlation is consistent with the correlation that higher ranked websites tend to adopt more security features, as discussed earlier.

- Web Security Score per business vertical in EU

In this section, we compare the security evolution of the websites per business vertical. For the ten most popular business vertical, the average score was calculated for websites that belonged to that business vertical. Figure 7 shows the average *OverallScore* for ten business verticals, sorted by their 2013 security score, to easily identify business verticals that got better than their adjacent peers.

Figure 7. Average overall security score for each business vertical



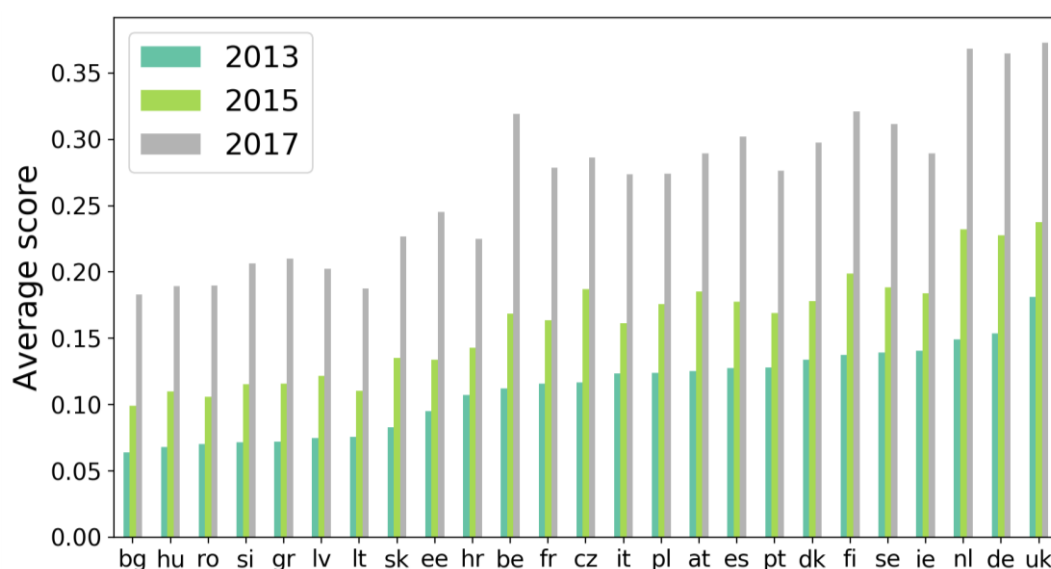
The *Education* and *Finance* verticals are the two best performing categories, which is consistent with the finding that educational and financial organizations tend to adopt more security features (as shown in figure 7). In addition, we observe that the *Business*, *Shopping*,

and Marketing sectors improved a lot and eventually caught up their neighbours. This improvement might have been driven by the fast growth of E-commerce in recent years (www.economist.com/node/21730546). As more companies expand their business online, and more people choose online shopping, websites from these sectors are incentivized to provide better web protection.

- Web Security Score per country in EU

In this section, we compare the security evolution of the websites per country. For each EU country, the average score was calculated for websites that belonged to that country. Figure 8 shows the average *OverallScore* for 25 EU countries. Cyprus(.cy), Malta(.mt) and Luxemburg(.lu) were removed from the dataset, as the number of websites in these countries were less than 100. The countries in Figure 8 are sorted by their 2013 security score, to easily identify countries that got better than their adjacent peers.

Figure 8. Average overall security score for each EU country



One can easily observe that the Netherlands (.nl), Germany (.de) and the United Kingdom (.uk) stayed ahead over the past few years. Others' positions fluctuated a bit, but there were no big changes, except for Belgium (.be), which improved exponentially between 2015 and 2017, making it the fourth best EU country in terms of web security performance.

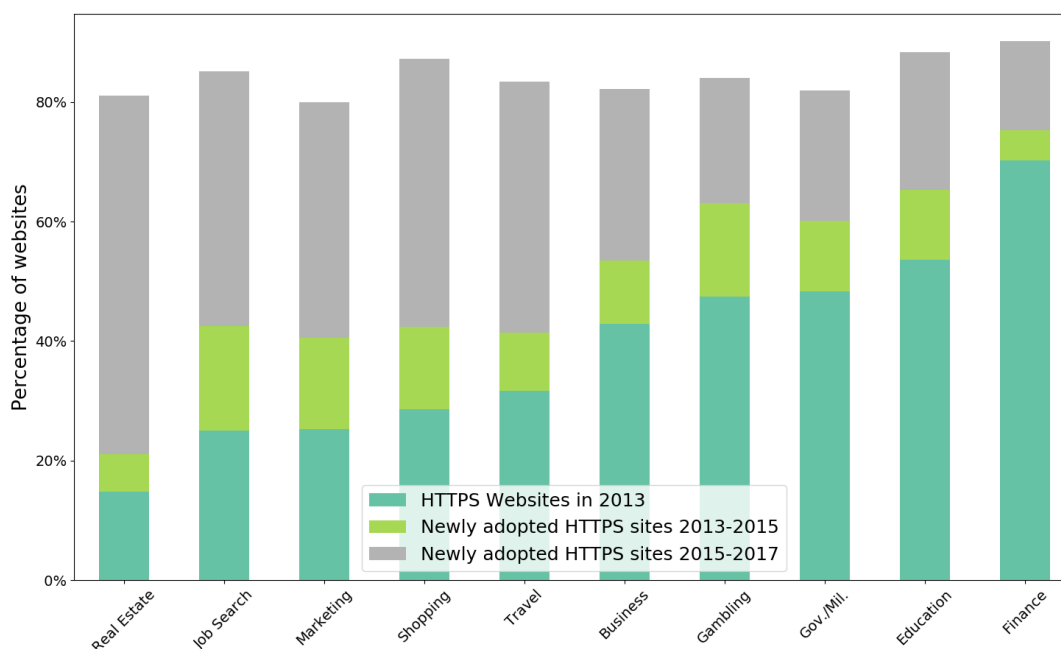
- HTTPS Migration Analysis

HTTPS is the standard solution for securing web traffic nowadays. Although it increases performance overhead and operating costs, the security benefits it brings outweigh these disadvantages. As previously shown in table 13, more than 70% of websites had enabled HTTPS support as of September 2017. In this section, we investigate the websites that had adopted HTTPS since 2013. We call these websites the newly adopted HTTPS sites.

To understand the types of newly adopted HTTPS sites, we plot the top 10 sectors that have the most percentage of websites with HTTPS support in figure 9. One can see that *Finance* and *Education* sectors were the first movers of HTTPS adoption, with more than 50% of websites having HTTPS support in 2013. They remained the best two verticals over years,

but other sectors caught up by 2017. In particular, between 2015 and 2017 there was a substantial improvement of HTTPS adoption in other sectors such as *Shopping* and *Real Estate*.

Figure 9. Percentage of websites in each business vertical that adopted HTTPS over time



While HTTPS already provides securing communication, it would be better to also implement HSTS and Secure Cookies to have stronger protection against Man-in-the-middle (MITM) attacks. In this section, we investigate whether the newly adopted HTTPS sites implemented HSTS and Secure Cookies as well, when migrating to HTTPS.

As shown in table 16, 14% of the newly adopted HTTPS sites from 2013 to 2015 had HSTS implemented, which was more than the overall percentage (11% of all HTTPS sites in 2015). In addition, the use of Secure Cookies in newly adopted HTTPS sites was also higher than the overall percentage. The same pattern could also be found for the newly adopted HTTPS sites between 2015 and 2017.

Table 16. Percentage of newly adopted HTTPS sites that enabled Secure Cookies and HSTS features

| | HTTPS sites in 2015 | Newly adopted sites 2013-2015 | HTTPS sites in 2017 | Newly adopted sites 2015-2017 |
|--------|---------------------|-------------------------------|---------------------|-------------------------------|
| HSTS | 11.4% | 14.1% | 27.2% | 38.1% |
| Secure | 24.5% | 32.8% | 34.7% | 48.4% |

Table 16. indicates that HTTPS sites adopted in recent years tend to be more security conscious than websites having HTTPS already for a long time. In other words, the use of Secure Cookies and HSTS features would occur more often on new HTTPS websites.

- Summary

To mitigate common web attacks, websites owners can adopt several defensive mechanisms. This section gives an overview of the evolution of the adoption of these security features on the European web for the past few years. More than 8 million webpages

of 20,000 websites were crawled for analysis, through which we could observe the following longitudinal trends:

- First, the usage of client-side security mechanisms increased over time, especially the last two years (2016 and 2017), which have seen a greater improvement than the previous two-year timeframe.
- Second, the most popular websites (according to the Alexa ranking) had a higher web security metric than less popular websites. Moreover, these popular websites were adopting new security features quicker than less popular websites.
- Third, by examining the websites based on their business vertical, we can state that Education and Finance were outperforming other verticals. They were the first movers of the adoption of security features, and stayed ahead over the past few years.

To compare the web security level of different websites, we also proposed a web security scoring system. The scoring system can be used to establish a web security baseline among a set of websites, and this might help website operators to consider the adoption of security features.

The proposed web security scoring system is not optimal, since the weights given for each security feature were arbitrarily chosen based on their relative importance. To further understand the importance of these defensive mechanisms, we present a correlational study in the next section.

Correlation with Cybercrime Cost – Modelling

The past few years have seen a rapid adoption of client-side security mechanisms on the web (as discussed in the previous section). These security features are developed by security community to thwart common web attacks. In addition to reducing attack surfaces, adopting client-side security mechanisms also shows a website's security awareness, which helps to build trust with its customers. Thus, website operators are recommended to adopt these security features. However, it is unclear whether the adoption can help organizations to reduce the actual cost of cybercrime as well.

It can be argued that the adoption of advanced security practices by a website not only secures the web presence, but is also proxy for the quality of the businesses' security management practice in general. Thus, organizations with a secure presence should ultimately suffer less losses due to security incidents. To verify the hypothesis, this section presents a preliminary correlation study to analyse the relationship between the cost of cybercrime and web security posture.

To the best of our knowledge, this is the first work that studies this correlation. Our analysis indicates that businesses with better web security defences tend to have less business loss and reputation damage. The finding can motivate businesses to focus on web security, and to devote more attention to cybersecurity. Practical implications may also be significant. For example, it may also serve as an assessment factor when establishing cyber insurance premiums or audit costs.

For the analysis, we surveyed 263 Belgian businesses about the impact of cybercrime on their business (for more information on the survey used, see section 3.2.2, first wave) and gathered the statistics on the usage of security features on their websites.

- Industry Survey Result

As shown in table 17, of the valid 263 samples, about 44% (118) experienced business loss and reputation damage due to unauthorised/illegal access to IT systems, and about 22% (55) experienced business loss and reputation damage due to cyber extortion. The statistics show that the threat of cybercrime should be a real concern for businesses.

Table 17. Cybercrime experiences of 263 Belgian businesses

| cyber attacks | business loss | reputation damage |
|---------------------|---------------|-------------------|
| unauthorised access | 44.9% | 43.7% |
| cyber extortion | 22.1% | 22.1% |

While advanced attackers tend to target large companies that possess strategic resources, cybercrime poses threat to SMEs as well. As shown in table 18, more SMEs experienced unauthorised/illegal access to IT systems than large businesses did. However, large businesses had more cyber extortion experiences than SMEs, which might have been due to their higher market value.

Table 18. Cybercrime experience over different business size

| | unauthorised access | cyber extortion |
|-------------------|---------------------|-----------------|
| Small (< 50) | 38.4% | 24.2% |
| Medium (50 – 250) | 26.5% | 21.2% |
| Large (> 250) | 35.1% | 54.5% |

- Website Crawling – Hygiene Measurements

We manually checked the samples to find out the corresponding website for each survey sample, which resulted in 263 valid websites (sites with less than 10 pages were excluded from the dataset). After that, we used the web crawling approach introduced earlier to analyse these websites. For a comparative analysis, we also crawled more than 18,000 European websites, which were the popular websites from the 28 member states in the EU. The selection was based on the ccTLD (country code top-level domain) of each EU country. All the crawling experiments were all done in September 2016, within a week's time frame.

In order to assess a website's security posture, we used the web security scoring system introduced earlier to calculate feature scores for each website. Table 19 gives an overview on the use of security features on the 263 surveyed Belgian websites and the 18,731 EU websites. The percentage of EU websites that had security features enabled was greater than the surveyed Belgian websites for most features (except XCTO and XFO); this was probably due to the EU set being comprised of the popular websites, which tend to adopt more security features (Chen, Desmet, Huygens & Joosen, 2016).

Table 19. Overview of the use of security features on the European web

| Security feature | % of websites | | ECDF Avg. & Std. Error | |
|------------------|---------------|--------|------------------------|-------------|
| | BE | EU | BE | EU |
| HTTPS Support | 37.3% | 49.7% | 0.28, 0.37 | 0.37, 0.38 |
| Secure Cookies | 13.0% | 15.0% | 0.12, 0.31 | 0.14, 0.33 |
| HSTS | 6.8% | 10.0% | 0.07, 0.24 | 0.10, 0.28 |
| HPKP/CTO | 0.0% | 0.2% | 0.00, 0.00 | 0.002, 0.04 |
| HttpOnly Cookies | 41.4% | 50.2% | 0.33, 0.40 | 0.38, 0.39 |
| XCTO | 25.1% | 15.9% | 0.23, 0.41 | 0.15, 0.34 |
| CSP | 2.3% | 2.0% | 0.02, 0.15 | 0.02, 0.14 |
| XFO | 27.00% | 23.53% | 0.24, 0.40 | 0.21, 0.37 |

However, when comparing the average ECDF scores with the statistical z-test, there were no significant differences in the use of security features between the Belgian and EU websites.

- Correlation with each security feature

We used Spearman's rank correlation coefficient to analyse the relationship between the cost of cybercrime and web security posture.

Tables 20-21 show the correlations between the use of web security features and the impact of unauthorised/illegal access to IT systems and cyber extortion, respectively. For cyber extortion, all the correlations were negative, which indicates that the use of client-side security features helped to reduce the business loss and reputation damage caused by cyber extortion. However, many of the p-values were greater than the significance level of 5%. Hence, this negative correlation was not significant for many features. The same case goes for unauthorised/illegal access to IT systems.

Table 20 Spearman's rank correlation between the impact of unauthorised access to IT systems and web security features

| | unauthorised access | |
|------------------|---------------------------------------|-------------------------------------------|
| | business loss coefficient, p-value | reputation damage coefficient, p-value |
| HTTPS Support | -0.05, 0.611 | -0.03, 0.725 |
| Secure Cookies | -0.11, 0.232 | -0.22, 0.017 |
| HSTS | -0.04, 0.658 | -0.14, 0.126 |
| HttpOnly Cookies | -0.09, 0.351 | -0.002, 0.978 |
| XCTO | -0.13, 0.163 | -0.19, 0.041 |
| CSP | 0.06, 0.531 | -0.18, 0.055 |
| XFO | -0.08, 0.414 | -0.04, 0.660 |

Table 21 Spearman's rank correlation between the impact of cyber extortion and web security features

| | cyber extortion | |
|------------------|---------------------------------------|-------------------------------------------|
| | business loss coefficient, p-value | reputation damage coefficient, p-value |
| HTTPS Support | -0.24, 0.065 | -0.06, 0.658 |
| Secure Cookies | -0.30, 0.023 | -0.27, 0.044 |
| HSTS | -0.19, 0.154 | -0.19, 0.149 |
| HttpOnly Cookies | -0.27, 0.035 | -0.01, 0.951 |
| XCTO | -0.31, 0.016 | -0.38, 0.003 |
| CSP | -0.15, 0.255 | -0.18, 0.178 |
| XFO | -0.31, 0.018 | -0.22, 0.093 |

To further analyse this correlation, we dichotomised the business loss and reputation damage variables and ran a logistic regression over the different security features. As shown in tables 22-23, the β coefficient for most features was negative in the case of

unauthorised/illegal access to IT systems, pointing to a negative association between the use of security features and the impact of unauthorised/illegal access to IT systems. However, many of the coefficients were not significant. Tables 24-25 give the logistic regression result on the impact of cyber extortion over web security features. Also here we see negative, but mostly insignificant, correlations.

Table 22. Logistic regression on the business loss due to unauthorised access to IT systems over web security features

| | business loss | | | |
|------------------|---------------|------|---------------|-------|
| | β | SE | 95% CI | P |
| Constant | -1.19 | 0.35 | -1.88 ~ -0.51 | 0.001 |
| HTTPS Support | 0.31 | 0.85 | -1.35 ~ 1.98 | 0.71 |
| Secure Cookies | -3.71 | 3.82 | -11.2 ~ 3.78 | 0.33 |
| HSTS | -0.02 | 1.40 | -2.76 ~ 2.71 | 0.98 |
| HttpOnly Cookies | -0.83 | 0.77 | -2.36 ~ 0.68 | 0.28 |
| XCTO | -1.66 | 1.07 | -3.78 ~ -0.45 | 0.12 |
| CSP | 4.84 | 3.74 | -2.49 ~ 12.18 | 0.19 |
| XFO | 0.72 | 0.99 | -1.17 ~ 2.70 | 0.44 |

Table 23. Logistic regression on the reputation damage due to unauthorised access to IT systems over web security features

| | reputation damage | | | |
|------------------|-------------------|------|--------------|-------|
| | β | SE | 95% CI | P |
| Constant | 1.47 | 0.38 | 0.72 ~ 2.22 | 0.000 |
| HTTPS Support | 0.50 | 0.90 | -1.27 ~ 2.27 | 0.58 |
| Secure Cookies | -1.25 | 0.89 | -3.09 ~ 0.38 | 0.13 |
| HSTS | -0.23 | 0.81 | -2.08 ~ 1.62 | 0.81 |
| HttpOnly Cookies | 0.08 | 0.67 | -1.22 ~ 1.38 | 0.90 |
| XCTO | -1.67 | 0.86 | -3.37 ~ 0.01 | 0.05 |
| CSP | -1.60 | 1.31 | -4.17 ~ 0.98 | 0.22 |
| XFO | 1.69 | 0.99 | -0.25 ~ 3.62 | 0.09 |

Table 24. Logistic regression on the business loss due to cyber extortion over web security features

| | business loss | | | |
|------------------|---------------|-------|----------------|------|
| | β | SE | 95% CI | P |
| Constant | -0.11 | 0.48 | -1.05 ~ 0.84 | 0.83 |
| HTTPS Support | -0.44 | 0.97 | -2.33 ~ 0.64 | 0.27 |
| Secure Cookies | -25.2 | 7.9e4 | -1.6e5 ~ 1.6e5 | 1.00 |
| HSTS | -16.7 | 4.2e3 | -8.3e3 ~ 8.3e3 | 1.00 |
| HttpOnly Cookies | -1.12 | 0.90 | -2.88 ~ 0.64 | 0.21 |
| XCTO | -1.95 | 1.70 | -5.28 ~ 1.38 | 0.25 |
| CSP | -5.3 | 2.6e6 | -5.1e6 ~ 5.1e6 | 1.00 |
| XFO | 0.66 | 1.54 | -2.36 ~ 3.70 | 0.67 |

Table 25. Logistic regression on the reputation damage due to cyber extortion over web security features

| | reputation damage | | | |
|------------------|-------------------|------|--------------|-------|
| | β | SE | 95% CI | P |
| Constant | 2.54 | 0.88 | 0.81 ~ 4.27 | 0.004 |
| HTTPS Support | 0.08 | 1.66 | -3.16 ~ 3.32 | 0.96 |
| Secure Cookies | -1.62 | 1.72 | -4.99 ~ 1.76 | 0.35 |
| HSTS | 0.12 | 1.53 | -2.88 ~ 3.13 | 0.93 |
| HttpOnly Cookies | -0.38 | 1.28 | -2.90 ~ 2.13 | 0.76 |
| XCTO | -4.53 | 3.13 | -10.7 ~ 1.60 | 0.15 |
| CSP | -0.02 | 1.47 | -2.90 ~ 2.86 | 0.99 |
| XFO | 5.07 | 3.46 | -1.70 ~ 11.8 | 0.14 |

- Correlation with overall security score

In the previous section, we found a negative correlation for some security features in some cases, through a series of detailed analyses. For website owners, it would be better to have

a simple conclusion regarding the issue. Thus, we utilised the web security scoring system presented earlier, with some changes, to calculate a security score and analyse the overall correlation.

Previously, we arbitrarily assigned the weight to each feature based on maturity and importance. However, in this case, we reassigned the weights according to the correlational findings. Higher weights were given to features with more significant correlations with cybercrime costs. In particular, the following weights were used to calculate the subscores:

- **Secure Communication Score:** this subscore was measured by applying a weighted average of the HTTPS, HSTS, and Secure Cookies usage. Compared to the earlier formula, a higher weight was given to *SecureCookies* here, since it showed more significant correlations with cybercrime costs.

$$\text{SecureCommunicationScore} = \frac{30}{100} \times \text{HTTPS} + \frac{50}{100} \times \text{SecureCookies} + \frac{20}{100} \times \text{HSTS}$$

- **XSS Mitigation Score:** this subscore was measured by applying a weighted average of the HttpOnly Cookies, XCTO, and CSP usage. Compared to the earlier formula, a higher weight was given to *CSP* here, since it showed more significant correlations with cybercrime costs.

$$\text{XSSMitigationScore} = \frac{50}{100} \times \text{HttpOnlyCookies} + \frac{10}{100} \times \text{XCTO} + \frac{40}{100} \times \text{CSP}$$

- **Secure Framing Score:** this subscore was measured by the XFO usage.

$$\text{SecureFraming} = \frac{100}{100} \times \text{XFO}$$

And then for each (group of) website(s), we defined an overall security score (*OverallScore*) as a weighted average of these three scores:

$$\begin{aligned} \text{OverallScore} &= \frac{30}{100} \times \text{SecureCommunicationScore} + \frac{60}{100} \times \text{XSSMitigationScore} + \frac{10}{100} \\ &\times \text{SecureFramingScore} \end{aligned}$$

We then analysed the correlation between the obtained *OverallScore* and the cost of cybercrime, as shown in table 26. The negative coefficients imply that the higher the *OverallScore* was, the lower the costs of cybercrime were. For unauthorised access/illegal access to IT systems, the p-values were around 10%, which indicates that the correlation was not significant. However, the correlation between cyber extortion and overall web security was significant.

Table 26. Correlation between the cost of cybercrime and overall web security

| Spearman's rank correlation | | β | P |
|-----------------------------|-------------------|---------|--------|
| unauthorised access | business loss | -0.16 | 0.089 |
| | reputation damage | -0.15 | 0.106 |
| cyber extortion | business loss | -0.43 | 0.0008 |
| | reputation damage | -0.27 | 0.037 |

4.2.2.2. Surveys

In this paragraph, we first discuss the extent to which businesses have been confronted with cybercrime in the 12 preceding months. Next, we focus on the business representatives' perceptions of the likelihood of their business being attacked in the following 12 months. Third, we estimate the harms to material support, that is, the costs of cybercrime that the businesses have experienced. Fourth, we discuss the business representatives' assessments of the non-material harm of cybercrime that the businesses have experienced.

Victimization

- First Wave

Two thirds of the businesses (66.5% or 181 businesses) have been victims of cybercrime, at least once in the last 12 months. Specifically, illegal access to IT systems and data/system interference are much more prevalent than the other types: 50% of the businesses (or 155 businesses) report illegal access to their IT systems and 44% (or 128 businesses) data/system interference. Less than a quarter admit cyber extortion (24.1% or 68 businesses), and still fewer internet fraud (12.9% or 35 businesses) and cyber espionage (3.6% or 10 businesses).

The majority of the businesses have suffered repeated attacks. The data shows that 83.2% of the 155 victims report repeated attempts at illegal access to their IT system; 72.7% of the 128 victims experience repeated incidents of data or system interference, and 57.4% of the 68 victims report repeated cyber extortion incidents. Four out of the ten victims experience repeated incidents of cyber espionage and 22 out of the 35 victims experience more than one incident of internet fraud. Only for cyberespionage, the number of repeat victims is lower than half.

- Second Wave

Half of the businesses in our sample (53.6% or 125 businesses) have been victims of one of the five cybercrime types, at least once in the last 12 months. Specifically, illegal access to IT systems is the most prevalent: 32.7% (or 83 businesses). About a fifth of the respondents reported being victims of data/system interference (20.2% or 49 businesses), or cyber extortion (18.9% or 47 businesses). Slightly more than a tenth of the respondents indicated that their business had been a victim of internet fraud (12.6% or 30 businesses) or cyber espionage (10.6% or 29 businesses).

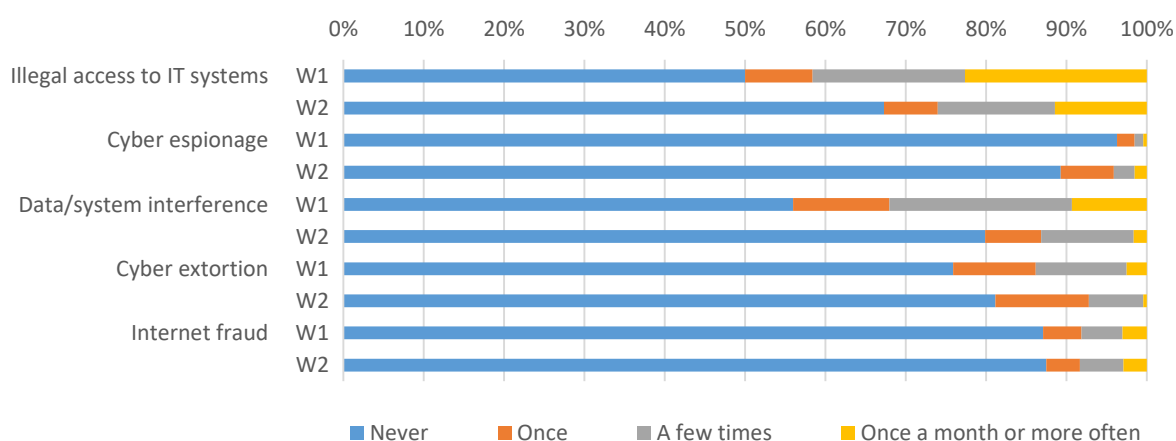
For three of the cybercrime types, there were more repeated victims than single victims: 79.5% of the victims report repeated incidents of illegal access to IT systems, 65.3% of data/system interference, 66.6% internet fraud. On the contrary, for cyber espionage and

cyber extortion, there were more single victims (cyber espionage: 62.1%; cyber extortion: 61.7%) than multiple victims.

- Comparison

We observe a substantial decrease in the percentage of businesses reporting victimization of at least one type of cybercrime (from 66.5% in the first wave to 53.6% in the second wave; see figure 4 for a visual representation). In particular, the victimization rates of illegal access to IT systems and data/system interference are substantially lower in the second wave than in the first wave (32.7% compared to 50.0% and 20.2% compared to 44.0%, implying declines of -17.3% and -23.8%, respectively). The percentage of businesses reporting victimization of cyber extortion has also decreased, but to a lesser extent (from 24.1% to 18.9%: -5.2%). However, the victimization rate of cyber espionage has increased from 3.6% in the first wave to 10.6% in the second wave (+7%). The percentage of businesses admitting victimization of internet fraud is more or less equal in both waves (12.9% in the first wave versus 12.6% in the second wave; see figure 10).

Figure 10. Incidence of cybercrime in past 12 months



Note. W1: wave 1, W2: wave 2. Samples sizes varied between 272 and 310 in the first wave and between 239 and 74 in the second wave. Answer possibilities roughly once a month, roughly once a week, roughly once a day, several times a day and hundreds of times a day were combined into the category once a month or more often to keep the figure clear for the reader.

A comparison of the incidences of each cybercrime type reveals that businesses in the second wave ($M = 0.96$, $SD = 1.74$; $M = 0.35$, $SD = 0.77$; $M = 0.27$, $SD = 0.62$, respectively) are less often confronted with illegal access to IT systems, data/system interference and cyber extortion than businesses in the first wave ($M = 1.53$, $SD = 1.98$; $M = 0.91$, $SD = 1.25$ and $M = 0.41$, $SD = 0.83$, respectively; $t(559.13) = 3.653$, $p < .001$; $t(491.10) = 6.330$, $p < .001$ and $t(514.58) = 2.308$, $p = .021$, respectively). On the other hand, the incidence of cyber espionage is significantly higher in the second wave ($M = 0.19$, $SD = 0.72$) than in the first wave ($M = 0.05$, $SD = 0.31$; $t(370.34) = -2.875$, $p = .004$). No significant differences between the two waves are found for the incidence of internet fraud ($t(509) = 0.001$, $p = .999$).

Perceived Victimization Risk

- First Wave

Most of respondents assess their business's risk of being victimized in the next 12 months, as "very unlikely" or "unlikely," with the exception of illegal access to IT systems. For this cybercrime type, the most frequent answers chosen by the respondents are "unlikely" and "likely." Especially illegal access to IT systems (via the use of hackertools and techniques) is perceived as likely to occur in the next 12 months. Approximately 60% of the representatives assess their business's probability of experiencing this crime in the next 12 months as "likely" or "very likely" (see table 27).

- Second Wave

Similarly to the first wave, most respondents assess their business's risk of being victimized in the next 12 months as "very unlikely" or "unlikely," with the exception of illegal access to IT systems. For the latter cybercrime type, the most frequent answers are "unlikely" and "likely." Once again illegal access to IT systems via the use of hackertools and techniques is perceived as likely to occur in the next 12 months: about 55% of the representatives assess their business's probability of experiencing this crime in the next 12 months as "likely" or "very likely" (see table 27)

- Comparison

We find no significant differences between the two waves for cybercrime in general ($t(515) = 0.443$, $p = .658$). However, a separate test for the different cybercrime types reveals that the perceived risk of victimization of cyber espionage is significantly higher in the second wave ($M = 0.98$, $SD = 0.61$) than in the first wave ($M = 0.83$, $SD = 0.68$; $t(524.69) = -2.778$, $p = .006$), whereas for data/system interference the perceived risk is significantly lower in the second wave ($M = 1.01$, $SD = 0.60$) than in the first wave ($M = 1.13$, $SD = 0.66$). For the perceived risk of the other three cybercrime types, no significant differences are found between the two waves (illegal access to IT systems: $t(538) = 1.616$, $p = .107$; cyber extortion: $t(513) = -0.788$, $p = .431$; internet fraud: $t(484) = 0.742$, $p = .458$).

Table 27. Perceived victimization risk of cybercrime in next 12 months

| Type/technique | Wave | Perceived risk of victimization | | | |
|------------------------------------------|------|---------------------------------|----------|--------|-------------|
| | | Very unlikely | Unlikely | Likely | Very likely |
| Illegal access to IT systems | | | | | |
| • Hackertools and – techniques | W1 | 11.4% | 29.2% | 33.2% | 26.2% |
| | W2 | 12.9% | 33.2% | 39.4% | 14.5% |
| • Exceeding access privileges by users | W1 | 21.8% | 47.0% | 21.8% | 9.4% |
| | W2 | 23.3% | 46.3% | 27.1% | 3.3% |
| • Exploiting vulnerabilities in security | W1 | 13.7% | 44.1% | 33.4% | 8.7% |
| | W2 | 16.6% | 41.5% | 35.7% | 6.2% |
| • Other | W1 | 18.6% | 40.7% | 30.7% | 10.0% |
| | W2 | 16.5% | 47.5% | 31.8% | 4.2% |
| Cyber espionage | | | | | |
| • Bulk business data | W1 | 32.8% | 49.8% | 15.5% | 1.9% |
| | W2 | 21.9% | 50.9% | 25.3% | 1.9% |
| • High value IP | W1 | 39.6% | 44.9% | 14.0% | 1.5% |
| | W2 | 38.3% | 46.8% | 13.0% | 1.9% |
| • Tactical corporate information | W1 | 35.5% | 47.9% | 15.5% | 1.1% |
| | W2 | 24.9% | 56.9% | 15.6% | 2.6% |
| • Other | W1 | 34.4% | 48.6% | 15.8% | 1.2% |
| | W2 | 19.0% | 53.4% | 25.0% | 2.6% |

| Data/system interference | | | | | |
|-----------------------------------------------------|----|-------|-------|-------|-------|
| • Data interference | | | | | |
| - Webserver | W1 | 20.7% | 41.9% | 30.0% | 7.4% |
| | W2 | 22.9% | 48.9% | 24.7% | 3.5% |
| - Mailserver | W1 | 15.6% | 41.9% | 28.9% | 13.7% |
| | W2 | 19.5% | 44.6% | 30.7% | 5.2% |
| - Services for online storage of internal documents | W1 | 30.6% | 46.3% | 17.9% | 5.2% |
| | W2 | 29.9% | 49.4% | 19.9% | 0.9% |
| • System interference | | | | | |
| - PC-infrastructure | W1 | 18.2% | 52.8% | 23.0% | 5.9% |
| | W2 | 22.9% | 55.4% | 21.2% | 0.4% |
| - Network infrastructure | W1 | 22.7% | 53.2% | 19.3% | 4.8% |
| | W2 | 26.0% | 51.9% | 21.6% | 0.4% |
| - Peripherals | W1 | 25.8% | 56.6% | 14.2% | 3.4% |
| | W2 | 29.1% | 56.5% | 13.9% | 0.4% |
| - Business website | W1 | 20.0% | 52.5% | 22.6% | 4.9% |
| | W2 | 23.9% | 51.3% | 23.5% | 1.3% |
| Cyber extortion | | | | | |
| • Protection money | W1 | 28.3% | 49.3% | 19.9% | 2.6% |
| | W2 | 24.0% | 53.3% | 21.9% | 0.8% |
| • Ransom money | W1 | 23.0% | 42.0% | 26.8% | 8.2% |
| | W2 | 16.1% | 45.5% | 33.1% | 5.4% |
| • Hush money | W1 | 35.3% | 47.4% | 14.7% | 2.6% |
| | W2 | 30.4% | 51.7% | 16.7% | 1.3% |
| Internet fraud | | | | | |
| • Advance fee fraud | W1 | 33.2% | 40.7% | 21.3% | 4.7% |
| | W2 | 36.1% | 37.4% | 18.7% | 7.8% |
| • Consumer fraud | W1 | 37.5% | 45.1% | 15.0% | 2.4% |
| | W2 | 47.4% | 38.7% | 11.7% | 2.2% |
| • Fraud with internet banking | W1 | 30.7% | 39.8% | 21.7% | 7.9% |
| | W2 | 29.9% | 41.1% | 23.4% | 5.6% |

Costs

As noted earlier, we have operationalized the costs (that is, harms to material support), through the internal and outsourced staff time and the related costs invested in neutralizing cyber incidents as well as the business's assessment of four direct costs—(1) hardware and software replacement, (2) value of other lost or damaged assets (e.g., data files), (3) the money paid to offender and (4) fines and compensation payments—as well as the opportunity cost of potential revenue lost.

- Staff Costs

- First Wave

Most respondents reported that they resolved the only or last incident in less than one business day (illegal access to IT systems: 81.7%; data/system interference: 79.6%; cyber extortion: 68.2%). However, about 18% to 32% of these incidents required more than one business day to be neutralized (illegal access to IT systems: 18.3%; data/system interference: 20.3%; cyber extortion: 31.8%), a percentage that grows up to more than 49.2% for all incidents of illegal access to IT systems recorded in the last 12 months (see table 28).

Table 28. Staff time invested in neutralizing cyber incidents suffered (first wave)

| Type | | Staff time invested | | | | |
|--------------------------------|--------------|---------------------|--------------------------|-------------------------|---------------------|-------------------|
| | | < 1 hour | 1 hour – < Half a day | Half a day – < 1 day | 1 day – < 1 week | 1 week or more |
| Percent values | | | | | | |
| • Illegal access to IT systems | Only/last | 32.0% | 28.1% | 21.6% | 14.4% | 3.9% |
| | All | 16.7% | 15.1% | 19.0% | 29.4% | 19.8% |
| • Data/system interference | Only/last | 20.3% | 34.1% | 25.2% | 18.7% | 1.6% |
| | Most serious | 15.2% | 27.8% | 29.1% | 22.8% | 5.1% |
| • Cyber extortion | Only/last | 12.1% | 30.3% | 25.8% | 24.2% | 7.6% |
| Absolute values | | | | | | |
| • Cyber espionage | Only/last | - | 2 | 3 | 3 | - |

Outsourcing to external businesses or consultants occurs in less than half of all incidents, but the neutralization of data/system interference is outsourced more frequently than the neutralization of other cybercrime types. In fact, the only/last incidents of illegal access to an IT system and cyber extortion have been dealt with in more than half of the cases without external business or consultants, whereas this percentage decreases to 42.4% in the case of incidents of data/system interference. The latter type of cybercrime is likely to be considered the most complicated to deal with, as its neutralization is also most frequently fully outsourced: 27.1% of the only/last incidents of data/system interference are fully outsourced, whereas this percentage decreases to 15% in the case of illegal access to IT systems and 6.1% for cyber extortion (see table 29).

Table 29. Staff time invested in neutralizing cyber incidents outsourced to external businesses or consultants (first wave)

| Type | | Outsourced staff time | | | | |
|--------------------------------|--------------|-----------------------|--------|-------|-------|-------|
| | | None | < Half | Half | Most | All |
| Percent values | | | | | | |
| • Illegal access to IT systems | Only/last | 56.9% | 11.8% | 7.2% | 9.2% | 15.0% |
| | All | 49.2% | 14.8% | 10.7% | 10.7% | 14.8% |
| • Data/system interference | Only/last | 42.4% | 10.2% | 8.5% | 11.9% | 27.1% |
| | Most serious | 41.8% | 12.7% | 11.4% | 12.7% | 21.5% |
| • Cyber extortion | Only/last | 68.2% | 7.6% | 6.1% | 12.1% | 6.1% |
| Absolute values | | | | | | |
| • Cyber espionage | Only/last | 5 | 2 | - | - | 1 |

○ Second Wave

Most businesses report that incidents were primarily addressed by their own employees. More concretely, we see that more than 60% of the illegal access to IT systems and cyber extortion incidents were resolved only by employees of the business itself. However, this percentage decreases to about 40% for incidents of data/system interference, indicating that such incidents are more complicated to deal with by the businesses. The same is true for cyber espionage, for which only 13 of the 27 incidents were solely addressed by own employees (see table 30).

Table 30. Parties responsible for neutralization of cyber incidents (second wave)

| Type | | Responsible for neutralization | | | |
|--------------------------------|--------------|--------------------------------|----------------|----------------|---------------------------|
| | | No one | Internal staff | External staff | Internal & external staff |
| Percent values | | | | | |
| • Illegal access to IT systems | Only/last | 2.5% | 62.0% | 24.1% | 11.4% |
| | Most serious | 3.6% | 63.6% | 21.8% | 10.9% |
| • Data/system interference | Only/last | 4.2% | 43.8% | 27.1% | 25.0% |
| • Cyber extortion | Only/last | 4.3% | 66.0% | 12.8% | 17.0% |
| Absolute values | | | | | |
| • Cyber espionage | Only/last | - | 13 | 10 | 4 |

Note. Samples sizes were 79 and 55 for the last/only and most serious incidents of illegal access to IT systems, respectively, 48 for data/system interference and 47 for cyber extortion.

By multiplying the number of man hours spent by (IT) employees on neutralizing an incident by the average salary of such an employee, we have obtained a rough estimate of the internal staff costs. Although the sample sizes are very small and answers are widely dispersed (in particular for data/system interference), the findings indicate that internal staff costs are the lowest for illegal access to IT systems, followed by cyber extortion and data/system interference. The internal staff costs of cyber espionage incidents tend to be the highest (see table 31).

Table 31. Internal staff costs of cyber incidents (second wave)

| Type | | n | Internal staff costs (in €) | | | | |
|--------------------------------|--------------|----|-----------------------------|-----------|----------|----------|----------|
| | | | Min | Max | M | SD | Med |
| • Illegal access to IT systems | Only/last | 26 | 18.30 | 2,250.00 | 339.68 | 539.09 | 92.00 |
| | Most serious | 19 | 22.00 | 3,750.00 | 720.26 | 915.23 | 520.00 |
| • Cyber espionage | Only/last | 8 | 117.66 | 6,000.00 | 1,962.46 | 2,144.94 | 1,366.00 |
| • Data/system interference | Only/last | 19 | 19.61 | 11,250.00 | 1,086.83 | 2,536.85 | 280.00 |
| • Cyber extortion | Only/last | 20 | 33.00 | 3,500.00 | 810.45 | 885.28 | 440.00 |

In addition, we considered the costs of outsourcing the neutralization of these four cybercrime types. First of all, some respondents indicated that they did not have to pay the external consultant or business responsible for the neutralization of an incident, because they had an open-ended contract with them. This was the case for 4 out of the 19 only/last, and 2 out of the 14 most serious incidents of illegal access to IT systems, 1 out of the 11 incident(s) of cyber espionage, and 6 out of the 18 incidents of data/system interference. Hence, these incidents did not result in additional outsourcing costs. If businesses outsourced the neutralization of cybercrime, the external staff costs tend to be the highest for cyber espionage and the lowest for cyber extortion (see table 32). However, important to keep in mind in interpreting this data is that the sample sizes are very small and the answers widely dispersed.

Table 32. External staff costs of cyber incidents (second wave)

| Type | | n | External staff costs (in €) | | | | |
|--------------------------------|--------------|----|-----------------------------|-----------|----------|----------|----------|
| | | | Min | Max | M | SD | Med |
| • Illegal access to IT systems | Only/last | 15 | 100.00 | 15,000.00 | 2,863.40 | 4,344.76 | 900.00 |
| | Most serious | 12 | 200.00 | 25,000.00 | 4,271.45 | 7,506.31 | 1,200.00 |
| • Cyber espionage | Only/last | 10 | 250.00 | 10,000.00 | 3,290.00 | 3,332.40 | 1,750.00 |
| • Data/system interference | Only/last | 12 | 50.00 | 20,000.00 | 3,794.75 | 6,630.58 | 650.00 |
| • Cyber extortion | Only/last | 14 | 201.00 | 10,000.00 | 1,800.07 | 2,707.14 | 800.00 |

- Non-Staff Costs

- First Wave

Hard- and software replacement. More than half of the businesses have had no costs for replacing hardware or software after suffering illegal access to their IT systems (55.6%), data/system interference (57.5%) or cyber extortion (66.7%). Only between 1.5% and 4% of the businesses report replacement costs of €10,000 or more due to the only/last incident of illegal access to their IT systems, data/system interference or cyber extortion – and the order of magnitude remains similar for all incidents of illegal access to IT systems and for the most serious incident of data/system interference.

Value of other lost or damaged assets. More than half of the businesses victim of cyber extortion report no lost or damaged assets. For data/system interference this percentage is higher than 60% for the most serious incident and over 70% for the only/last incident. Only 9% of the businesses suffering cyber extortion report costs of €10,000 or more; for data/system interference, the percentage is in all cases lower than 3%.

Money paid to offender. Only 6.1% of the businesses suffering cyber extortion did pay ransom, “protection”, or “hush” money to the offender; in any case the sum paid to the offender remained below €10,000.

Fines and compensation payments. For cyber extortion as well as for illegal access to IT systems (only/last and all), and the only/last incidents of data/system interference, more than 90% of the businesses report paying no fines or compensation to injured parties. Only for the most serious incidents of data/system interference, this percentage slightly decreases to 86.4%.

Lost revenue. Finally, a large majority of the businesses also indicate that they have not lost any revenue because of cyber incidents, even if there are considerable differences from one cybercrime type to the other. The percentage experiencing no loss is—unsurprisingly—the highest for illegal access to IT systems (only/last: 76.8%; all: 72.4%), followed by cyber extortion (only/last: 72.7%), and data/system interference (only/last: 61.7% and most serious: 60%). However, between 11.3% and 24.2% of the businesses estimate losing between €1 and €9,999 because of one of these three cybercrime types. Much smaller percentages of businesses confronted with illegal access to their IT system (only/last: 3.3%; all: 3.2%) and

data/system interference (only/last: 5.8%; most serious: 6.3%) admit suffering losses of €10,000 or more.

- Second Wave

Hard- and software replacement. The large majority of the victimized businesses incurred no costs for replacing hardware or software after suffering illegal access to their IT systems (82.9%), data/system interference (68.2%) or cyber extortion (71.7%). Only 1.9% to 2.6% percent of the victimized businesses had replacement costs of more than €10,000 due to the only/last incident of illegal access to their IT systems or data/system interference. None of the victimized businesses had replacement costs over €10,000 due to the only/last incident of cyber extortion.

Value of other lost or damaged assets. The large majority of the victimized businesses reported no lost or damaged assets for data/system interference (75.0%) or cyber extortion (62.2%). However, cyber extortion incidents are slightly more likely to result in lost or damaged assets than data system interference incidents. Only 13.3% of the businesses suffering cyber extortion reported costs of €1,000 or more; for data/system interference, this percentage is only 4.6%.

Money paid to offender. For the only/last incident, sums demanded by the offender range from €20 all the way up to €250,000 (25% quartile: €500; Med: €1,000; 75% quartile: €6,500). However, only one of the victimized businesses (or 2.2%) admitted giving in and paying €500.

Fines and compensation payments. For illegal access to IT systems and data/system interference, only very few of the victimized businesses paid fines or compensation to injured parties due to the only/last incidents (2.6% and 2.3%, respectively). For cyber extortion, none of the representatives of the victimized businesses indicated that fines or compensation was paid as a result of the only/last incident.

Lost revenue. A large majority of the victimized businesses indicated that they did not lose any revenue because of the cybercrime incidents, even if there are considerable differences from one type to the other. The percentage experiencing no loss is—unsurprisingly—the highest for illegal access to IT systems (only/last: 86.8%; most serious: 78.8%), followed by cyber extortion (only/last: 77.8%), and data/system interference (only/last: 68.2%). However, between 5.2% and 13.6% of the businesses estimate losing between €1 and €10,000 because of incidents, and between 2.2% and 5.2% estimate losing more than €10,000. In the case of internet fraud, eight of the 26 victimized businesses report revenue losses up to €500 due to the only/last incident, three report losses between €1,001 and €2,500, two report losses between €10,001 and €25,000, and six report losses higher than €50,000. Seven victimized businesses do not provide an amount.

○ Comparison

Overviews of the costs of the only or last incidents of each cybercrime type in the two waves are given in table 33. We briefly discuss below the similarities and differences between the two waves for the three cybercrime types for which we have substantial data (i.e. illegal access to IT systems, data/system interference and cyber extortion):

- Hard- and software replacement: the costs for hard- and software replacement resulting from illegal access to IT systems and data/system interference are significantly higher in the first wave ($M = 0.69$, $SD = 1.11$ and $M = 0.54$, $SD = 0.76$, respectively) than in the second wave ($M = 0.24$, $SD = 0.66$ and $M = 0.28$, $SD = 0.61$, respectively); $t(211.72) = 3.696$, $p < .001$ and $t(81.71) = 2.177$, $p = .032$, respectively) no significant statistical difference can be found for cyber extortion ($t(105) = 0.277$, $p = .785$).
- Value of other assets lost or damaged: the value of the other assets lost or damaged as a result from data/system interference and cyber extortion incidents is not significantly different in the two waves ($t(141) = 0.116$, $p = .908$; $t(87.52) = 1.928$, $p = .057$).
- Fines and compensation payments: for none of the three cybercrime types the fines and compensation payments are significantly different in the two waves (illegal access to IT systems: $t(217) = -0.378$, $p = .706$; data system interference: $t(153) = 0.630$, $p = .530$; cyber extortion: $t(63) = 1.930$, $p = .058$).
- Revenue lost: for this category as well, the data indicate no significant statistical difference for any of the three cybercrime types (illegal access to IT systems: $t(210) = 0.734$, $p = .464$; data/system interference: $t(92.40) = 0.630$, $p = .530$; cyber extortion: $t(63) = 1.930$, $p = .058$).

Table 33. Costs resulting from the cyber incidents suffered

| Aspect | Type | Wave | Cost | | | | | |
|---------------------------------------|--------------------------------|------|-------------|--------------|------------------|-------------------|-------------------|------------|
| | | | Nothing | € 1 - €1,000 | €1,001 – €10,000 | €10,001 - €50,000 | More than €50,000 | Don't know |
| Hard & software replacement | • Illegal access to IT systems | W1 | 84 (55.6%) | 36 (23.8%) | 18 (11.9%) | 3 (2.0%) | 3 (2.0%) | 7 (4.6%) |
| | | W2 | 63 (82.9%) | 6 (7.9%) | 3 (3.9%) | 2 (2.6%) | - | 2 (2.6%) |
| | • Data/system interference | W1 | 69 (57.5%) | 34 (28.3%) | 10 (8.3%) | 3 (2.5%) | - | 4 (3.3%) |
| | | W2 | 30 (68.2%) | 8 (18.2%) | - | 1 (2.3%) | - | 5 (11.4%) |
| | • Cyber extortion | W1 | 44 (66.7%) | 18 (27.3%) | 1 (1.5%) | 1 (1.5%) | - | 2 (3.0%) |
| | | W2 | 33 (71.7%) | 6 (13.0%) | 4 (8.7%) | - | - | 3 (6.5%) |
| | • Cyber espionage | W1 | 4 | 3 | - | - | - | 2 |
| | | W2 | 16 | 4 | 3 | - | - | 3 |
| Value of other assets lost or damaged | • Data/system interference | W1 | 86 (71.7%) | 16 (13.3%) | 3 (2.5%) | 1 (0.8%) | 1 (0.8%) | 13 (10.8%) |
| | | W2 | 33 (75.0%) | 1 (2.3%) | 1 (2.3%) | - | 1 (2.3%) | 8 (18.2%) |
| | • Cyber extortion | W1 | 33 (50.0%) | 10 (15.2%) | 7 (10.6%) | 1 (1.5%) | 5 (7.6%) | 10 (15.2%) |
| | | W2 | 28 (62.2%) | 3 (6.7%) | 4 (8.9%) | 2 (4.4%) | - | 8 (17.8%) |
| | • Cyber espionage | W1 | 1 | 3 | - | - | 2 | 3 |
| | | W2 | 7 | 2 | 5 | 3 | 1 | 8 |
| Fines and compensation payments | • Illegal access to IT systems | W1 | 137 (90.7%) | 5 (3.3%) | 1 (0.7%) | - | - | 8 (5.3%) |
| | | W2 | 74 (97.4%) | - | 1 (1.3%) | 1 (1.3%) | - | - |
| | • Data/system interference | W1 | 111 (93.3%) | 4 (3.4%) | - | 1 (0.8%) | - | 3 (2.5%) |
| | | W2 | 38 (86.4%) | 1 (2.3%) | - | - | - | 5 (11.4%) |
| | • Cyber extortion | W1 | 60 (90.9%) | 3 (4.5%) | 1 (1.5%) | - | - | 2 (3.0%) |
| | | W2 | 41 (89.1%) | - | - | - | - | 5 (10.9%) |
| | • Cyber espionage | W1 | 5 | 2 | - | - | - | 2 |
| | | W2 | 24 | - | - | - | - | 2 |
| Revenue lost | • Illegal access to IT systems | W1 | 116 (76.8%) | 6 (4.0%) | 11 (7.3%) | 4 (2.6%) | 1 (0.7%) | 13 (8.6%) |
| | | W2 | 66 (86.8%) | 3 (3.9%) | 1 (1.3%) | 3 (3.9%) | 1 (1.3%) | 2 (2.6%) |
| | • Data/system interference | W1 | 74 (61.7%) | 12 (10.0%) | 13 (10.8%) | 4 (3.3%) | 3 (2.5%) | 14 (11.7%) |
| | | W2 | 30 (68.2%) | 4 (9.1%) | 2 (4.5%) | 2 (4.5%) | - | 6 (13.6%) |
| | • Cyber extortion | W1 | 48 (72.7%) | 10 (15.2%) | 6 (9.1%) | - | - | 2 (3.0%) |
| | | W2 | 55 (77.8%) | 4 (8.9%) | 1 (2.2%) | - | 1 (2.2%) | 4 (8.9%) |
| | • Cyber espionage | W1 | 2 | 3 | - | 1 | 1 | 2 |
| | | W2 | 15 | 1 | 4 | 2 | - | 4 |

Harms

In the two survey waves, we also considered the severity of the harms caused by cybercrime to three interest dimensions, functional integrity (split up into services to customers and internal operational integrity), reputation, and privacy. For this assessment, respondents could choose among six ratings: none, marginal, moderate, serious, grave and catastrophic. In our comments, we combine the ranking of marginal and moderate, as well as serious and grave, to better illustrate the key points.

- **First Wave**

For the three cybercrime types for which we have substantial data (i.e., illegal access to IT systems, data/system interference and cyber extortion), the victimized businesses consistently report that the internal operational activities are more seriously affected than the services to customers, reputation and privacy. Between 33.3% and 65.8% of the victimized businesses, for example, report no harm to these last three dimensions. The percent of no harm generally decreases to about 30% to 20% in the case of internal operational activities (last/only incident of illegal access to an IT system: 33.3%; only/last incident of data/system interference: 18.3%; and only/last incident of cyber extortion: 19.7%).

Even for the services to customers, reputation, and privacy, between 35% and 50% of the victimized businesses report marginal or moderate harm to these three interest dimensions, with slightly higher percentages for the harms to customers' services in all the incidents of illegal access to IT systems and the most serious incidents of data/system interference. About five to ten percent of the victimized businesses have experienced serious or grave harm to one or more of these three interest dimensions, a percentage that goes up to 13.4% for services to customers after the most serious incident of data/system interference. Moreover, in the case of cyber extortion, small percentages of the victimized businesses suffer catastrophic harms to the services to customers (3.1%), reputation (1.6%), and privacy (3.3%).

Respondents consistently rank the harms to the internal operational activities higher than to other dimensions. Only for the only or last incident of illegal access, one third of the respondents report no harm, otherwise the percent of no harm is as low as 20%. Between 52.5% and 63.3% of the victimized business have experienced marginal or moderate harm to their internal operational activities, and between 14.2% and 21.6% report serious or more harm. About 1% of the victimized business even admit catastrophic harm to their internal operational activities because of illegal access or data/system interference. For cyber extortion, the percentages are higher. For the only or last incident of this cybercrime type, 16.7% of the businesses describe the harm suffered as serious or grave, and 4.5% admit having suffered catastrophic harm.

In the case of cyber espionage and internet fraud, there is no interest dimension that appears to be more affected than the other ones (but the data should to be interpreted with great caution) due to the low numbers. The businesses that were victim of cyber espionage (n = 7 or 8), provide the following harm assessments of the only or last incident:

- Services to customers: one reports no harm, five report marginal or moderate harm, one reports serious harm and one catastrophic harm to this interest dimension;
- Internal operational activities: one reports no harm, five report marginal or moderate harm, one reports grave harm and one catastrophic harm to this interest dimension;
- Reputation: one reports no harm, five report marginal or moderate harm, one reports serious harm and one catastrophic harm to this interest dimension;
- Privacy: two report no harm, three report marginal or moderate harm, one reports serious harm and one catastrophic harm to this interest dimension.

The businesses that fell victim to internet fraud (n = 27 or 28) assess the harm of the only/last incident as follows:

- Services to customers: 16 report no harm, seven marginal or moderate harm and five serious or grave harm;
- Internal operational activities: 13 report no harm, 12 marginal or moderate harm and four serious or grave harm to this interest dimension;
- Reputation: 14 report no harm, ten marginal or moderate harm and four serious or grave harm to this interest dimension;
- Privacy: 15 report no harm, nine marginal or moderate harm and three serious or grave harm to this interest dimension.

None of the victims of internet fraud assess the harm to one of the four interest dimensions as catastrophic.

- Second Wave

For the three cybercrime types for which we have substantial data (i.e., illegal access to IT systems, data/system interference and cyber extortion), we see once again that the victimized businesses report that the internal operational activities are more seriously affected than the services to customers, reputation and privacy. However, depending on the cybercrime, the harms to the internal operational activities are assessed differently. For the only or last incident of illegal access to an IT system, one third of the respondents reported no harm, whereas this percentage was lower than 10% for the only/last incidents of data/system interference or cyber extortion. In general, about 65% of the victimized business have experienced marginal or moderate harm to their internal operational activities, and about 25% to 30% reported serious or more harm for the three crimes here considered. However, for illegal access to IT systems, these percentages were lower: for the only or last incident of this cybercrime type, 47.8% of the businesses described the harm suffered as marginal or moderate, and 13% admitted having suffered serious or more harm. Hence, we can conclude that incidents of illegal access to IT systems are less harmful to the internal operational activities than incidents of data/system interference and cyber extortion.

In addition, we see that the incidents of illegal access to IT systems generate similar harms (or lack thereof) for the businesses' reputation and privacy as they do for the internal operational activities: between 39.1% and 44.9% of the representatives of the victimized businesses assessed these incidents as harmless for these three interest dimensions. For marginal or moderate and serious or more harm, there are some differences between the

three dimensions: about 45% of the representatives of the victimized businesses assessed the harms of incidents of illegal access to IT systems to internal operational activities and privacy as marginal or moderate, whereas only 34.7% did so for reputation. On the contrary, about 20% of the representatives of victimized businesses assessed the harms of incidents of illegal access to IT systems to reputation as serious or more, whereas only 13% did so for internal operational activities and privacy.

Even for the services to customers, reputation, and privacy, about 35% to 60% of the victimized businesses reported marginal or moderate harm due to incidents of illegal access to IT systems, data/system interference or cyber extortion. About 10 to 25% of the victimized businesses have experienced serious or grave harm to these three interest dimensions. Moreover, in the case of illegal access to IT systems and cyber extortion, small percentages of the victimized businesses suffer catastrophic harms to reputation (1.4% and 2.2%, respectively) and privacy (1.4% and 2.2%, respectively).

In the case of cyber espionage, the data also indicates that internal operational activities are most seriously affected, but the data should to be interpreted with great caution due to the low number of businesses confronted with this cybercrime type. More concretely, the representatives of the businesses that were victims of cyber espionage (n = 25 to 27) provided the following harm assessments of the only/last incident:

- Internal operational activities: six reported no harm, 14 marginal or moderate harm, six serious or grave harm and one catastrophic harm to this interest dimension;
- Services to customers: 13 report no harm, eight marginal or moderate harm, and six serious or grave harm to this interest dimension;
- Reputation: ten report no harm, ten marginal or moderate harm, and five serious or grave harm to this interest dimension;
- Privacy: 11 report no harm, eight marginal or moderate harm, seven serious or grave harm to this interest dimension.

In the case of internet fraud, the data indicates that reputation was more seriously affected than the internal operational activities. However, once again the data should to be interpreted with great caution due to the low number of victimized businesses. Specifically, the representatives of businesses that fell victim to internet fraud (n = 28 or 29) assessed the harms of the only/last incident as follows:

- Internal operational activities: 12 reported no harm, 12 marginal or moderate harm, four serious or grave harm and one catastrophic harm to this interest dimension;
- Services to customers: 14 reported no harm, ten marginal or moderate harm, four serious or grave harm and one catastrophic harm to this interest dimension;
- Reputation: nine reported no harm, 13 marginal or moderate harm, four serious or grave harm and two catastrophic harm to this interest dimension;
- Privacy: 12 report no harm, 13 marginal or moderate harm, three serious or grave harm and one catastrophic harm to this interest dimension.

- Comparison

Overviews of the non-material harms of the only or last incidents of each cybercrime type in the two waves are given in table 34. We briefly discuss below the similarities and differences between the two waves for the three cybercrime types for which we have substantial data (i.e. illegal access to IT systems, data/system interference and cyber extortion):

- Services to customers: the harm to businesses' customer services resulting from data/system interference is significantly higher in the second wave ($M = 1.56$, $SD = 1.20$) than in the first wave ($M = 0.99$, $SD = 1.08$; $t(155) = -2.873$, $p = .005$); no significant statistical difference can be established in the case illegal access to IT systems and cyber extortion ($t(199) = 0.481$, $p = .631$ and $t(109) = -1.431$, $p = .155$, respectively).
- Internal operational activities: for none of the three cybercrime types is the harm to the internal operational activities significantly different between the two waves (illegal access to IT systems: $t(208) = 0.612$, $p = .541$; data system interference: $t(162) = -1.327$, $p = .187$; cyber extortion: $t(110) = -1.215$, $p = .227$).
- Reputation: the harm to businesses' reputation resulting from data system interference and cyber extortion is significantly higher in the second wave ($M = 1.32$, $SD = 1.20$ and $M = 1.18$, $SD = 1.37$, respectively) than in the first wave ($M = 0.88$, $SD = 1.02$ and $M = 0.70$, $SD = 1.08$, respectively; $t(155) = -2.323$, $p = .021$ and $t(107) = -2.021$, $p = .046$, respectively); for illegal access to IT systems no significant statistical difference can be found ($t(104.43) = -1.941$, $p = .055$).
- Privacy: as far as businesses' ability to maintain private data is concerned, the harm arising from the three types of cybercrime is not significantly different in the two waves (illegal access to IT systems: $t(202) = -0.835$, $p = .405$; data system interference: $t(154) = -0.478$, $p = .633$; cyber extortion: $t(105) = -1.896$, $p = .061$).

The comparison of the percentages of businesses assessing some harms as serious, or more, also reveals a few other considerable changes that are however not found significantly different by our significance tests. In particular, the percentages of businesses perceiving serious or more harms to the internal operational activities and services to customers following the only/last incident of cyber extortion have grown considerably from the first (21.2% and 10.8%) to the second wave (28.3% and 17.3%, respectively). A large percent increase is also reported for harm to internal operational activities resulting from only/last incidents of data/system interference: while 18.3% of the businesses rated such harm as serious or more in the first wave, the same ratings were selected by 25% of the victimized businesses in the second wave. Our significance tests, though, do not find these changes statistically significantly different because of the low absolute number of units giving such scores and/or because our tests focus on the mean scores, rather than on the percentages.

Table 34. Businesses' assessments of the severity of the harms caused to other interest dimensions by the cyber incidents suffered

| Aspect | Type | Wave | Harm | | | | | |
|---------------------------------|--------------------------------|------|------------|------------|------------|------------|-----------|--------------|
| | | | None | Marginal | Moderate | Serious | Grave | Catastrophic |
| Services to customers | • Illegal access to IT systems | W1 | 69 (51.9%) | 33 (24.8%) | 20 (15.0%) | 7 (5.3%) | 4 (3.0%) | - |
| | | W2 | 39 (57.4%) | 16 (23.5%) | 7 (10.3%) | 3 (4.4%) | 3 (4.4%) | - |
| | • Data/system interference | W1 | 50 (44.6%) | 26 (23.2%) | 25 (22.3%) | 9 (8.0%) | 2 (1.8%) | - |
| | | W2 | 9 (20.0%) | 16 (35.6%) | 9 (20.0%) | 8 (17.8%) | 3 (6.7%) | - |
| | • Cyber extortion | W1 | 30 (46.2%) | 20 (30.8%) | 8 (12.3%) | 2 (3.1%) | 3 (4.6%) | 2 (3.1%) |
| | | W2 | 14 (30.4%) | 13 (28.3%) | 11 (23.9%) | 6 (13.0%) | 2 (4.3%) | - |
| | • Cyber espionage | W1 | 1 | 3 | 2 | 1 | - | 1 |
| | | W2 | 13 | 4 | 4 | 5 | 1 | - |
| | • Internet fraud | W1 | 16 | 6 | 1 | 3 | 2 | - |
| | | W2 | 14 | 7 | 3 | 2 | 2 | 1 |
| Internal operational activities | • Illegal access to IT systems | W1 | 47 (33.3%) | 42 (29.8%) | 32 (22.7%) | 10 (7.1%) | 9 (6.4%) | 1 (0.7%) |
| | | W2 | 27 (39.1%) | 20 (29.0%) | 13 (18.8%) | 4 (5.8%) | 4 (5.8%) | 1 (1.4%) |
| | • Data/system interference | W1 | 22 (18.3%) | 39 (32.5%) | 37 (30.8%) | 15 (12.5%) | 6 (5.0%) | 1 (0.8%) |
| | | W2 | 4 (9.1%) | 14 (31.8%) | 15 (34.1%) | 8 (18.2%) | 3 (6.8%) | - |
| | • Cyber extortion | W1 | 13 (19.7%) | 28 (42.4%) | 11 (16.7%) | 4 (6.1%) | 7 (10.6%) | 3 (4.5%) |
| | | W2 | 4 (8.7%) | 14 (30.4%) | 15 (32.6%) | 9 (19.6%) | 4 (8.7%) | - |
| | • Cyber espionage | W1 | 1 | 3 | 2 | - | 1 | 1 |
| | | W2 | 6 | 9 | 5 | 4 | 2 | 1 |
| | • Internet fraud | W1 | 13 | 8 | 4 | 2 | 1 | - |
| | | W2 | 12 | 7 | 5 | 3 | 1 | 1 |
| Reputation | • Illegal access to IT systems | W1 | 66 (48.9%) | 43 (31.9%) | 14 (10.4%) | 8 (5.9%) | 4 (3.0%) | - |
| | | W2 | 31 (44.9%) | 17 (24.6%) | 7 (10.1%) | 5 (7.2%) | 8 (11.6%) | 1 (1.4%) |
| | • Data/system interference | W1 | 51 (45.1%) | 37 (32.7%) | 16 (14.2%) | 6 (5.3%) | 3 (2.7%) | - |
| | | W2 | 11 (25.0%) | 19 (43.2%) | 7 (15.9%) | 3 (6.8%) | 4 (9.1%) | - |
| | • Cyber extortion | W1 | 37 (57.8%) | 17 (26.6%) | 5 (7.8%) | 3 (4.7%) | 1 (1.6%) | 1 (1.6%) |
| | | W2 | 19 (42.2%) | 11 (24.4%) | 9 (20.0%) | 1 (2.2%) | 4 (8.9%) | 1 (2.2%) |
| | • Cyber espionage | W1 | 1 | 3 | 2 | 1 | - | 1 |
| | | W2 | 10 | 3 | 7 | 3 | 2 | - |
| | • Internet fraud | W1 | 14 | 8 | 2 | 3 | 1 | - |
| | | W2 | 9 | 7 | 6 | 3 | 1 | 2 |
| Privacy | • Illegal access to IT systems | W1 | 66 (48.9%) | 34 (25.2%) | 22 (16.3%) | 5 (3.7%) | 8 (5.9%) | - |
| | | W2 | 28 (40.6%) | 23 (33.3%) | 9 (13.0%) | 4 (5.8%) | 4 (5.8%) | 1 (1.4%) |
| | • Data/system interference | W1 | 64 (57.7%) | 27 (24.3%) | 11 (9.9%) | 4 (3.6%) | 5 (4.5%) | - |
| | | W2 | 25 (55.6%) | 9 (20.0%) | 7 (15.6%) | 2 (4.4%) | 2 (4.4%) | - |
| | • Cyber extortion | W1 | 34 (55.7%) | 16 (26.2%) | 6 (9.8%) | 2 (3.3%) | 1 (1.6%) | 2 (3.3%) |
| | | W2 | 16 (34.8%) | 14 (30.4%) | 8 (17.4%) | 6 (13.0%) | 1 (2.2%) | 1 (2.2%) |
| | • Cyber espionage | W1 | 2 | 2 | 1 | 1 | - | 1 |
| | | W2 | 11 | 5 | 3 | 5 | 2 | - |
| | • Internet fraud | W1 | 15 | 6 | 3 | 2 | 1 | - |
| | | W2 | 12 | 7 | 6 | 1 | 2 | 1 |

4.2.3. Government

In this paragraph, we discuss our empirical results with regards to the impact of cybercrime on the Belgian federal government. First, we present the results of our analysis of the answers of the Belgian federal government to parliamentary questions concerning the impact of cybercrime. Secondly, we present the result of the interview with the representative of the Belgian federal government.

4.2.3.1. Analysis of Parliamentary Questions

Here we summarize the cybercrime situation during the year 2015 as experienced and subsequently reported by the Belgian Federal Government in January 2016. This overview is based on a qualitative data analysis performed on the responses to a parliamentary question, posed by Nele Lijnen, Member of Parliament for the Flemish Liberal party Open VLD on January 14th, 2016. The Q&As were retrieved from the website of the Belgian Chamber of Representatives in April 2017 by using the Eurovoc-descriptor 'Computercriminaliteit' as a search term. At the moment this data was collected, for our purposes, Mrs. Lijnen's question was the only parliamentary attempt that was elaborate and profound enough to make a systematic analysis possible; it provided us with the opportunity to take a timeframe of exactly one calendar year (i.e., 2015) into consideration. At the time the data was collected other Q&As on the topic could be retrieved as well by making use of the above mentioned Eurovoc-descriptor. However, for several reasons, this data was considered ineligible for the purpose – which was primarily aimed at complementing the data that was supposed to be gathered by means of the government survey targeting the Federal Public Services. Questions posed by parliamentarians that were not part of our scope included unanswered questions (e.g. questions on the victimization of Belgian newspapers), or where the answers were not entirely relevant for the analysis due to their fragmentary and/or superficial nature (e.g. questions on the victimization of government agencies spanning a timeframe of four years, without further specification). Well aware of the fact that cybercrime remained a topical subject, Member of Parliament Lijnen sent out a questionnaire with seven questions, among which sub-questions on the incidence of cyber attacks, the type of the attack and their impact.

This set of questions was sent to – and subsequently answered by – a group of 18 Ministers and Secretaries of State belonging to the Belgian Federal Government. The respondents included (in order of discussion): the Prime Minister; the Minister of Employment, Economy and Consumer Affairs (also entrusted with Foreign Trade); the Minister of Security and the Interior (also entrusted with Buildings Agency); the Minister of Development Cooperation, Digital Agenda, Telecom and Postal Services; the Minister of Foreign and European Affairs (also entrusted with Beliris and Federal Cultural Institutions); the Minister of Justice; the Minister of Social Affairs and Public Health; the Minister of Pensions; the Minister of Finance (also entrusted with Tax Fraud); the Minister of Energy, Environment and Sustainable Development; the Minister of Defense (also entrusted with Civil Service); the Minister of Budget (also entrusted with National Lottery); the Minister of Mobility (also entrusted with Belgocontrol and the National Railway Company of Belgium); the Minister of Small Businesses, Self-employment, Small and Medium-sized Enterprises, Agriculture and Social

Integration; the Secretary of State for Foreign Trade; the Secretary of State for Asylum Policy and Migration (also entrusted with Administrative Simplification); the Secretary of State for the Fight against Social Fraud, Privacy and the North Sea; and the Secretary of State for Combating Poverty, Equal Opportunities, Disabled People and Science Policy (also entrusted with Larger Towns).

- Preliminary Considerations

When asked about how often the government entities under their authority were victimized by cybercriminals in 2015, the interviewed government officials consistently described cybercrime related incidents as rather infrequent and inconsequential. However, these descriptions should be interpreted with caution considering that only a handful of organizations and institutions, such as the Chancellery of the Prime Minister, Smals, CERT and the CCB, seem to have an overview of the incidence of cybersecurity in the Belgian public sector. Almost all respondents acknowledged that some security incidents may slipped through the net of detection, or had not been recognized as such. Therefore, most federal departments and their underlying institutions and public services seem to operate according to a so-called “presumed breach”-reflex. For instance, some respondents (e.g. the Minister of Finance) recognized the existence of some types of malware that are very hard to detect and therefore may have led to unnoticed information leakages. A similar statement can also found in the answer of the Minister of Pensions. He stated that “traditional firewalls and antivirus-software have increasing difficulties in detecting malicious email-attachments.” However, a minority of the respondents explicitly stated that it would seem “unlikely”, “highly unlikely” or “rather unrealistic” to them that cybersecurity incidents were able to go unnoticed, while Belspo simply stated that “there was no evidence that there were attacks directed at their systems that went unnoticed.” Information on the actual impact of actual incidents was only (or could only be) reported in a minority of the 18 answers.

It should be borne in mind, however, that solely based on the analysis of the Q&A’s at hand, it is impossible to determine whether these observations mainly have to do with issues of confidentiality, or whether they possibly reflect a lack of registration capacities (or the felt need to do so), or whether they result from inadequate communication between the competent authorities in early 2016. To rule out some of these assumptions, it is of utmost importance that a scientific data-collection exercise be undertaken at the level of the Belgian federal government, and that this endeavor receive the complete support of the competent authorities.

- The Statements of the Single Government Entities

The first answer presented here was given by the Belgian head of government: the Prime Minister . He stated that all incidents (“not only the security incidents, but also all the other incidents”) are systematically recorded and followed up by means of the ICT Shared Serviceticketing-system. Based on the data at his disposal, he declared that in 2015 on average two or three “security incidents” were recorded and subsequently dealt with each month. With regard to 2015, he reported six “specific security incidents” that targeted the Federal Public Service Chancellery of the Prime Minister and an additional 73 incidents with regard to all Shared Services. However, most incidents seemed to be of “minor importance”.

Alas, no further information could be retrieved regarding the specific nature of these incidents, nor regarding the impact they may have had. The Prime Minister continued by stating that since 2010 no loss of personal information was recorded and that there was not a single incident that had specifically targeted the databases of the ICT Shared Services, despite the “pressures” that were exerted on these services on a daily basis. However, the answer of the Prime Minister makes mention of a criminal complaint that was filed and related to a DDOS-attack targeting and temporarily taking down the website of the Chancellery of the Prime Minister in October 2015. Typically, if successful, such an attack results in what would be classified as an IT failure under our typology.

The Minister of Employment, Economy and Consumer Affairs (also entrusted with Foreign Trade) declared that his department had not been confronted with an incident of illegal access in 2015, but that it had to deal with the threat of computer viruses “et cetera” on a daily basis. Later on in his answer, he also speaks about a morbid growth of harmful ransomware, but without revealing whether or not his services have been impacted by this kind of malicious software and if so: to what extent. According to his knowledge, attacks (or attempts?) were on the rise, gaining complexity and also increasingly aimed at “specific servers directly under the control” of his department. In addition, and making his own contribution to the apparent secretiveness and blurry character of the cybercrime-situation at the Belgian federal level, he made reference to “one incident” which was at the time the subject of a formal judicial inquiry, while stating explicitly that he didn’t want to comment any further on this in order to respect the investigative secrecy. In a supplementary answer, the minister also shed light on the situation as it was experienced by the Federal Public Service Employment, Labor and Social Dialogue. At that time, this Federal Public Service was said to be registering attempts of attacks, mainly directed towards their mail server on a daily basis. The malicious mails that were targeting their mail server mostly consisted of ransomware. In this case too, no further information was or could be provided concerning the exact or relative complexity of this type of malware, nor with regard to the harmful potential of the attempts discussed. Fortunately, “up till now [January 2016], all these attempts were successfully parried by the firewall.” Yet, one other ray of hope: according to this minister, the missing information about cybercrime threats is now being collected by other organizations such as CERT, with which the Ministry collaborates closely.

The Minister of Security and the Interior reported no successful cyberattacks directed at the National Register of Natural Persons in 2015. However, he noticed a slightly increased rate when comparing the (unsuccessful) attempts with previous years. He stressed the growing complexity of the attacks, which were mainly targeting their web- and mail servers. To his knowledge, most attempts concerned malicious emails with a virus attached or a fraudulent web link inside, or concerned attempts to attack their webpages in order to provoke an IT failure. One of the other institutions under his authority - the Government Crisis Control Centre - had to deal with a ransomware-infection that initially encrypted some data present in the IT system. However, the targeted data was restored from a backup within 24 hours. The Buildings Agency, as well as the Federal Agency for Nuclear Control (FANC) – two other institutions under his control – reported no successful attempts or malicious actions that could be attributed to hackers or cybercriminals. The Central Services and VPS was also

targeted by a DDOS-attack originating from the notorious hackers collective DownSec in October 2015; as a result of this, the official website of the Interior Department (www.ibz.be) suffered from downtime, or according our typology from an IT-failure, for a couple of minutes. In this case, a criminal complaint was filed.

The response submitted by the Minister of Development Cooperation, Digital Agenda, Telecom and Postal Services indicates that several of his services were confronted with virtual threats in 2015. The Federal Public Service for Information and Communication Technology (Fedict) was targeted five times by cybercriminals who launched DDOS-attacks against their services (which generally lead to an instance of IT failure, according to our typology). Unfortunately, more information about the specific nature of the attacks was lacking in the given answer with the exception of the statement that the attacks were of “limited strength”. Reading the answer carefully, one can conclude that these attacks resulted in the interruption of the services provided by this federal public service, but only for “a short period of time”, compared to the impact of similar attacks in the years before. The Minister also declared to the Parliament that no information had been lost as a result of the incidents and that Fedict was able to successfully avert “other attempts” (again without specifying the exact nature of these) on a regular basis. Oddly enough, in his answer to the Parliament, this Minister quoted verbatim the statement of the Minister of Foreign and European Affairs regarding the cybercrime situation experienced by the Federal Public Service for Foreign Affairs ; this is despite the fact that the Minister of Development Cooperation, Digital Agenda, Telecom and Postal Services has nothing to do with the entities under the auspices of the Minister of Foreign and European Affairs. With regard to the Belgian Institute for Postal Services and Telecommunications (BIPT), the appropriate Minister stated that this institute was not in possession of numerical data on cyber incidents. Yet, this Minister was able to tell (notwithstanding the apparent lack of data on the subject) that some of the computers of employees got infected with a virus “in a number of cases”, but that these problems each time were solved by the IT service of the institute. Further information on the impact could not be retrieved from the answer.

The answer of the Minister of Foreign and European Affairs indicates that in 2015, there were three intrusions in the IT systems belonging to the entities under his control. These intrusions were, to his knowledge, not specifically targeting his department. One of these “intrusions” involved an incident where ransomware was involved (which could lead to cyber extortion according to our typology), while another incident involved a banking Trojan aimed at stealing banking credentials (which would be classified as cyber-espionage according to our typology). The final incident he referred to, was the use of phishing (what we consider as a technique that can be used to commit a wide range of cybercrimes). According to the Minister, “these attacks were discovered timely”, so they resulted only in limited impact, without further explanation apart from the conclusion that there had not been any loss of information. He also mentioned “numerous attempts of hacking on a daily basis” that have systematically been detected by different layers of security, adding that he could not avoid the impression that his department, as well as all the other federal public services, were increasingly confronted with (attempts of) highly sophisticated cyberattacks.

The Minister of Justice provided the author of the question only a brief answer. To his knowledge, the IT infrastructure of the Federal Public Service under his authority, had not been confronted with cybercrime in 2015. However, he also stated that he did not want to rule out the possibility that some incidents would have remained unnoticed, given the existence of media reports on cybersecurity incidents at the level of internet service providers.

The next answer that was analyzed originated from the Minister of Social Affairs and Public Health . This minister stated that the services of the Federal Public Service for Social Security have not been victimized by hackers or cybercriminals in 2015. However, there were some unsuccessful and thus “harmless” attempts, which targeted the website of the Federal Public Service – a website that is hosted externally by Smals and Fedict . The Federal Public Service for Health, Food chain safety and Environment encountered a series of ten “security incidents” in 2015, which could be considered as “malicious attacks from the outside”. Reading the answer carefully, one can learn that in most of the cases it concerned working stations which were infected by malware, while two incidents involved infections with ransomware and two other incidents involved infections with a cryptolocker. The impact of the latter four incidents was “limited”, since the contaminated software and the contaminated data files were restored from backup. This Federal Public Service also detected an attempt to identity theft (without giving further specifications, apart from the fact that it appeared to be a new type of attack) and parried an exploit-attack successfully (an attack-technique that can be used to perform a wide array of computer crimes as included in our typology). It is worth noting the Minister’s statement that the registered incidents showed that the quality of the attacks is on the rise and that they were in most instances based on the technique of social engineering, adding to the credibility of the attempts and heightening the chances that such attempts would prove successful sooner or later.

The Minister of Pensions started his answer by stating that the National Pension Office (RVP) had not been the victim of a successful cyberattack by hackers or cybercriminals in 2015. Yet, he acknowledged that two “major” cryptolocker-attacks (what could lead to what is subsumed under cyber extortion according to our typology) were initially successful and resulted in “damage”: a shared drive of a file server got encrypted. Nevertheless, in both cases, the damage was mitigated by restoring the contaminated files from backup. No further indications about the impact of these incidents were given. The good news is that during the last four months of 2015, a total of 708,167 presumed cyberattacks (targeting the RVP) have been averted. In a majority of these cases (75%) the alerts resulted from software bugs, while the remainder of the alerts comprised of automatic data requests “aimed at the gathering of information on the structure of the RVP.” The National Civil Servant’s Pension Office (PDOS), another entity under the aegis of this Minister, also became the victim of a successfully executed cyberattack where ransomware (that was attached to an email) was installed and encrypted “some” data files. But also in this case, the contaminated files were restored from backup. No further indications about the impact were reported, apart from the statements that “no theft of confidential data” had taken place and that the functioning of the Office had not been impaired. Nevertheless, there seem to exist differences in the perception of the RVP and the PDOS regarding their detection capabilities. Although both offices fall

under the competence of the same Minister, the RVP stated that there was a reasonable chance that a couple of cyber attacks would remain undetected, whereas the PDOS considered it implausible that instances of cybercrime would be able to stay under their radar.

The Minister of Finance had no knowledge of cybercriminals who successfully obtained illegal access to the IT system of his department in 2015, although he acknowledged that the department constantly had to face a steady stream of malware-attacks attempts. Luckily, each month 2000 to 3000 attempts were successfully neutralized by the security measures in place at the time, resulting in 'no serious infections with a computer virus.' Given this formulation, the question whether or not they had to deal with other than 'serious' infections in 2015, remains unanswered.

In response to the question, the Minister of Energy, Environment and Sustainable Development (rightly) referred to the answers given by the Minister of Employment, Economy and Consumer Affairs (with regard to the experiences of the Federal Public Service for Economy, S.M.E.s, Self-employed and Energy) and those given by the Minister of Social Affairs and Public Health (with regard to the experiences of the Federal Public Service for Health, Food chain safety and Environment). He further declared that with regard to the Federal Institute for Sustainable Development he is dependent on the Federal Public Service Chancellery of the Prime Minister for the administrative and logistic support. Therefore, this Minister referred to the answer given by the Prime Minister. As is the case in several other referrals, no specific information with regard to the Federal Institute for Sustainable Development could be retrieved from that answer.

The Minister of Defense declared to Parliament that there has not been a single attack targeted at the department's website in 2015, nor to those of the parastatals in the field of defense. He continued on the subject by stating that "the total amount of cyberattacks has not increased during the timeframe 2010-2015", without elaborating on the subject in terms of the types of attacks, their impact or frequency. This minister is also entrusted with matters related to Civil Service. With regard to this domain, he explains that the IT infrastructure (e.g. firewalls) was under attack, daily, by cyber criminals, but that these attempts were parried "as a rule". However, he acknowledges that Selor, the federal administration selection bureau, became the victim of a minor SQL-injection type of attack in August 2015 (which, if successful, leads to an IT failure according to our typology). Since it was only a minor incident, it did not take long before it was discovered and the weaker parts of the application that formed the target of the attack were remediated almost immediately. However, no information was or could be given concerning the actual impact, except the fact that it was "very limited". All the departments within Selor remained operational and their services remained accessible to the public, while there was no damage reported to the physical infrastructure either.

The Minister of Budget reported that the services under his competence had to deal with 2 to 3 security incidents each month, without providing further details about these incidents. The reason for this lies probably in the fact that he also mentioned that these security incidents

were registered and dealt with by the earlier mentioned IT Shared Services. Attempts to provoke an IT-failure due to data traffic directed against the webpages were prevalent, but only one successful attempt in October 2015 was quoted as an example.

The Minister of Mobility (also entrusted with Belgocontrol and the National Railway Company of Belgium) was very brief in his answer. Asked how many times his services and/or administrations became the victim of hackers or cybercriminals in 2015, he replied: "Never."

The Minister of Small Businesses, Self-employment, Small and Medium-sized Enterprises, Agriculture and Social Integration provided the author of the question with a rather extensive answer. In 2015, the Federal Agency for the Safety of the Food Chain (FAVV) was targeted by cybercriminals who tried to gain illegal access, but all these attempts (2382) were parried by their firewall. The execution of malicious code, what constitutes a technique in order to provoke what is subsumed under "an IT failure" in our typology, was prevented 135 times. The FAVV also had to deal 4154 times with failed attempts to take their website down (what would also constitute an IT failure under our typology). Although the organization Smals performs a preliminary scan for malicious incoming emails at the level of the central federal mail server, still 0,1% of the mails were blocked at the level of the FAVV because they contained a virus or other malicious code. The Veterinary and Agrochemical Research Centre (CODA) did not make note of any cyberattacks at all in 2015, as stated by the minister. The National Social Insurance Institute for the Self-employed (RSVZ) was not confronted with any malicious actions originating from hackers or cybercriminals in 2015, according to the knowledge of this Minister. The Public Planning Service for Social Integration did not encounter "an instance of hacking that influenced their operations or that left behind visible traces." However, due to the imprudence of an employee, the service became the victim of ransomware once in 2015, as a result of which the contaminated files had to be restored from backup. No further indications about the impact were mentioned by the Minister in relation to this incident, apart from the fact that they decided not to file a criminal complaint against persons unknown due to the "vague and universal nature" of the incident.

The Secretary of State for Foreign Trade seemed unable to provide the Parliament with the requested information, but referred the author of the question to the Minister of Employment, Economy and Consumer Affairs (also entrusted with Foreign Trade) for a more comprehensive and detailed picture instead.

The Secretary of State for Asylum Policy and Migration was the next in line to report on the experiences of his services with cybercrime. According to him, neither the Office of the Commissioner-General for Refugees and Stateless Persons (CGVS), nor the Council for Alien Law Litigation (RvV) were victims of cybercrimes in 2015. The Immigration Office (DVZ), on the contrary, had a brief encounter in October with the earlier mentioned group DownSec; the Offices' website was inaccessible for a few minutes as a result of the actions of this nefarious group. Also as a result of this incident, a criminal complaint was filed against the collective. Fedasil, the federal institution providing refugees with material support, was targeted five times by cybercriminals. Some further clarifications were given regarding the

latter. The first was that these attacks “were not aimed directly at the Agency.” The second clarification, while still keeping us in a state of relative uncertainty concerning the exact impact of the attacks, was that the attacks were performed by means of the newest cryptoware-techniques used by cybercriminals at the time, which led to the significant increase of attacks the agency was confronted with compared to previous years. A statement of this Secretary of State further shows the poor state of the Belgian Federal IT landscape at least until 2015. Accordingly, the IT system of the Agency for Administrative Simplification was managed by the Chancellery of the Prime Minister and therefore the Secretary of State was unable to assess the cybercrime-situation of this agency despite the fact that the agency is under his control.

The Secretary of State for the Fight against Social Fraud, Privacy and the North Sea, in his written answer, declared to Parliament that he had no Federal Public Services that fell exclusively under his control. Therefore he referred to the answers of the relevant Ministers and Secretaries of States who received the same question from the Member of Parliament.

The answer of the Secretary of State Combating Poverty, Equal Opportunities, Disabled People and Science Policy concludes the list. This Secretary reported that his services have not been impacted greatly by cyber criminals (e.g. Public Planning Service for Social Integration). However his statement is worth elaborating on. In his answer, the Secretary cited frequent, albeit, largely unsuccessful attempts to gain illegal access. On a few occasions in 2015, cyber criminals attacked several websites that fall under his competence. While the majority of these attempts were unsuccessful, two attempts resulted in an IT failure due to data traffic. Concerning these two successful attacks, no further information was available since these website were hosted externally, as is the case with ALL the websites of the Federal Government. One of his institutions (i.e. the State Archives of Belgium) was confronted with 3 successful attempts to gain illegal access and related to this there were some demands for an amount of money on behalf of the criminals (without giving any further specifications). This institution also had to deal with an instance of cyber extortion: the ransomware virus Cryptolocker was installed on the IT system, but eventually no harm was done since the infected files could be easily restored from a back-up. Another institution under his authority, the Belgian Science Policy Office, had exactly the same experience the Cryptolocker virus, however, in addition some harm to the operational integrity of the department was reported in this case.

4.2.3.2. Selected interviews

- Cybersecurity

First of all, the interviewee indicated that each ministry and other federal agency has its own cybersecurity strategy. Hence, there are differences between the different ministries and agencies with regards to the organization of cybersecurity. For example, some decide to fully outsource it, whereas others decide to organize it themselves (often because of mistrust in external organizations).

Notwithstanding the foregoing, in the interviewee’s view most ministries and other federal agencies implement similar technical cybersecurity measures. Standard measures applied

are firewalls, anti-virus software, anti-phishing software, anti-spam software and anti-back-up software. More advanced measures, such as measures against Advanced Persistent Threats (APT), however, are too expensive for most ministries and other federal agencies to be implemented. As regards procedural cybersecurity measures (i.e., updates of software, browser and operating system etc.), there are some differences between the different ministries and other federal agencies, but the small updates and patches do not cause problems for most of them. Larger patches and updates, such as moving to a new operating system, are more likely to result in problems.

The interviewee also mentioned that, in the last couple of years, ministries and federal agencies have started to exchange expertise and explore possibilities for joint initiatives. These joint initiatives can go from simply concluding the same contracts with external organizations – which is done quite often – to using the exact same platform – which is done only by a few. However, some ministries and federal agencies are not open at all to joint initiatives, because they want to keep full control over the cybersecurity of their service. Hence, they are still operating more or less on an island as far as the organization of cybersecurity is concerned.

Finally, as regards training of federal government employees, the interviewee mentioned that the CCB organizes cybersecurity courses for the members of the ministries (or “FOD”), but not for the members of Public Social Security Services (or “OISZ”) and Federal Public Utility Services (or “ION”). Employees belonging to one of the latter two types of agencies might be interested in these courses as well, but due to budgetary constraints, they are excluded. In addition, according to the interviewee, only a limited number of employees of each ministry can participate in these courses. Hence, in his view, these courses are aimed at training the most important employees of each ministry, who would then have to share their expertise with their colleagues. An important caveat is that the CCB offers these courses, but each service autonomously decides whether they want to make use of them or not.

- Cybercrime

Although the interviewee stressed that he did not have a full picture of the cyber incidents suffered by the ministries and other federal agencies, he reported that a couple of years ago, some ministries were confronted with (D)DOS attacks and, as a result, an anti-(D)DOS infrastructure was established. Since then, all (D)DOS attempts have been blocked by the security system. The interviewee also mentioned that each ministry and other federal agency was recently confronted with some minor ransomware incidents. Furthermore, he said that attempts of illegal access to IT systems occur all of the time, but that nearly all of them are blocked by the security system. The interviewee could provide no information with regards to cyber espionage and cyber fraud.

Next, the interviewee supposed that at least the CCB and CERT.be are informed only of ‘substantial’ incidents (e.g., the large (D)DOS attacks that have happened). Hence, minor cyber incidents (e.g. ransomware on a local computer) are not likely to be reported. He noted that the new GDPR (European Parliament and the Council of the European Union, 2016) has

generated obligations to report certain cyber incidents that imply a personal data breach to the Data Protection Authority and the data subject.

As regards the impact of cyber incidents, the interviewee hypothesized that future incidents would have no or only limited impact because of the recent investments in cybersecurity. (D)DOS attacks would have the highest impact, according to him. In his view, non-material harms are incident-specific. For example, cyber espionage would primarily affect the interest dimensions of privacy and reputation, whereas (D)DOS attacks would be most harmful to the services to citizens and ransomware incidents would harm both the services to citizens and internal operational activities. However, he also mentioned that very serious incidents, such as the (D)DOS attacks of a couple of years ago generated serious harm for all interest dimensions.

For the coming years, the interviewee supposed that the number of cybercrime incidents would increase, but also that the impact of the incidents that are hot today (e.g. ransomware), would decrease as a result of past and future countermeasures. According to the interviewee, a similar evolution was recorded after the (D)DOS attacks that happened a couple of years ago: following the establishment of adequate anti-(D)DOS infrastructure in response to these attacks, later attacks were largely blocked by the security system, and so did not result in negative impact.

Finally, the interviewee mentioned two steps that could be taken to improve the cybersecurity of ministries and other federal agencies. First, he stressed that exchanging information and learning from each other's good practices would allow them to increase their cybersecurity. According to him such practices have become more common the last couple of years (see earlier). Secondly, merging the ministries' and agencies' security budgets together in one budget – and consequently centralizing cybersecurity – would allow each of them to increase their cybersecurity level. Now, certain more advanced cybersecurity measures cannot be implemented by the ministries and other federal agencies due to budgetary constraints, but in a centralized cybersecurity system, these measures could be implemented. However, the interviewee mentioned that there is currently very limited support for this centralization idea. In addition, even if cybersecurity would be centralized, additional budget would be needed to implement several advanced measures.

4.2.4. Forecast

For each question we provide the answers followed by a brief discussion. For the first questions, we have a total of 261 respondents. This number dropped to 255 for the last question.

- *How is the effectiveness of your security program evaluated?*

Table 35 Response to question 1

| | Number | Percentage | Cumulative percentage |
|-------------------------------------------------------|--------|------------|-----------------------|
| Penetration testing bij ICT personnel in your company | 30 | 11% | 11% |
| Penetration testing by external consultants/company | 85 | 33% | 44% |
| By Vulnerability assessment | 20 | 8% | 52% |
| Not | 31 | 12% | 64% |
| By Risk Assessment | 71 | 27% | 91% |
| Others | 24 | 9% | 100% |

Only 12% of the respondents' answers that their security program is not evaluated. This indicates a widespread concern about cyber criminality and also a concern that the implemented security measures might not be sufficient. One third of the respondents pays external people to do penetration testing, and 35% claims to perform vulnerability or risk assessment. This means that a considerable amount of time and money are spent on the evaluation of the security program.

- *What IT or security certifications does your company have? Are there any that the company is pursuing within a time frame of two years?*

All in all a fair number of companies claims to have or to be pursuing a security-related certification. The companies answering that they have a firewall or that they are using SSL may have misunderstood the question.

- *Does your company have an insurance to protect itself from cybercrime and if yes how much does your company pay for it?*

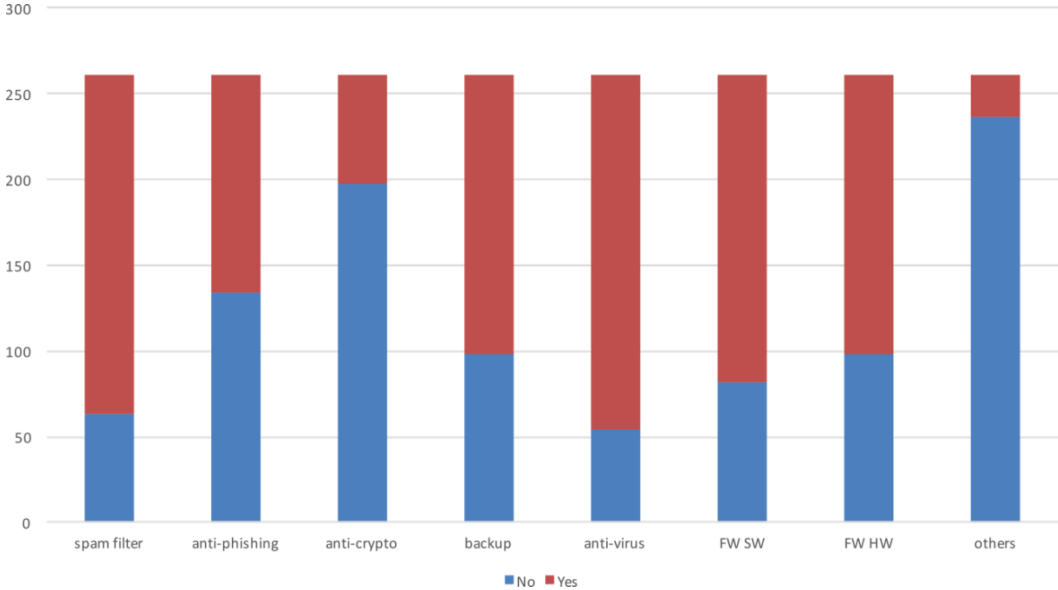
Table 36 Response to question 3

| | Number | Percentage | Cumulative percentage |
|--------------------------------|--------|------------|-----------------------|
| No insurance | 222 | 87.4% | 87.4% |
| Less than € 500 | 2 | 0.8% | 88.2% |
| Between € 501 and € 1,000 | 4 | 1.6% | 89.8% |
| Between € 1,001 and € 2,000 | 3 | 1.2% | 90.9% |
| Between € 2,001 and € 5,000 | 3 | 1.2% | 92.1% |
| Between € 5,001 and € 10,000 | 2 | 0.8% | 92.9% |
| Between € 10,001 and € 20,000 | 2 | 0.8% | 93.7% |
| Between € 20,001 and € 50,000 | 1 | 0.4% | 94.1% |
| Between € 50,001 and € 100,000 | 2 | 0.8% | 94.9% |
| More than € 100,000 | 8 | 3.1% | 98.0% |
| Amount not entered | 5 | 2.0% | 100 % |

It appears that the vast majority of the companies does not believe in the added value of an insurance against this risk.

- *Has your company in the last 12 months acquired any of the following tools to protect the company computers and electronic data? Indicate all that apply.*

Figure 11. Response to question 4



Not surprisingly, the most popular tool is the anti-virus software, although it is worrying that more than 50 respondents indicate that they did not acquire any. The least popular tools are anti-phishing software and anti-cryptolocker software. This could be due to a lower awareness of the threats imposed by these malware, or to the fact that such tools are less available.

- *How many man-hours per week does your company invest in the prevention of cybercrime?*

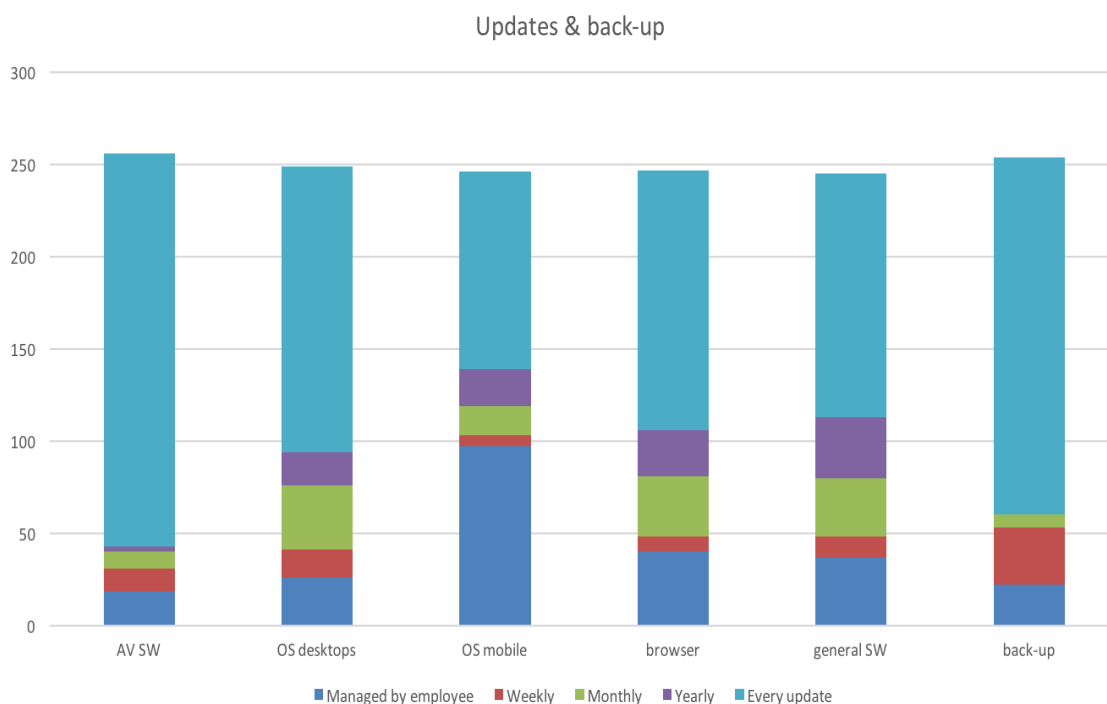
Table 37 Response to question 5

| | Number | Percentage | Cumulative percentage |
|-------------------|--------|------------|-----------------------|
| None | 44 | 17% | 17% |
| Less than 1 | 87 | 34% | 51% |
| Between 1 and 10 | 81 | 32% | 83 % |
| Between 11 and 50 | 20 | 8% | 91% |
| More than 51 | 23 | 9% | 100% |

Half the companies spend no time or less than 1 man-hour per week on the prevention of cybercrime. This result nicely completes the answers to Question 1. 9% of the respondents claims that their company spends more than 51 hours every week in the prevention of Cyber Crime. Even though we can expect that it is exactly the larger and more security-aware companies who took the effort of filling out our survey, this result still indicates a significant investment of time and money in countermeasures.

- *What does your company do to keep itself updated in the prevention of cybercrime?*

Figure 12. Response to question 6



We consider the answer managed by employee as an indication that this action is not really followed up by the company. In particular for the mobile devices, companies do not seem to be worried about Cyber Crime, since about 40% of the companies leave this to the individual employees. For the updates of anti-virus software and back-up operations, most companies ensure that this happens very regularly.

In conclusion, most respondents are aware that cybercrime can be a threat to their assets and take several countermeasures, like making regular back-ups, updating the OS regularly and keeping the anti-virus software up-to-date. Only a small minority takes more advanced (more expensive, more time consuming) countermeasures like going through a certification process and buying insurance.

4.3. Policy Recommendations

Based on the results, we formulate following recommendations. We split up these recommendations into general recommendations and recommendations particularly for Belgian citizens, businesses and government agencies.

4.3.1. General

- Pursue a differentiated approach towards cybercrime, in research, policy-making and cybersecurity strategies. Given the differences in the incidence and impact of different cybercrime types, it is necessary to develop a differentiated approach in studying, and dealing with, cybercrime. Specifically, time has come to agree upon, and consistently adopt, a thorough and harmonized typology of cybercrime for research and practical public and private cybersecurity purposes. We need to acknowledge that cybercrime consists of different types that are committed with (partially) different modalities and motivations by different subsets of perpetrators, occur with different frequencies, generate different harms for their immediate victims and other bearers and are likely to be at least partially susceptible to different types of preventive measures.
- Adopt a broad conceptualization of cybercrime impact, including non-material harms and multiple bearers. Reducing impact to monetary costs would give a partial, limited picture of the impact of cybercrime. A valid assessment of the impact of cyber- (and other) crimes has to complement an estimation of the monetary costs (i.e., harms to material support) with an assessment of non-material harms. A full assessment ought also to consider the harm cybercrimes generate for indirect bearers of harm.
- Systematically and empirically assess the harms of cybercrimes. Only through an empirical, systematic harm assessment it is possible to assess whether a new activities is harmful enough to be criminalized, to establish rational, evidence-informed goals for crime prevention and control, to set and mete out proportionate sentences, to deliver restorative programs that take the different harms suffered into account. Ultimately, only through an empirical, systematic harm assessment it is possible to find out if criminal policy and preventive interventions helps reducing harm to protected interests, rather than just crime, and to envisage the optimal package of interventions for such an end.
- Expand research on cybercrime prevention and its effectiveness. As prevention is resorted much more frequently than repression in dealing with cybercrime, it is of crucial importance to find out which preventive measures are most (cost-)effective and which effects, including the unintended ones, the different measures produce. Moreover, such assessment could enable individuals, businesses, NGOs, and government agencies to identify the preventive measures that are most effectively tackle their vulnerabilities rather than blindly adopting the measures suggested by cybersecurity and consultancy companies.
- Keep cybercrime specificities into proper account. In conducting research on cybercrime and the related preventive and policy options, it is important to take the specificities of cybercrime into proper account: cybercrime processes are discrete,

non-stationary and have heavy-tailed distributions with black swan events (i.e., events that are random and unexpected). Therefore, a mere traditional statistical analysis—particularly when it relies on cross-sectional designs—might not always provide a firm basis for appreciating the evolution of cybercrime, its incidence or impact or for assessing the effectiveness of preventive measures.

- Collect longitudinal data on cybercrime victimization from representative samples. To reliably estimate cybercrime victimization and costs, assess their non-material harm and evaluate the effectiveness of preventive measures, it is necessary to collect data from representative samples of the population. In addition, cybercrime victimization surveys should adopt a longitudinal design, and follow the samples over a prolonged period of time. Only through a longitudinal design one can fully appreciate the interaction between these factors and the surrounding socio-economic and policy context (and make valid trend analyses that can be inferred to the population).
- Set up and fund long-term multidisciplinary teams. To collect and analyze complex data on cybercrime victimization and impact and their interaction with prevention and cybersecurity measures, multidisciplinary teams need to be set up and funded over an extended period of time. Other national governments and/or universities have already established permanent research and expert centers. If national and EU governments are serious about cybersecurity and want to have the related strategies informed by scientific and independent evidence, they have no alternative but start funding long-term multidisciplinary research consortia—or even better permanent institutes—devoted to the study of cybercrime and cybersecurity.
- Keep supporting existing initiatives like the Cyber Security Week and/or adding new initiatives that raise the public's awareness of cybercrime. As a general rule of thumb, cyber security must be built on strong foundations. There are a number of basic security measures that need to be taken and that can easily be taken. These can be communicated and learned through supporting courses, education for experts and low-entry trainings for daily users. It is important that trainings are done by knowledgeable professionals as much well-meant advice that is given for free, is actually not helpful or even hindering security.
- Investing with future developments of cyber security in mind can lead to an increased resilience against cybercrime. Investing in technical research can incubate the creation of innovative products and training methods. Investing in behavioral research can uncover (and fix) why users fail to adopted well-known good practices. Investing in new businesses with creative but effective solutions can provide new defenses against the increasing attack surfaces. Incentivizing companies to exert cautiousness when deploying Internet-of-Things applications; and keeping companies accountable for severe shortcomings forms a promising approach at dealing with this challenge. Finally, funding regularly performed pressure tests can quantifies the effectiveness of deployed defenses.
- Comply with and take into account the rights and obligations contained in data protection legislation when processing personal data. This includes the European GDPR and the Belgian law based thereon . As these laws contain a number of legal provisions relating to transparency, accountability, cybersecurity and the prevention

or mitigation of cybercrime, it is recommended that citizens, businesses and public institutions exercise their rights and fulfill their obligations.

4.3.2. Citizens

- Don't use one size-fits all methods in risk communication to citizens. Risk communication should be tailored to different kinds of internet users and different kinds of cybercrimes. Internet users react differently to different stimuli and are in need of different adaptations depending on previous behavior. (e.g. In more than 80% of the cases of victimization by hacking or malware carries there was no monetary cost. For scams, however, almost half of the victims do experience direct monetary costs. Scams made the least victims but caused the highest direct financial cost). We refer to D7.2 where recommendations for this risk communication are discussed in depth.
- Opportunity costs should be taken into account when setting up awareness campaigns. Next to monetary costs, cybercrime also results in opportunity costs, where internet users reduce their usage of the internet in fear of victimization. This opportunity cost is often marginalized, but affects all but the most experienced internet users.
- Defense costs make up a huge percentage of monetary losses caused by cybercrime, especially by less internet savvy people. These people should be informed and aided in setting up less costly (or free) defense systems, like the ones build in by operating systems.
- The least experienced internet users face a greater risk of being infected without being cognizant. Risk communication should focus on educating these less internet savvy people on what is and what isn't dangerous.
- To change the behavior of taking security measures, people should be informed of the severity of the cybercrimes and should be informed on the effectiveness of security measures.
- Subjective norm is an important predictor of taking security measures against cybercrime. Further research should incorporate subjective norm to a greater extent to measure what predictive value it has in protecting oneself against cybercrime. In turn, these results should be translated into adequate communication strategies.
- Pessimistic defensive internet users and inexperienced unknowing internet users experience the greatest risk and should be the first target group of risk communication. They are least aware of risks and or unsuccessful to effectively protect themselves.

4.3.3. Businesses

- Business should be made aware of their legal obligations with respect to ICT (GDPR, breach disclosure, ...).
- Given that website security technology evolves, an effort should be made to promote rapid adoption of protection technologies by businesses.
- Since large scale web security observation is feasible at low costs, it can be considered to offer this as a public service, to signal common issues.
- Smaller websites tend to adopt security features more slowly – therefore efforts should be primarily directed at SMEs.
- Efforts should not be spread evenly over businesses, but can be made more effective by focusing on specific sectors with low adoption rates.
- Complement victimization surveys with other data, such as businesses' (compulsory) reports of cyber victimization to government agencies notifications and/or face-to-face interviews. This allows the researchers to triangulate the assessments with other types of data and thus come to a more solid, "objective" harm assessment.
- Comply to the fullest extent possible with data protection legislation when processing personal data. This includes the European GDPR and the Belgian law based thereon . As these laws contain a number of legal obligations relating to cybersecurity and the prevention or mitigation of cybercrime, it is recommended that businesses seeking legal compliance do the following:
 - Adhere to the general data protection principles of lawfulness, data security, data minimization and purpose limitation. Following these general principles can prevent potential crimes and intrusions or minimize their impact in case an offense does take place;
 - Inform the persons whose data is being recorded, stored, processed or transferred ('the data subject') of their rights and provide them with sufficient information on certain modalities of the storage, usage and accessibility of their data, especially when requested by the persons involved;
 - Follow the requirements of data protection by design and by default in order to implement appropriate technical and organizational measures for the protection of the personal data collected, stored or processed;
 - Comply with the requirements on data security and the involvement of third parties for the processing of personal data. This includes, among others, measures of encryption, access controls, backup capabilities, and system integrity and confidentiality, as well as contractual obligations requiring similar standards when involving other actors in the processing of data;
 - Keep records and logs of the processing activities to, where possible, document the security measures taken to protect data as well as general information on access, storage and use;
 - Alert the Belgian DPA of any data breaches within the timeframe dictated by law. In certain instances, this alert should be extended to the persons whose data might have been affected by the intrusion;

- Where necessary, conduct a data protection impact assessment (DPIA) when the data processing is likely to result in high risks to the rights of natural persons. This is particularly relevant when new technologies are being used. When a business is legally required to conduct a DPIA, it must consider the possible implications of their processing activities and implement the necessary measures to avoid negative consequences. This includes security techniques to prevent illegal access to systems and data;
- Cooperate with the DPA to the fullest by providing all necessary information and complying with further requests;
- Take into account and follow any opinions, guidelines, codes of conduct or corporate rules presented by data protection authorities;
- If necessary, appoint a data protection officer and provide him or her with sufficient resources and discretion to monitor legal compliance with the abovementioned points and provide advice on data protection.

4.3.4. Government

- Stimulate the exchange of cybersecurity expertise and other information among the IT departments and staff members of government agencies operating at the same governmental level (e.g. between the different ministries and other federal agencies or between several cities) or at different governmental levels (e.g., between a federal or regional ministry and one or more cities). Through such an exchange, cybersecurity would no doubt become more (cost-) effective.
- Ensure that all government agencies in Belgium—irrespective of the level at which they operate—systematically register cyber incidents in the same standardized format. Nowadays, several government agencies do not even register incidents, and hence nobody knows for sure how frequently the Belgian government, with all its agencies, is confronted with cybercrime, let alone how frequently different cybercrimes occur or how serious their impact is. However, such a systematic, standardized registration, together with a thorough assessment of the vulnerabilities, risks and harm of different agencies, is crucial to organize cybersecurity in an effective way.
- Ensure that all government agencies in Belgium, irrespective of their governmental level, systematically report incidents to a central cybersecurity organization (such as the CERT). To encourage notification, the value added for the notifier should be improved (e.g., not only a message thanking him or her for the notification, but also a summary of what the central organization has done with the notification, and if possible tips about how to improve his or her agency's protection against cybercrime).
- Task the central cybersecurity organization with the preparation of annual reports giving an overview of the incidents reported during the previous calendar year, identifying future risks as well as sharing, and encouraging a debate on, best practices.

- Ensure that all government employees working with IT devices (hence the overwhelming majority of them) receive a basic cybersecurity training. Moreover, depending on their specific tasks, all government employees should be given the opportunity, be encouraged or even be required to participate in more specialized cybersecurity training, organized within or outside their government agency.
- Ensure that all government agencies have an adequate cybersecurity budget so that they can adopt the cybersecurity measures necessary to counter their specific risks of cyber victimization. Hence, if certain risks increase, they should also be able to increase the budget for cybersecurity, so that adequate measures to counter these risks can be taken. In any case, government agencies should always assess whether, given their particular vulnerabilities, certain cybersecurity measures are necessary.
- Centralize the organization of cybersecurity within the Belgian federal government. Nowadays, each ministry or federal agency is responsible for its own cybersecurity. Through centralization, cybersecurity would become much more (cost-)effective way for all ministries and other federal agencies. More concretely, the responsibility for the organization of basic cybersecurity measures could be given to a central organization (e.g., CCB), whereas more specific measures could still be the responsibility of the different ministries and other federal agencies.
- Reinforce the role of the CCB, by providing it not only with the means to organize basic cybersecurity measures for all ministries and other federal agencies, but also to open up its cybersecurity courses to all employees of the ministries and other federal agencies, and if possible to employees of regional and local governmental organizations. Hence, the CCB would ideally be the responsible for both basic cybersecurity measures and basic training of all Belgian government employees.
- Comply to the fullest extent possible with data protection legislation when processing personal data. Most government agencies are not exempt from the scope of the GDPR or the Belgian law implementing it. As such, the requirements and recommendations described for businesses apply to government agencies as well. The same security measures, data protection standards and general obligations must be followed by them. However, also a couple specific recommendations for government agencies can be made. More concretely, they are advised to do the following:
 - Inform citizens of their rights under data protection law and raise public awareness of privacy and data protection in general. Recent legislative changes have granted Belgian citizens extensive rights to manage their own personal data. This includes the capability to request information on how their data is being managed and to be informed of data breaches affecting the institutions that store or process their information. Citizens also have the opportunity to rely on the DPA to assist them in the exercise of these rights as well as to obtain redress and compensation in case that data protection rules were not followed. It is important that citizens are made aware of their standing and grounds on which they can take the necessary actions;
 - Consider that law enforcement agencies are also bound by certain data protection requirements contained in the Law Enforcement Data Protection

Directive and the Belgian law implementing it⁴. While the requirements for law enforcement agencies are frequently less stringent than those for businesses and other public institutions, they still contain obligations to inform data subjects, follow general data protection principles, conduct impact assessments, cooperate with the DPA, implement safeguards and security measures, keep logs and records, and notify data breaches;

- Enforce data protection legislation by supporting data subjects in the exercise of their rights and holding businesses and public institutions accountable for the processing of personal data and potential non-compliance with the law, in particular when it concerns the requirements of data security, cooperation with the data protection authorities, and the duty of notification in case of data breaches;
- Ensure that the DPA has the necessary resources, independence and competences to fulfill its tasks of monitoring legal compliance, promoting public awareness, drafting guidelines and opinions, and assisting both citizens and businesses.

⁴ Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 30 juli 2018.

5. DISSEMINATION AND VALORISATION

The results were disseminated to different types of audiences: academics, businesses and government as well as citizens and students. For each audience we discuss the way in which they were informed of the results of the project.

Academics

- Journal articles and books
- Conference presentations
 - Visschers, J., Verstraete, C., & Paoli, L. (2017, June). *Cybercriminaliteit tegenover Belgische bedrijven: Prevalentie, incidentie en impact*. Paper presented at the Dutch Society of Criminology Conference, Leiden, the Netherlands.
 - Visschers, J., Verstraete, C., & Paoli, L. (2017, September). *The impact of cybercrime on businesses: The results of a survey in Belgium*. Paper presented at the European Society of Criminology Conference, Cardiff, UK.
 - Ping, C., Visschers, J., Verstraete, C., Paoli, L., Huygens, C., Desmet, L., & Joosen, W. (2017, September). *The relationship between the cost of cybercrime and web security posture: A case study on Belgian companies*. Paper presented at the European Conference on Software Architecture, Canterbury, UK.
 - Ping, C., Huygens, C., Desmet, L., & Joosen, W. (2016, April). *Longitudinal study of the use of client-side security mechanisms on the European web*. Paper presented at the 25th International Conference Companion on World Wide Web, Montreal, Canada.
 - Van Goethem, T., Chen, P., Nikiforakis, N., Desmet, L., & Joosen, W. (2014, June). *Large-scale security analysis of the web: Challenges and findings*. Paper presented at the 7th International Conference Trust and Trustworthy Computing, Heraklion, Greece.
 - Paoli, L., & Visschers, J. (2018, August). *Cybercrime: A growing threat for businesses? The results of two business victimization surveys in Belgium*. Paper presented at the European Society of Criminology Conference, Sarajevo, Bosnia & Herzegovina.

Businesses/Government

- Presentations at Cyber Security Coalition meetings (2015; 2017)
- Distribution of the results to interested participants of the second wave of the business survey

Citizens

- Press release about the results of the first wave of the population survey
- Radio talk on URGENT.FM (Mensentaal S02E01) 2/10/18 (<https://www.mixcloud.com/urgentfm/mensentaal-s02e01-cybercriminaliteit-led-technologie/>)

- Kraks@DeKrook concerning cybercrime together with the FCCU and the CCB 16/10/18 (<https://soundcloud.com/bibdekrook/sets/kraksdekrook-cybercriminaliteit>)

Students

- Extension of the course material for the following courses:
 - E-Security (B-KUL-H09L4A), lectured by Prof. V. Rijmen as an optional course in the master programmes Master of Electrical Engineering and Master of Mathematical Engineering at the KU Leuven
 - Cryptography & Network security (B-KUL-H05D9A (Dutch) and B-KUL-H05E1A (English)), lectured by Prof. Bart Preneel and Prof. Vincent Rijmen as a mandatory course in the master programme Master of Electrical Engineering and an optional course in the master programme Master of Mathematical Engineering at the KU Leuven
 - Introduction to Criminology (B-KUL-C01A5A), lectured by Prof. L. Paoli as a mandatory course in the bachelor programme Bachelor of Criminology and an optional course in the bachelor programme Bachelor of Law at the KU Leuven

6. PUBLICATIONS

The project resulted in different publications. Here, we give an overview of the academic journal articles, the academic books and the reports that were written within the context of the project.

Academic journal articles (peer-reviewed)

- Ping, C., Visschers, J., Verstraete, C., Paoli, L., Huygens, C., Desmet, L., & Joosen, W. (2017). The relationship between the cost of cybercrime and web security posture: A case study on Belgian companies. *Proceedings 11th European Conference on Software Architecture*, pp. 115-120.
- Ping, C., Huygens, C., Desmet, L., & Joosen, W. (2016). Longitudinal study of the use of client-side security mechanisms on the European web. *Proceedings of the 25th International Conference Companion on World Wide Web*: 457-462.
- Van Goethem, T., Chen, P., Nikiforakis, N., Desmet, L., & Joosen, W. (2014). Large-scale security analysis of the web: Challenges and findings. *Trust and Trustworthy*, 7: 110-125.
- Paoli, L., Visschers, J., & Verstraete, C. (2018). The Impact of cybercrime on businesses: A new conceptual framework and its application to Belgium. *Crime, Law and Social Change*. Advance online publication. doi: 10.1007/s10611-018-9774-y
- Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, 92, 139–150. <https://doi.org/10.1016/J.CHB.2018.11.002>

Academic books

- Paoli, L., Visschers, J., Verstraete, C., & Van Hellemont, E. (2018). *The impact of cybercrime on Belgian businesses*. Mortsels: Intersentia.

Reports

- Verdegem, P., Teerlinck, E., & Vermote, E. (2015). *Measuring cost and impact of cybercrime in Belgium (BCC): Risk perception monitor report (1st wave, 2015)*. Ghent: iMinds-MICT.
- Rijmen, V., & De Cnudde, T. (2017). *Report on cost forecast for new types of cybercrime*. Leuven: COSIC.
- Rijmen, V., & De Cnudde, T. (2018). *Guidelines for future investments in cybercrime countermeasures*. Leuven: COSIC.
- Paoli, L., Visschers, J., Verstraete, C., & Van Hellemont, E. (2017/2018). *The impact of cybercrime on Belgian businesses*. Leuven: Leuven Institute of Criminology / Centre for IT IP Law.
- Martens, M., & De Wolf, R. (2018). *Measuring cost and impact of cybercrime in Belgium (BCC): Risk perception monitor report (2nd wave, 2017)*. Ghent: imec-mict-UGent.

7. ACKNOWLEDGEMENTS

The BCC project was set up on the basis of expertise gained by *B-CCENTRE*, which was the first main platform for collaboration and coordination with regard to cybercrime matters in Belgium. *B-CCENTRE* was initiated and coordinated by CiTiP's predecessor ICRI and managed by Ann Mennens. CiTiP expresses its thanks for the initial steps she took together with Prof. Jos Dumortier for laying the foundations of the current BCC project.

Secondly, the promoters of the BCC project and the authors of the present report thank all those who have helped in enabling them carrying out the research. Special mention should be made of the organisations Comeos, Febelfin and VBO/FEB. In particular, the cooperation of the latter, through the persons of Stefan Maes en Anneleen Dammekens of, was highly appreciated.

Further thanks go to the members of the guidance committee for their constructive remarks during the yearly scientific meetings. Members included Cathrin Bauer-Bulst (DG HOME, European Commission), Olivier Burgersdijk (European Cybercrime Centre - Europol), Phédra Clouner (Centre for Cyber Security Belgium-CCB), Walter Coenraets (Federal Computer Crime Unit-FCCU), Christine Darville (FEB), Gert De Boeck (The National Institute for Criminalistics and Criminology (NICC-INCC), -FOD Justitie), Miguel De Bruycker (Centre for Cyber Security Belgium-CCB), Christel De Craim (Dienst voor het Strafrechtelijk beleid-DGWL 38), Kris Decramer (FOD Justitie), Marjolein Delplace (Federal Computer Crime Unit-FCCU), Frederic Fanuel (Cabinet Prime Minister), Jeroen Gobin (CERT.be), Alain Godfurnon (Direction générale de la Réglementation économique Télécommunications et Société de l'Information), Rachid Kerkab (FOD Binnenlandse Zaken, Algemene Directie Veiligheid en Preventie), Luc Lebrun (SPF Economie), Daniel Letecheur (Fedict – the Federal Public Service for Information and Communication Technology), Stefan Maes (FEB), Christophe Mincke (The National Institute for Criminalistics and Criminology (NICC-INCC), -FOD Justitie), Aziz Naji (Belspo), Michael Palmer (European Commission - DG Home), Pascal Pétry (Veiligheid van de Staat - Sûreté de l'Etat-VSSE), Steve Purser (ENISA), Stefan Thomaes (FOD Justitie, Dienst voor het Strafrechtelijk beleid), Pierre Thomas (SPF Intérieur / FOD Binnenlandse Zaken), Tim Van Hamme (CERT.be), Christian Van Heurck (CERT.be), Nathalie Van Raemdonck (CERT.be), Björn Vanneste (Belgian Defence), Pieter Verdegem (UGent - MICT), Patrick Wynant (Febelfin)

Last but not least, this research would not have been possible without the financial support of the BELSP0 – the Belgian Service Science Policy Office. We are especially indebted to Mr. Aziz Naji, its program administrator for the pleasant cooperation.

REFERENCES

- Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., ... Upton, D. (2016). Cyber Harm: Concepts, Taxonomy and Measurement. *Said Business School Research Papers*, 23(8), 1–45.
- Aike, M., Mahon, C., Haughton, C., O'Neill, L., & O'Carrol, E. (2016). A consideration of the social impact of cybercrime examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, 11(4), 373–391. <https://doi.org/10.1080/21582041.2015.1117648>
- Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, 8(1), 5. <https://doi.org/10.1186/s13673-018-0128-7>
- Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Human Computer Studies*, 82, 69–82. <https://doi.org/10.1016/j.ijhcs.2015.05.005>
- Anderson, R., Barton, C., Bhöme, R., Clayton, R., Van Eeten, M., Levi, M., ... Savage, S. (2013). Measuring the Cost of Cybercrime: a workshop. *The Economics of Information Security and Privacy*, 265–300.
- Barth, A. (2011). HTTP state management mechanism. *IETF RFC 6265*.
- Belshe, M., & Peon, R. (2015). Hypertext transfer protocol version 2 (HTTP/2). *IETF RFC 5280*.
- Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *Cyberpsychology, Behavior, and Social Networking*, 21(2), 84–90. <https://doi.org/10.1089/cyber.2016.0727>
- Bernaards, F., Monsma, E., & Zinn, P. (2012). *High tech crime: Criminaliteitsbeeldanalyse 2012*. Woerden, The Netherlands: Korps Landelijke Politiediensten.
- Bijleveld, C. C. J. H. (2009). *Methoden en technieken van onderzoek in de criminologie*. The Hague: Boom.
- Button, M., Lewis, C., & Tapley, J. (2009). *Fraud typologies and the victims of fraud: Literature review*. London, UK: National Fraud Authority.
- Centraal Planbureau (2016). *Risicorapportage cyberveiligheid economie*. Retrieved from www.cpb.nl.
- Chawla, M., & Chouhan, S. S. (2014). A Survey of Phishing Attack Techniques. *International Journal of Computer Applications*, 93(3), 32–35. <https://doi.org/10.5120/16197-5460>
- Chen, P., Huygens, C., Desmet, L., & Joosen, W. (2016). Longitudinal study of the use of client-side security mechanisms on the European web. *Proceedings of the 25th International Conference Companion on World Wide Web*: 457-462.
- Chou, H. L., & Sun, J. C. Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers and Education*, 112, 83–96. <https://doi.org/10.1016/j.compedu.2017.05.003>

- Clough, J. (2015). *Principles of cybercrime (2nd ed.)*. Cambridge, UK: Cambridge University Press.
- Computer Security Institute [CSI]. (2011). *15th Annual 2010/2011 Computer Crime and Security Survey*. Retrieved from www.cours.etsmtl.ca/qti619/documents/divers/CSIsurvey2010.pdf.
- CSIS - Center for Strategic and International Studies (2018). *No Slowing Down Economic Impact of Cybercrime*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1ldhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938
- Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database*, 45(4), 51–71. <https://doi.org/10.1145/2691517.2691521>
- Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers and Security*, 48, 281–297. <https://doi.org/10.1016/j.cose.2014.11.002>
- De Cuyper, R. H., & Weijters, G. (2016). *Cybercrime in cijfers: Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices*. Retrieved from www.wodc.nl.
- Deloitte (2016). *Cyber value at risk in the Netherlands*. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf>
- Detica (2011). *The cost of cybercrime: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*. Guilford, UK: Detica.
- Dierks, T., & Allen, C. (1999). The TLS protocol version 1.0. *IETF RFC 2246*.
- Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *Journal of Strategic Information Systems*, 17(3), 214–233. <https://doi.org/10.1016/j.jsis.2007.09.002>
- Domenie, M. M. L., Leukfeldt, E. R., van Wilsem, J. A., Jansen, J., & Stol, W. Ph. (2013). *Victimisation in a digitised society – A survey among members of the public concerning e-fraud, hacking and other high-volume crimes*. The Hague, The Netherlands: Eleven International Publishing.
- European Commission (2003). Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. *Official Journal of the European Union*, 124: 36-41.
- European Parliament and the Council of the European Union, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, 119: 1-88.

- European Union Agency for Network and Information Security [ENISA] (2016). *ENISA threat landscape 2015*. Retrieved from www.enisa.europa.eu.
- Europol (2016). *Internet organised crime threat assessment 2016*. Retrieved from www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf.
- Eurostat. (2016). *Eurostat model for the EU survey on ICT usage in households and by individuals 2015, version 3.1*.
- Evans, C., Palmer, C., & Sleevi, R. (2015). Public key pinning extension for HTTP. *IETF RFC 7467*.
- Feinberg, J. (1984). *Harm to others*. New York, NY: Oxford University Press.
- FOD Economie (2016). *Aantal actieve btw-plichtige ondernemingen volgens werknemersklasse en plaats maatschappelijke zetel, meest recente jaar* [Webpage]. Retrieved from www.bestat.economie.fgov.be/bestat/crosstable.xhtml?view=9d19ebe2-f35a-4b51-ac1a-c153e6d77d67.
- Froomkin, A. M. (2015). Regulating mass surveillance as privacy pollution: Learning from environmental impact statements. *University of Illinois Law Review*, 2015(5), 1713–1790. <https://doi.org/10.2139/ssrn.2400736>
- Gemalto (2016). 2015: The year data breaches got personal. Retrieved from www.gemalto.com/brochures-site/downloads/entBreach_Level_Index_Annual_Report_2015.pdf.
- Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*, 2: 13-20. doi:10.1007/s11416-006-0015-z
- Greenfield, V. A., & Paoli, L. (2013). A framework to assess the harms of crimes. *The British Journal of Criminology*, 53: 864-885. doi: 10.1093/bjc/azt018.
- Greenfield, V. A., & Paoli, L. (2013). A framework to assess the harms of crimes. *British Journal of Criminology*, 53(5), 864–885. <https://doi.org/10.1093/bjc/azt018>
- Hodges, J., Jackson, C., & Barth, A. (2012). HTTP strict transport security (HSTS). *IETF RFC 6797*.
- Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in Progress*. <https://doi.org/10.4324/9781315775944>
- Interpol. (2017). *Cybercrime*. Retrieved November 8, 2017, from <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>
- Jackson, B.A., Dixon, L., & Greenfield, V.A. (2007). *Economically targeted terrorism: A review of the literature and a framework for considering defensive approaches*. Santa Monica, CA: RAND Corporation.
- Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, 25(2), 165–180. <https://doi.org/10.1108/ICS-03-2017-0018>
- Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology*, 35(5), 368–379. <https://doi.org/10.1080/0144929X.2016.1160287>
- Klahr, R., Amili, S., Shah, J. N., Button, M., & Wang, V. (2016). *Cyber security breaches survey 2016*. Retrieved from www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf.

- Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G., Button, M., & Wang, V. (2017). *Cyber security breaches survey 2017*. Retrieved from [www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber Security Breaches Survey 2017 main report PUBLIC.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf).
- Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58–74. <https://doi.org/10.1016/j.cose.2014.05.006>
- Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(9), 1–10. Retrieved from <http://www.crimesciencejournal.com/content/3/1/9>
- Leukfeldt, E. R., Domenie, M. M., & Stol, W. P. (2009). *Verkenning cybercrime in Nederland 2009*. Retrieved from www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/2009-09-17%20VCN2009%20DEFdef.pdf.
- Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology & Criminal Justice*, *8*: 389-419. doi: 10.1177/1748895808096470
- Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *6*: 3-20. doi: 10.1007/s10611-016-9645-3
- Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology*, *48*: 293-318. doi: 10.1093/bjc/azn001.
- Li, X. (2016). Taxonomy of Cybercrime. *Journal of Legal Studies*, *1*(1), 1–27.
- Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13. <https://doi.org/10.1177/2053951714541861>
- Marlinspike, M. (2009). *New tricks for defeating SSL in practice*. Blackhat.
- Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid*. The Hague, The Netherlands: Rathenau Instituut.
- Nationaal Cyber Security Centrum [NCSC] (2016). *Cybersecuritybeeld Nederland 2016*. Retrieved from www.ncsc.nl.
- Paoli, L., Visschers, J., Verstraete, C., & van Hellemons, E. (2017). *The Impact of Cybercrime on Business*. *Whitepaper*.
- Rens, B. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*(4), 396–411. <https://doi.org/10.1108/JFC-06-2014-0030>
- Rescorla, E. (2000). HTTP over TLS. *IETF RFC 2818*.
- Reyns, B. W., Randa, R., & Henson, B. (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety*, *18*(1), 38–59. <https://doi.org/10.1057/cpcs.2015.21>
- Riek, M., Böhme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. <https://doi.org/10.1109/TDSC.2015.2410795>
- Sen, A., (1987). The standard of living: Lecture I, concepts and critiques; The standard of living: Lecture II, lives and capabilities. In G. Hawthorn (Ed.), *The standard of living: The Tanner lectures* (pp. 1-38). Cambridge, UK: Cambridge University Press.
- Stabek, A., Watters, P., & Layton, R. (2010). The seven scam types: Mapping the terrain of

- cybercrime. In *Proceedings - 2nd Cybercrime and Trustworthy Computing Workshop, CTC 2010* (pp. 41–51). <https://doi.org/10.1109/CTC.2010.14>
- Stamm, S., Sterne, B., & Markham, G. (2010). Reining in the web with content security policy. *Proceedings of the 19th International Conference on World Wide Web*: 921–930.
- Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a “Digital Criminology”? *International Journal for Crime, Justice and Social Democracy*, 6(2), 17–33. <https://doi.org/10.5204/ijcjsd.v6i2.355>
- Strauss, A. & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Newbury Park: Sage.
- Tsakalidis, G., & Vergidis, K. (2017). A Systematic Approach Toward Description and Classification of Cybercrime Incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, PP(99)*, 1–20. <https://doi.org/10.1109/TSMC.2017.2700495>
- United Nations Office on Drugs and Crime [UNODC] (2013). *Comprehensive study on cybercrime*. Vienna, Austria: United Nations Office on Drugs and Crime.
- Van der Hulst, R. C., & Neve, R. J. M. (2008). *High-tech crime, soorten criminaliteit en hundertads: Een literatuurinventarisatie*. Retrieved from www.wodc.nl.
- Van der Hulst, R. C., & Neve, R. J. M. (2008). *High-tech crime, soorten criminaliteit en hundertads: Een literatuurinventarisatie*.
- Van Leiden, I., Appelman, T., Van Ham, T., & Ferwerda, H. (2014). Ondergaan of ondernemen: Ontwikkelingen in de aard en aanpak van afpersing van het bedrijfsleven. Retrieved from www.wodc.nl.
- Verdegem, P., Teerlinck, E., & Vermote, E. (2015). *Measuring Cost and impact of cybercrime in Belgium (BCC): D.3.1.1. Risk Perception Monitor Report (1st wave, 2015)*. Ghent.
- Verizon (2016). *2016 Data breach investigations report*. Retrieved from www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.
- von Hirsch, A., & Jareborg, N. (1991). Gauging criminal harm: A living-standard analysis. *Oxford Journal of Legal Studies*, 11: 1-38.
- Wall, D.S. (2007). *Cybercrime: The transformation of crime in the information age*. Malden, MA: Polity Press.
- West, M. (2016). Content security policy level 3. *W3C Working Draft*.
- West, M., Barth, A., & Veditz, D. (2016). Content security policy level 2. *W3C Recommendation*.
- Wickramasekera, N., Wright, J., Elsey, H., Murray, J., & Tubeuf, S. (2015). Cost of crime: A systematic review. *Journal of Criminal Justice*, 43, 218–228. <https://doi.org/10.1016/j.jcrimjus.2015.04.009>

LIST OF TABLES AND FIGURES

Tables

Belgian Citizens

1. Total sample: Online activities Citizens
2. Total sample: perceived security of online activities
3. Total sample: Correlations between online activity & perceived safety
4. Total sample: Amount of security measures taken
5. Total sample: percentage of people who perform certain security measures
6. Total sample: amount of security measures in total
7. Total sample: victimisation rate
8. Total sample: security measures taken against cybercrime by victimization
9. Total sample: direct monetary costs by cybercrime
10. Total sample: direct non-monetary cost by cybercrime
11. Total sample: defence costs

Belgian Businesses

12. Overview of European web dataset for longitudinal study
13. Overview of the use of security features on the European web
14. Correlation between the adoption of security features in a website and its Alexa rank
15. Correlation between the security score of a website and its Alexa rank
16. Percentage of newly adopted HTTPS sites that enabled Secure Cookies and HSTS features
17. Cybercrime experiences of 263 Belgian businesses
18. Cybercrime experience over different business size
19. Overview of the use of security features on the European web
20. Spearman's rank correlation between the impact of unauthorised access to IT systems and web security features
21. Spearman's rank correlation between the impact of cyber extortion and web security features
22. Logistic regression on the business loss due to unauthorised access to IT systems over web security features
23. Logistic regression on the reputation damage due to unauthorised access to IT systems over web security features
24. Logistic regression on the business loss due to cyber extortion over web security features
25. Logistic regression on the reputation damage due to cyber extortion over web security features
26. Correlation between the cost of cybercrime and overall web security
27. Perceived victimization risk of cybercrime in next 12 months
28. Staff time invested in neutralizing cyber incidents suffered (first wave)
29. Staff time invested in neutralizing cyber incidents outsourced to external businesses or consultants (first wave)
30. Parties responsible for neutralization of cyber incidents (second wave)
31. Internal staff costs of cyber incidents (second wave)

32. External staff costs of cyber incidents (second wave)
33. Costs resulting from the cyber incidents suffered
34. Businesses' assessments of the severity of the harms caused to other interest dimensions by the cyber incidents suffered
35. Response to question 1: How is the effectiveness of your security program evaluated?
36. Response to question 3: Does your company have an insurance to protect itself from cybercrime and if yes how much does your company pay for it?
37. Response to question 5: How many man-hours per week does your company invest in the prevention of cybercrime?

Figures

Belgian Citizens

1. Example of HttpOnly and Secure Cookies stored in a browser
2. Large-scale web crawling approach
3. ECDFs for each security feature

Belgian Businesses

4. Percentage of websites that adopted more security features in 2017 versus 2013, plotted per 10k Alexa ranks
5. Percentage of websites that adopted more security features in 2017 versus 2013, grouped per business vertical
6. Average overall security score for per 10k Alexa ranks
7. Average overall security score for each business vertical
8. Average overall security score for each EU country
9. Percentage of websites in each business vertical that adopted HTTPS over time
10. Incidence of cybercrime in past 12 months
11. Response to question 4: Has your company in the last 12 months acquired any of the following tools to protect the company computers and electronic data? Indicate all that apply.
12. Response to question 6: What does your company do to keep itself updated in the prevention of cybercrime?