European Transport \ Trasporti Europei (2019) Issue 75, Paper n° 3, ISSN 1825-3997

Cybersecurity benefits and resilience of ports

Andrea Chiappetta[1*]

[1]*Professor of Geopolitics*
Università Telematica Niccolò Cusano
Via Don Carlo Gnocchi, 3, 00166 Roma RM
CEO @ ASPISEC
Piazzale Flaminio 19, 00196 Roma
a.chiappetta@aspisec.com

Abstract

The technological advancements and the general trend towards having high-risk data demand a better form of security to prevent any software theft or damage. The computers we used to have three decades ago were not connected to each other, and the Internet was just a connection between some researchers. Now, computers are linked, and the Internet is widely used; malwares can be transferred from one computer to another in many forms. Cyber security's main role is to guarantee integrity, confidentiality, and availability of data. This study aims to explore the benefits of cyber security with a focus on ports.

Keywords: Cybersecurity, Critical Infrastructure Protection, Ports, Infrastructures, Resilience, Public-Prvate Partnerhsip

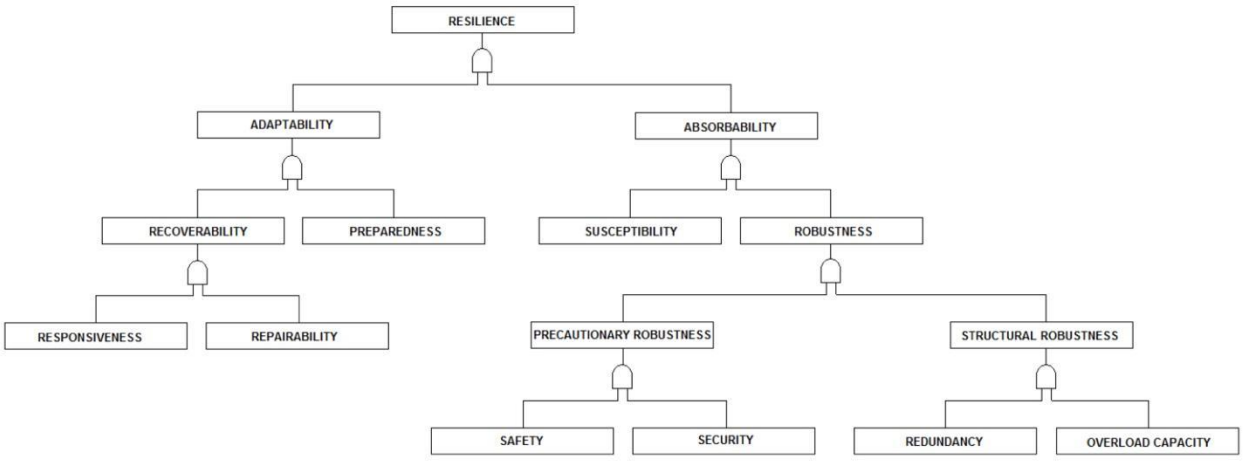
1. Cyber: converging dependencies

The cyber world is growing every day; several studies show that by 2025, Internet-related technologies such as IoT and cloud computing will create possible benefits to the economy between 8 and 32 trillion of dollars annually[1]. A clear value of the damage that could be related to cyber insecurity is not yet defined. Critical infrastructure means assets and systems which are important for preserving key social functions, safety, economic and health security, as well as the people's social wellbeing. This covers a variety of private and public sectors including banking and finance, health, transport, energy, etc. At the global level, all nations defined a list of Critical Infrastructure and related services that must be considered strategic and need to respect certain rules (Anderson et al., 2012).

[1] Mckinsey Global Institute (2013), Disruptive technologies: Advances that will transform life, business, and global economy.

The US issued the first approach during the Clinton Administration in the 90s, followed then by Canada in February 2001, when it initiated the OCIPEP (the Office of Critical Infrastructure Protection and Emergency Preparedness) within the National Defense organizational structure Department, and Europe (the European Commission adopted a Green Paper on a European program for Critical Infrastructure Protection, and in 2008, the European Council issued the Directive 2008/114/EC; Fuchs *et al*., 2016.). The main characteristics essential for evaluating critical infrastructures are resilience, absorbability, adaptability, robustness, structural robustness, precautionary robustness, susceptibility, preparedness, recoverability, responsiveness, reparability, redundancy, overload capacity, safety, and security. These characteristics apply to each type of critical infrastructure (e.g., transport) and for any level of detail selected for the critical infrastructure analysis (system, subsystem, component). To exact description of critical infrastructure characteristics and assessment them through parameters was possible, the set of features must be internally consistent.

Figure 1: Critical infrastructure characteristic tree



The Critical Infrastructure characteristics tree shows the relationship between the Critical infrastructure characteristics by the logic gates AND. Resilience is a series of processes form an umbrella attribute which is formed by partial features[2]. Resilience can thus be divided into basic indivisible features. These essential characteristics can be evaluated through one or several parameters. Furthermore, components at the higher level can be assessed through appropriate settings. Based on the Critical Infrastructure characteristic tree we can identify two types of interrelations among the Critical Infrastructure: additive and non-additive. The additive interrelation is valid for the Critical Infrastructure characteristics. Resilience can be fully described as the sum of

[2] Resilience is formed by a series of processes.

individual features. However, it is not possible to obtain the value of the resilience parameter as a sum of values of parameters of partial Critical Infrastructure characteristics. This non-additive must be respected when tools and methods of Critical Infrastructure assessment are selected.

Another important aspect is related to the Critical Infrastructures interdependencies that usually fall into four principal classes:

- Physical: operating one infrastructure depends on the other infrastructure's real output.
- Cyber: The level at which the information transmitted via the infrastructure can be depended upon.
- Geographic: The level of dependence on the local environmental effects which instantaneously impacts several infrastructures.
- Logical: Any dependency not grouped as geographic, cyber or physical. A comprehensive analysis of all types of interdependencies is challenging and requires extensive modeling efforts to provide a better understanding of CI systems.

In this framework ports are considered as Critical Infrastructure; it is true affirming that whereas no two ports are exactly alike, many share some features like size, closeness to a metropolitan area, the amount of cargo processed, and connections to complex transportation networks. These NO characteristics/standards can make them vulnerable to physical security threats because a standard procedure has not yet been developed[3]. Ports mean a physical and virtual infrastructure that moves goods, data, persons, etc. Ports are a fundamental player of the economy and growth of nations. Over time, several steps ahead were done in order to improve and increase the perimeter security. Less were made in favor of cyber-security, and this is the topic that we will try to explain, to define the standard and provide standard criteria to be adopted.

The enhancement of security, both physical and cyber, at ports is essential to ensure their smooth operation, serving the passenger and freight flows[4]. On the other hand, ports are considered as vulnerable infrastructure mainly due to their proximity to the sea and the problems faced in controlling the threats coming through it, the number of operations taking place in the ports and their different nature, and the considerable number of people working or involved in several activities in the ports. Internationally, the relevant legislation on port security is the ISPS Code (International Ship and Port Facility Security Code), implemented at EU level by the EU / 725/2004 and the EU / 65/2005, which requires the identification of authority, acts skills and objectives to establish and maintain security measures. In this context, it takes the definition of a Port Security Plan, drawn

[3] NO standards make a system vulnerable to attacks because of unavailability of standard procedures.

[4] In Airports, physical security on the computer systems is vital owing to the nature of information stored and transmitted

up by the Port Security Officer (PSO), which takes into account the analysis of the risks of ships and the port facility. Also, it identifies the Port Facility responsibilities and tasks of the Port Facility Security Officer (PFSO). It is also important to note that many European ports are to all parts of the city and therefore the effects of splitting the areas under Security checks presents greater complexity.

Table 1: Regulations Overview

EU Regulations	**US Regulations**
CIIP Directive (2012)	USA H.R. 3878(2015)
The cyber-security strategy for the EU (2013)	NIST 800-30
EIDAS Regulations (2014)	Port security grant program (2014)
European Agenda on security (2015)	Maritime & Port Security Information Sharing and Analysis Organization" (MPS-ISAO, 2017)
CPPP Initiative (2015)	Presidential Policy Directive 21 (PPD-21)
NIS Directive (2016) EU Cyber Security Strategy	US WH EO 13636

Concerning the ENISA report on cyber-security challenges in the Maritime Sector[5], it appears clearly that cyber threats are a growing menace, spreading to all industry sectors that rely on ICT systems[6]. Such incidents could be prevented by policies that neutralize the various market failures acting as a barrier to optimize private investment in cyber-security from public and private institutions, where an efficient cooperation and coordination in the real world experiences highlight the economic need for coordinated cyber defense (Brynjolfsson and Oh, 2012) to lower expenses on security for all partners involved (Flater et al., 2016).

The cost of a breach may not fall entirely on the immediate victim[7]. Many computers systems store valuable information about entities other than the system's owner. Starting from 2018 in the framework of the NIS Directive will also cover the Critical Infrastructure from a legislation point of view. Cyber-attack to maritime transports are an issue already consolidated: accessing a port's computers, or sending fake signals of GPS to change the route of a ship, changing a ship's automatic signal for identification to report a wrong location, infiltrating information systems and electronic chart display and software to change maps, and also pirates listening into transmissions by AIS to identify possible victims. The latest critical automation systems' disruptions, like Stuxnet, show that cyber-attacks can potentially affect infrastructures. Disturbance of such ICT systems may have

[5] Enisa Report: ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR
November 2011

[6] Sectors relying on ICT are the most vulnerable to attacks.

[7] The costs of breaching are felt by a chain of people, starting with the immediate victim onwards.

far reaching effects for the EU Member States' governments as well as their social well-being. A challenge arises to make sure that there is ICT robustness against cyber-attacks at pan-European and national level (Flater et al., 2016).

Some of the report's findings emphasized that currently there is a low Maritime cyber-security awareness and risk-based holistic approach along with a valuation of maritime cyber risks associated with the maritime authorities, and pointing out all important assets within this sector is highly necessary. The holistic security represents an answer: Physical and Cyber-security of the network, to guarantee Privacy Integration Protocols of the users. There are so many initiatives that come in response to the latest cyber-attacks that enabled abstraction of containers from the port in a seemingly legal way. For example, MSC initiated a new Container Release System that enables collection of containers from the port securely. Users need to log into a secure portal where they have to identify themselves to access to the container release data. The technology is currently being used across the port from efforts made by APCS. Furthermore, the Port of LA took a significant step towards reducing its cyber risks with the implementation of a state-of-the-art Cyber-security Operations Center (CSOC). The CSOC includes advanced hardware and software that is used to proactively monitor the computer environment to prevent a breach and be able to detect and respond if a breach does occur quickly. The CSOC is also the technical nerve center, which collects cyber-security data that can be analyzed and shared with other agencies.
Another useful instrument adopted by the US is the Port Security Grant Program[8]. It supports the implementation of the National Preparedness System by supporting the building, sustainment, and delivery of core capabilities essential to achieving the National Preparedness Goal of a secure and resilient Nation improving cyber security Capabilities. Something similar has not yet been developed at EU level. This delay could be an excellent opportunity to define a European strategy related to the port cyber resilience program identifying financial instruments, like incentives or institution of a specific plan to be included in the Connecting Europe Facility Funds, also to support the "hardenization" of the critical information infrastructure such as submarine fibre optic cables,the Domain Name System (DNS) and internet exchange points.

1.2 Benefits and costs of connectivity

The benefits and costs of connectivity should be considered for the next decade in order to allow governments and companies to adopt the right strategy to make more secure their data flows (financial, personal and consequently the critical infrastructures). This chapter will provide a benefit-cost framework based on the results of the transatlantic cyber insecurity and cybercrime report[9].

[8] The port security grant program was launched in 2008 by the US Gov. or the protection of critical port infrastructure from terrorism
[9] European Parliament – Transatlantic cyber-insecurity and cybercrime – Economic impact and future prospects. Members Research Service – Dec 2017 – PE 603.948

The study provided several application for cyber resilience, cybersecurity, and cybercrime taking into account the direct and indirect cost and benefit as showed in the table below.

In the table, direct benefit that is associated with cyber resilience and cyber security is preventing the possible causes that would have been incurred while preventing the data security issue. However there are other indirect benefits including economic growth, employment creation, increased productivity and higher consumer surplus.

There are also direct and indirect costs incurred by cybercrimes. The direct losses or costs incurred include the cost incurred in preventative measures against the cybercrimes, the cost of post incident recovery as well as reapportioned wealth from theft carried out online by frauds in different sectors. The indirect costs include the foregone economic activities while crippled with system attacks, opportunity costs as well as efficiency losses.

Table 2: The direct and indirect benefits associated with cyber resilience and cyber security and losses/costs associated with cybercrime

	BENEFITS	**COSTS/LOSSES**
Direct	Cost-avoidance	Cost of preventative measures Cost of post incident recovery Reapportioned wealth from theft
Indirect	Economic growth Employment creation Increased productivity Higher consumer surplus	Foregone economic activity Opportunity costs Efficiency losses

Methodology

The research focuses on cybersecurity, cyber-resilience, and cybercrime. Although much effort has been put into these topics, because of the nature of the advanced technologies that are involved and how concepts overlap, the related topics like data privacy, data protection, digital trade, internet governance and the others are occasionally referred to. This study also does not include the cybersecurity military aspects[10].

Benefit-cost framework

The benefit-cost framework is applied in this study to enable maker of policies to understand the degree of the economic losses and costs that are associated with

[10] The military aspects are left out because of the sensitive nature and lack of sufficient data to substantiate claims made in the report.

cybercrime and the advantages that are associated with cyber-resilience and cybercrime. During policy examination, the policymakers rarely focus on the economic centric view of the issues. This is, however, a very significant view because the risks of cybersecurity cannot be eliminated completely and therefore there is a requirement of an approach of risk management to put the finite resources in sectors where they can be most productive. The economic view together with a probability understanding helps in the implementation of the approach to risk management.

This will assist in the determination of the cybercrime, cyber-resilience and cybersecurity sectors where US and EU cooperation can have the greatest advantages and minimize costs at the same time. While the technical, social and political view is significant in making policies, this study focuses on the economic view. The study should be viewed as a process of policy-making input where the additional views are also part[11].

The study combines two frameworks to give a benefit-cost framework for cyber-resilience, cybersecurity, and cybercrime. For every equation of benefit-cost side, there is a component that is direct and indirect. The statistics which are given in all the parts of the framework offer a representation of the losses, costs, and benefits being studied. There is no intention of making them aggregated. The pictures are a presentation of an incomplete picture which is essential. This is part of the phenomena that is being examined and the data which is used to estimate them. The main aim of the framework is however not affected by the inability to measure the statistics[12].

The statistics enable policy makers to determine where are possible benefits, costs, and losses from the cooperation of EU and US in order to adjust the policies to initiatives that can lower the losses and costs and maximize the benefits.

	Benefits	**Loses/costs**
Direct costs	Avoidance of costs	Preventative measures cost Post-incident recovery cost Wealth reapportioned from theft
Indirect costs	The higher surplus of consumers Creation of employment Improved productivity. Growth in economy	Losses on efficiency. Economic activities forgone Opportunity costs.

[11] CRS report for congress - Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, Clay Wilson Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division, Updated January 29, 2008 - http://www.dtic.mil/docs/citations/ADA477642

[12] https://dl.acm.org/citation.cfm?id=2444747

Benefits and losses from Direct and Indirect costs

Taking into consideration the benefits assessment, direct benefits are defined from the view of investments as costs savings in the preventive measures or the reduced losses and costs which are associated with the lowered incidents of cybercrime (Flater et al., 2016). It can also be referred as cost avoidance. It applies similarly to organizations and infrastructure of the same nature. The direct costs and the indirect losses figures in the fifth section of the report are a side of the possible benefits. If preventive strategies could not be implemented, the losses and costs from the incidents could be higher. The reduction of the possible losses and costs are the benefits of investments in cybersecurity[13].

The report uses a framework that was created by Hughes et al. (2015) for the estimation of the extent of indirect benefits of a digital technology, which is also referred to as cybersecurity.

The advancements in cybersecurity and the reduction in the number cybercrimes have made enterprises and individuals to trust more advanced technology. This increased trust has lead to a massive adoption of such technologies, and this enables enterprises and individuals to benefit more from them. These benefits are:

- Increased employment;
- Increased productivity;
- Higher economic growth;
- Higher consumer surplus.

For the losses and costs, the study uses a framework of costs estimation of cybersecurity that was created by Brynjolfsson and Oh (2012).With other resources in the future, there is a possibility of further expanding the framework to include some particular estimates of the member states of the EU.

Results

Cybercrime: Indirect Losses and Direct Costs

The internet and advanced technology have quickened the establishment of existing and new forms of crime. This a space which is moving very fast with[14] the emergence of new methods and retreating every other year. This section examines the indirect losses and the direct costs that are related to the cybercrime forms. For the losses and costs, the

[13] Atkinson, Robert D. and McKay, Andrew S., Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution (March 2007). Available at SSRN: https://ssrn.com/abstract=1004516 or http://dx.doi.org/10.2139/ssrn.1004516

[14] Anderson R. et al. (2013) Measuring the Cost of Cybercrime. In: Böhme R. (eds) The Economics of Information Security and Privacy. Springer, Berlin, Heidelberg – DOI https://doi.org/10.1007/978-3-642-39498-0_1

report used a framework of cost estimation of the cybercrime that was developed previously by Flater et al., (2016).).

Direct Costs

Since this threat environment is evolving rapidly, the difference between crimes committed in the offline world and those committed in cyberspace is relatively small. As a result, the model developed by Anderson et al ., (2012)[15] categories that cybercrime directs costs into their main groups including:

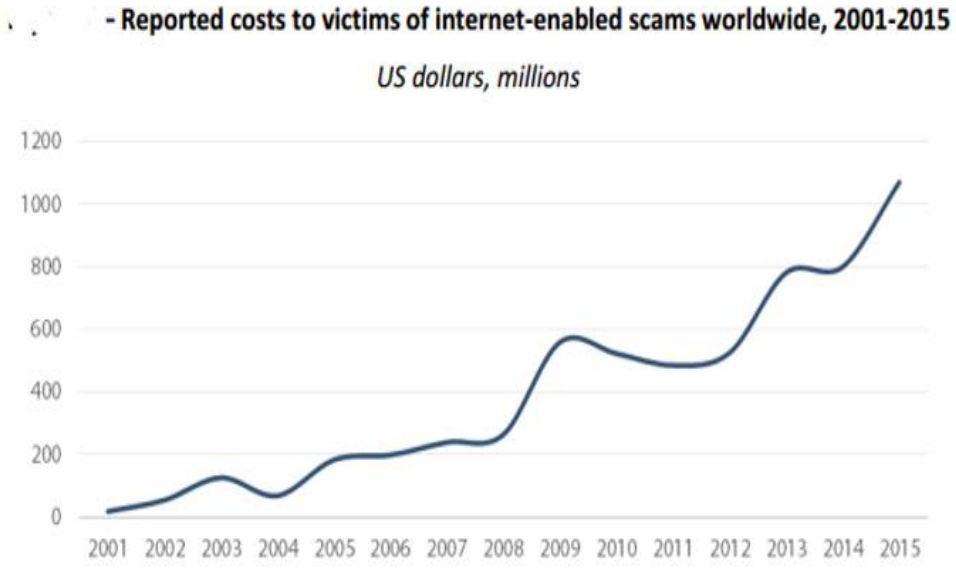
- Genuine cyber crimes which are the new crime forms perpetrated using digital technology like botnets;
- Traditional cyber crimes which were crimes that were perpetrated offline but are currently committed largely online because of the adoption of the advanced technology, like tax evasion;
- Transitional cyber crimes which were crimes that were perpetrated offline but are now increasingly - yet partly - perpetrated online like card fraud;

Genuine Cybercrime

There are new crime forms that are committed using the internet. Since the beginning of the 2000s, piracy and copyright infringements over networks have been the main cyber crimes done on the internet (Brynjolfsson and Oh, 2012).

The revenue made by the pirates and the services selling pirated videos, games, music, and pharmaceuticals that are patent-infringing is lower as compared to the $0.20 for every person annually (Flater et al., 2016).

[15] Transatlantic cyber-insecurity and cybercrime - Economic impact and future prospects - EPRS | European Parliamentary Research Service Members' Research Service December 2017 — PE 603.948 - Benjamin C. Dean, Iconoclast Tech http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603948/EPRS_STU(2017)603948_EN.pdf



Data source: IC3 2015 Internet Crime Reports 2001-2015

Table 2: Recorded losses to victims of scams through the internet in the year (2015)

	Total (US$)	**% of total**
Total globally	1 070 711 522	100
Compromise on business emails	246 226 016	23
Romance/confidence fraud	203 390 531	19
Non-delivery/non-payment	121 329 122	11
Investment	119 177 899	11
Identity Theft	57 294 859	5
Advance fee	50 721 226	5
Others	56 153 977	5

Source: IC3 2015 Internet Crime Report

On the other hand, there is a constant change in the variety of frauds and scams which has resulted in increased costs for internet users[16].

According to the Complaint Center of the International FBI in the year 2015, there was over $1.1 billion that was stolen from several victims of scams all over the world[17]. This was an increase from the 2006 figure that was $182 million (Brown et al., 2015).

The statistics from the year 2014 show that the yearly per capita costs in that year were $2.12 in the US and $0.52 in the UE. The figures on the costs that were caused to the

[16] Garon, Jon, 2015 Cyberlaw Year in Review – Seeking Security Over Privacy, Finding Neither (December 23, 2015). Available at SSRN: https://ssrn.com/abstract=2707756

[17] Money stolen from people because of cybercrimes is increasing on a daily basis.

victims of the scams that were internet-enabled in the year 2015[18] are shown in the figure below. The figures provided are worldwide statistics although the IC3 ones cover the US only (Brown et al., 2015).

The change that is most noticeable is the last few years are the emergence of email scams that are associated with the business[19]. The scams involve many criminals that comprise accounts of executives and then wire out money under the name of payments made to clients and suppliers. These comprised the biggest part of the cybercrimes that were reported in the year 2015, almost 23% (Brand and Makey, 1985). A big attention is now accorded to ransomware that involves the encryption of the hard-drive of the victim then demanding ransom in return. The ransom can be given or paid using Bitcoins, a pseudonymous currency Europol, 2016. In the year 2015, there were 2456 payments were made from victims, and this added up to $1.8 million, and this was 1% of the scam losses and costs in that year. In 2016, there were 2670 complaints that were labeled as ransomware with costs of over $2.6 million (IC#, 2015; 2016).

Table 3: Costs of Genuine cybercrime through different years

	United States		**European Union**	
	Total USD	*Per capita*	*Total USD*	*Per capita*
Software whose copyrights were infringed	23 042 782	0.07	1 728 209	0.003
Revenue earned from subscription of cyberlockers	21 120 000	0.07	21 120 000	0.04
Revenue attained by ads from cyberlockers	54 408 000	0.17	49 874 000	0.10
Pharmaceuticals affected by patent-infringing	7 926 572	0.23	5 394 493	0.01

Sources: Transatlantic cyber-insecurity and cybercrime

Transitional Cybercrimes

These are crimes which were basically done offline but are now changing to online too. The card fraud payment is one of these crimes, done either through credit or debit

[18] Anderson R. et al. (2013) Measuring the Cost of Cybercrime. In: Böhme R. (eds) The Economics of Information Security and Privacy. Springer, Berlin, Heidelberg

[19] Many people and companies have fallen victims on email scams perpetrated by cyber criminals around the world.

cards. According to the Federal Reserve payments study in the year 2016[20], in 2015 a big number of card payment frauds took place offline in the US. This is a lower figure compared to the 59% of 2012. The European Central Bank found out that a big number of frauds in the SEPA (Single Euro Payments Area) took place online in 2013, which was about 66% (FTC, 2016)[21]. This amounted to $5 per person in the United States in 2012 and $2.35 in the SEPA in 2013 (Flater et al., 2016).

Table 4: Average Costs of Genuine Cybercrime from the Year 2006 to 2015

Country/Region	**United States**		**European Union**	
Affected sector	*Total USD*	*Per capita*	*Total USD*	*Per capita*
Software whose copyrights were infringed	23 042 782	0.07	1 728 209-	0.003-
Revenue earned from subscription of cyberlockers	21 120 000	0.07	21 120 000	0.04
Revenue attained by ads from cyberlockers	54 408 000	0.17	49 874 000	0.10
Pharmaceuticals affected by patent-infringing	7 926 572	0.23	5 394 493	0.01

Source: Transatlantic cyber-insecurity and cybercrime

Estimation of the Data Breaches Costs

Among the most visible impacts of escalating attacks and poor cybersecurity is a series of data breaches of the last years. Incidents of high profile have happened on both sides of the Atlantic, affecting the private and public sectors in the same way (Florcruz, 2003). Besides the most obvious negative consequences of the data breaches, there are also financial costs (Baily & Montalbanon, 2016). The approach that is most commonly used in estimating such direct costs is finding the average cost for every record and then multiplying it by the number of records that have been stolen and thus find the total

[20] https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm

[21] Anderson R. et al. (2013) Measuring the Cost of Cybercrime. In: Böhme R. (eds) The Economics of Information Security and Privacy. Springer, Berlin, Heidelberg

figure[22]. This method that was created by the Institute of Ponemon applies the loss of very record of $154[23] (Bradley et al., 2013).

Another method that has been forwarded by Verizon calculates the value at $0.58. When thousands of millions of records are involved in data breaches, the difference in the number of estimates between the two methods is apparent. The Target case that saw over 40 million debit and credit card records and over 70 million records in other categories stolen is a case to consider (Australian Transport Safety Bureau, 2008).

Using the Ponemon method, costs amount to $16.9 billion using the cost for every record[24], while the method of Verizon estimates $6.275 billion. However, the costs that were associated with this breach were disclosed by Target in the SEC reports. In the 2015 first quarter, Target also calculated the gross expenses using the data breach as $242 million. However, when there is consideration of the insurance reimbursement, the losses can go down to $163 million. When tax deductions are also considered, the losses amount to $106 million (Florêncio and Herley, 2011). This is just a fraction of the estimates of Ponemon and Verizon (Brown et al., 2015). As much as Target had other indirect costs like reputational damage, the losses can be hard to estimate and cannot be constant in the entire period. Using the totals, the average costs for every record can be calculated from the Target data breach. If the figure of the gross expenses is divided by the lost records that are $242 divide by 110 million lost records, the average for every record is $2.28.

[22]AIS Electronic Library (AISeL)- Is There a Cost to Privacy Breaches? An Event Study http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1215&context=icis2006

[23] Since 2005, the Ponemon Institute has published their annual Cost of Data Breach Study which focuses on measuring the cost of data breaches and providing organizations with a means by which they can measure the potential impact of a data breach to the organization The Ponemon research focuses on determining the cost of a data breach by the number of individual records compromised in the breach. For 2016, their research concluded that the global average cost of a data breach is $158 per record compromised. The cost per record differs by country with the US having the highest cost per record of $221. The report goes on to conclude that US organizations paid the highest cost of $3.97 per record in the form of abnormal customer turnover, increased customer acquisition cost, reputation loss, and diminished goodwill
Detailed info: https://www.sans.org/reading-room/whitepapers/dlp/data-breach-impact-estimation-37502

[24] The most common approach to estimating such direct costs is to determine an average cost per record then multiply by the number of records stolen to reach a total. One method, developed
by Ponemon Institute, uses an average loss per record figure of US$154. Another, put forward by Verizon, estimates this same number at US$0.58. When data breaches involve hundreds of
millions of records, the difference in estimated impact between these two methods become readily apparent. To illustrate, consider the case of Target, which saw 40 million credit and debit card records and 70 million other records stolen. Using the average cost per record approach, the Ponemon method suggests costs of US$16.9 billion while the Verizon method suggests US$6.275 billion.

Using the figure of the net expense of 106 million, the cost for every record is $0.96. The costs are equivalent to less than one % of the total revenue of Target in the year 2015 (Australian Transport Safety Bureau, 2008).

The results show consistency with the 20 000 large-scale studies of cybersecurity incidents, and this includes the phishing crimes, privacy violations, and security incidents and data breaches[25]. It was realized that the cost per cyber incident is lower than $ 200 000 and this is just about the same as the annual security budget of IT of a firm. This represents almost 0.4 % of the annual revenue total (Arbor Networks Inc, 2016).

Table 5: Costs to Target because of a data breach as discovered by SEC filings

Method	40,000,000 million card records	70, 000,000 other records	Total cost estimation
Ponemon method	616 000 000	10 780 000 000	16 940 000 000
($154 for every record)			
Verizon method	23 200 000	6 252 400 000	625 600 000
($.58 for every record)			

Source: Transatlantic cyber-insecurity and cybercrime

Table 6: Costs to Target because of a data breach as discovered by SEC filings

	Gross Expenses	**Insurance Reimbursement**	**Pre-tax net expenses**	**Net tax expenses**
2013	191	46	145	94
2014	61	44	17	11
Total	252	90	162	105

Source: Transatlantic cyber-insecurity and cybercrime

The limitations of the approach of the cost per record are clear. One of the problems is that data breach average does not exist[26]. The outcome is determined probabilistically depending on various factors like the organization's preparedness, the type of data stolen, and the interconnection among entities (Arbor Networks Inc, 2016).

[25] The economic cost of publicly announced information security breaches: empirical evidence from the stock market - Campbell, Katherine | Gordon, Lawrence A. | Loeb, Martin P. | Zhou, Leitgbj DOI: 10.3233/JCS-2003-11308 - Journal of Computer Security, vol. 11, no. 3, pp. 431-448, 2003

[26] **The impact of information security breaches: Has there been a downward shift in costs Gordon, Lawrence A.a; b; * | Loeb, Martin P.a; b | Zhou, Leia - DOI: 10.3233/JCS-2009-0398 -Journal: Journal of Computer Security, vol. 19, no. 1, pp. 33-56, 2011**

In addition, the average estimates do not show great variance, especially where losses are not distributed normally like in data breaches (Andrews et al., 2016).

The main lesson for the makers of policies is the effect of the data breaches cannot be predicted, and it is hard to model. As much as even the big data breaches have not been enough to make companies such as Target insolvent, it doesn't imply that the event cannot occur again in the future (Baily & Montalbano, 2016).

Conclusions

Despite high visibility, genuine cybercrimes' direct costs are low in both the US and the EU. For example, the criminal revenues reported from scams and frauds in the whole world including that of ransomware are lower than $1 million in the year 2015. This is equivalent to less than $ 1.5 cost per capita for every person in the EU and the US. The traditional categories costs that have gone online like welfare fraud and tax evasion outdo the direct costs associated with other categories several times. Given their nature that is transitional the cooperation between the US and the EU can be significant in reducing and containing the future direct costs (Baker, 2016).

- The indirect losses associated with cybercrimes are higher than the direct costs. As much as it is hard to estimate the reliability, security prevented two in twelve EU consumers from doing a task on the internet in the year 2015.
- Most of the statistics used are not credible as such methodologically, but they are the ones which are available. Most of the data which can be reliable of the cybersecurity incidents has not been done in the last few years. The surveys of Eurostat on the most recent cybersecurity-related incidents do not have questions on the effect of the incidents on people and firms. Improvements are required in the statistics and data available for the impacts of the cybersecurity and cybercrime incidents.

Information communication technology is crucial for the success of logistics. Using information systems has increased the speed of communication in the port. Technology enables the actors to share information at the shortest time possible without physically moving to the destination of the information. Implementation of information communication technology in an organization requires total submission from all actors involved to embrace it.

Digital innovation vicissitudes the actors' business model along the supply chain of the maritime.

The supply chain of maritime invest in the information systems that are independent to facilitate their businesses as well as maintain competitiveness. That is, supporting the novel business models as well as deliver novel services.

With respect to maritime supply chain integration, the shareholders get into an independent situation. Cloud services applications will make it possible for innovations tom move forward.

All companies should embrace information systems in their operations for easy communication and sharing of information that is digital innovation.

Financial support is logistics facilitates the development and implementation of the information communication technologies in the port. The alignment exists between the strategies of various companies and success levels in the sector with respect to information communication technology-independent initiates.

The innovation initiatives of information communication technology are driven by profits.

Developing and implementing of cyber risk management technique should incorporate cyber safety and cybersecurity and should start a complete assessment.

Risk management in the port involves for possible actions which are the avoidance of risk, transfer of risk, risk acceptance and mitigation risk.

Last but not least, a European level, but in particular at the Mediterranean level cross-border cooperation is fundamental, and a intergovernamental cyber security competence center could support the common framework and provide standards (still missing) and interoperable solutions in the digital market. To reach this goal it could be necessary to identify incentives from the European Commission in order to create a Mediterranean Area based on the same strategy that will allow greater cohesion.

References

AIS Electronic Library (AISeL)- Is There a Cost to Privacy Breaches? An Event Study Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1215&context=icis2006

Anderson R., Barton C., Böhme R., Clayton R., van Eeten M. J. G., Levi M., Moore T. and Savage S. (2012), ‘ Measuring the cost of cybercrime’, Workshop on the Economics of Information Security, available from http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

Andrews D., Criscuolo C. and Gal P. (2016), ‘the Best versus the Rest: The Global Productivity Slowdown, Divergence across Firms and the Role of Public Policy’, OECD Productivity Working Papers No. 5, 2016. APEC (2012), ‘ Economic impact of submarine cable disruptions,’ APEC Policy Support Unit, December 2012.

Arbor Networks Inc. (2016), ‘Worldwide Infrastructure Security Report,’ Volume XI, available from https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf (accessed 25 January 2017).

Australian Transport Safety Bureau (2008), ‘In-flight upset - Airbus A330-303, VH-QPA, 154 km west of Learmonth, WA, 7 October 2008’, Investigation number: AO-2008-070, available from http://www.atsb.gov.au/publications/investigation_reports/2008/AAIR/pdf/AO20080 70_interim.pdf (accessed 18 September 2017).

Baily M. & Montalbano N. (2016), ‘Why is US productivity so slow? Possible explanations and policy responses’, Brookings Institute, Hutchins Center Working Paper 22.

Baker J. (2016), 'New EU telco rules will 'fragment' market says Skype, WhatsApp, YouTube,' Ars Technica, http://arstechnica.co.uk/tech-policy/2016/09/skype-whatsapp-youtube-claim-eutelco-rules-will-fragment-market/ (accessed 19 November 2016).

Bradley J., Reberger C., Dixit A. And Gupta V. (2013), 'Internet of Everything: A $4.6 Trillion Public-Sector Opportunity', available from http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf (accessed 17 January 2017).

Brand S. L. and Makey J. (1985), 'Department of Defense password management guideline', CSC-STD-002-85, Department of Defense Computer Security Center, April 1985.

Brown I., Krishnamurthy V. and Swire P. (2015), 'Reforming Mutual Legal Assistance Needs Engagement beyond the US', Lawfare Blog, available from https://www.lawfareblog.com/reforming-mutual-legal-assistance-needs-engagement-beyondus.

Brown T., Beyeler W. And Barton D. (2004), 'assessing infrastructure interdependencies: The challenge of risk analysis for complex adaptive systems,' Int J Crit Infrastruct, 1:108–117.

Brynjolfsson E. And Oh J. H. (2012), 'the Attention Economy: Measuring the Value of Free Digital Services on the Internet,' Thirty Third International Conference on Information Systems, Orlando 2012.

Campbell, Katherine | Gordon, Lawrence A. | Loeb, Martin P. | Zhou, Leitgbj(2011), The impact of information security breaches: Has there been a downward shift in costs. DOI: 10.3233/JCS-2009-0398 -Journal: Journal of Computer Security, vol. 19, no. 1, pp. 33-56, 2011

Clay Wilson Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division CRS report for congress - Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,Updated January 29, 2008 - http://www.dtic.mil/docs/citations/ADA477642

Enisa Report: ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR - November 2011.

European Parliament – Transatlantic cyber-insecurity and cybercrime – Economic impact and future prospects. Members Research Service – Dec 2017 – PE 603.948

Federal Reserve Payments Study Retrieved from https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm

Flater D., Black P. E., Fong E., Kacker R., Okun V., Wood S. & Kuhn D. R. (2016), 'A rational foundation for software metrology,' National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8101.pdf

Florcruz J. (2003), 'China censors SARS report,' CNN, 14 May 2003, available from http://edition.cnn.com/2003/WORLD/asiapcf/east/05/14/sars.censor/ (accessed 17 September 2016).

Florêncio D. and Herley C. (2011), 'Sex, Lies and Cybercrime Surveys,' In Proceedings (online) of the Workshop on Economics of Information Security, June 2011, available from http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf (accessed 20 November 2016).

FTC (2016), 'Consumer Sentinel Network Databook for January – December 2015', February 2016, available from https://www.ftc.gov/reports/consumer-sentinel-network-data-bookjanuary-december-2015 (accessed 10 January 2017).