Cyberattacks on critical infrastructure: an economic perspective

Lis, P. & Mendel, J.

Original citation:
Lis, P & Mendel, J 2019, 'Cyberattacks on critical infrastructure: an economic perspective', Economics and Business Review, vol. 5(19), no. 2, pp. 24-47.
https://dx.doi.org/10.18559/ebr.2019.2.2

DOI 10.18559/ebr.2019.2.2
ISSN 2392-1641
ESSN 2450-0097

Publisher: Sciendo

ISSN 2392-1641

Economics and Business Review

Volume 5 (19) Number 2 2019

CONTENTS

ARTICLES

Optimal growth processes in a non-stationary Gale economy with a multilane production turnpike
Emil Panek

Cyberattacks on critical infrastructure: An economic perspective
Piotr Lis, Jacob Mendel

Lessons from TARGET2 imbalances: The case for the ECB being a lender of last resort
Tomasz Chmielewski, Andrzej Sławiński

Convergence in GDP per capita across the EU regions—spatial effects
Maciej Pietrzykowski

'Dark matter' in the external sector of the United States
Konrad Sobański

Exploring service quality of low-cost airlines in Europe: An integrated MCDM approach
Mahmut Bakır, Şahap Akan, Emrah Durmaz

Poznań University of Economics and Business Press

Paper based publication

ISSN 2392-1641

POZNAŃ UNIVERSITY OF ECONOMICS AND BUSINESS PRESS
ul. Powstańców Wielkopolskich 16, 61-895 Poznań, Poland
phone +48 61 854 31 54, +48 61 854 31 55
www.wydawnictwo.ue.poznan.pl, e-mail: wydawnictwo@ue.poznan.pl
postal address: al. Niepodległości 10, 61-875 Poznań, Poland

Printed and bound in Poland by:
Poznań University of Economics and Business Print Shop

Circulation: 215 copies

sciendo

sciendo

Economics and Business Review, Vol. 5 (19), No. 2, 2019: 24-47
DOI: 10.18559/ebr.2019.2.2

Cyberattacks on critical infrastructure: An economic perspective[1]

Piotr Lis[2]**, *Jacob Mendel***[3]

Abstract: The aim of this article is to analyze the economic aspects of cybersecurity of critical infrastructure defined as physical or virtual systems and assets that are vital to a country's functioning and whose incapacitation or destruction would have a debilitating impact on national, economic, military and public security. The functioning of modern states, firms and individuals increasingly relies on digital or cyber technologies and this trend has also materialized in various facets of critical infrastructure. Critical infrastructure presents a new cybersecurity area of attacks and threats that requires the attention of regulators and service providers. Deploying critical infrastructure systems without suitable cybersecurity might make them vulnerable to intrinsic failures or malicious attacks and result in serious negative consequences. In this article a fuller view of costs and losses associated with cyberattacks that includes both private and external (social) costs is proposed. An application of the cost-benefit analysis or the Return on Security Investment (ROSI) indicator is presented to evaluate the worthiness of cybersecurity efforts and analyze the costs associated with some major cyberattacks in recent years. The "Identify, Protect, Detect, Respond and Recover" (IPDRR) framework of organizing cybersecurity efforts is also proposed as well as an illustration as to how the blockchain technology could be utilized to improve security and efficiency within a critical infrastructure.

Keywords: critical infrastructure, economics of cybersecurity, blockchain, globalized economy, smart grid.

JEL codes: D61, D62, D81, L9, O18.

---

[1] Article received 24 January 2019, accepted 17 April 2019.

[2] School of Economics, Finance & Accounting, Coventry University, Coventry, CV1 5FB, United Kingdom, piotr.lis@coventry.ac.uk, ORCID: https://orcid.org/0000-0001-6060-2423.

[3] The Hogeg Blockchain Research Institute, Coller School of Management, Tel-Aviv University.

Introduction

Continuous functioning of countries, governments, international organizations, corporations and many public services often depends on undisturbed access to a critical infrastructure which in this article is defined as systems and assets, whether physical or virtual, that are so vital that their incapacitation or destruction would have a debilitating impact on national, economic or operational security, as well as public health or safety (NIST, 2017). The technological progress over recent decades means that more and more cyber solutions are being introduced into all aspects of modern life which also leads to an increasing dependence of critical infrastructure on digital systems. Not surprisingly new cyber threats emerge and nations and organizations face vulnerabilities on new fronts which are likely to be amplified by the connectivity of such systems. As Smith (2018) put it, "when everything is being connected, anything can be disrupted". The scale of threats and potential disruptions is further multiplied by ongoing globalization which relies on technological progress and connectivity to reduce the significance of distance and create a global interrelated system (Kowalski, 2013). It is not only the increasing number of cyberattacks on critical infrastructure that is concerning (see US Homeland Security NCCIS, 2015), but also the fact that some governments are learning to use them against other countries by either influencing their domestic political processes or developing cyberweapons that may be used against critical infrastructure. Thus in practice changing the nature of warfare (Smith, 2018). Cyberattacks sponsored by nation-states are highly concerning because they are often conducted by well-funded and highly capable operators and aimed at disabling or damaging another nation's critical infrastructure (Ponemon Institute LLC, 2019).

Finding solutions that could improve the security of critical infrastructure systems and ensure their undisturbed and continuous functioning is becoming one of the major challenges facing individual firms, nations and the global economy as a whole. An obvious area of research is within the strict limits of cybersecurity, or the protection of hardware, software and data from cyberattacks in internet-connected systems (Singer & Friedman, 2014). Nonetheless the development and implementation of technological solutions requires the allocation of scarce resources as well as a development and introduction of certain management processes and organizational culture, meaning that the problem is also interesting from the perspective of economics and management. This motivates the current article in which the aim is to evaluate some of the economic implications of cybersecurity efforts and cyberattacks, explore methods to determine an optimal level of investment in cybersecurity of critical infrastructure and propose potential solutions that could lead to the development of sustainable, efficient and resilient systems.

Cybercrime costs the global economy up to $575 billion annually (Sobers, 2019). The rise of disruptive technologies, such as the Internet of Things (IoT),

and more than 50 billion devices connected to the Internet by 2020 means that the world is facing an increasing risk of cyberattacks. Estimates show that cybercrime extracts up to 20% of the value created by the Internet meaning that as much as $3 trillion of global economic value could be at risk by 2020 (Bank of America Merrill Lynch, 2015). A recent survey revealed that 90% of organizations that rely on operational technology, including critical infrastructure providers, experienced a cyberattack, and half of those organizations suffered downtime as a result of cyberattacks in 2017-2018 (Ponemon Institute LLC, 2019). Going into more detail, 37% of the surveyed organizations reported that malware caused significant disruptions to their operations, 33% admitted experiencing "significant" downtime as a result of a cyberattack and, even more worrying, 23% claimed they had been hit by attacks orchestrated by nation states (Ponemon Institute LLC, 2019). A high profile example[4] of a widespread cyberattack that also affected critical infrastructure is the WannaCry malware attack in May 2017. Within a matter of days it disabled over 250,000 computers in over 150 countries. In the UK the National Health Service (NHS) cancelled more than 19,000 patient appointments as a result, many of them critical operations. Shortly after the NotPetya attack affected a third of computers in Ukraine and eventually impaired international shipping and air delivery operations (Smith, 2018). Both of these attacks involved nation-states using cyberweapons to attack computers on which people rely for their daily lives and which exemplified the above argument of the changing nature of warfare.

It is likely that the scale and cost of cybercrime will continue to rise as more activities and business functions are moved online and to cloud services thus underlining the importance of research into cybersecurity. When it comes to the critical infrastructure domain the issue is further complicated by the fact that many such systems are 10, 20 or more years old and their design was completed before cyber threats emerged, which means that they lack the visibility and cybersecurity policy enforcement layers typical of the more modern IT networks (Ponemon Institute LLC, 2019). In addition significant technological upgrades are difficult to implement as the requirement for the continuous availability of critical infrastructure systems means that operators cannot afford the downtime necessary for some major upgrades and even if downtime is not required, upgrades may be associated with higher unforeseen risks of failures which cannot be mitigated. An electric smart grid, which is an integration of a traditional electrical power network with modern information and communication technology, is a case in point. The objective of the smart grid is to yield an electric grid system that is available at all times, capable of self-healing, self-managing, self-organizing and self-optimizing. Smart grids are becoming an important factor in modern economies, requiring special cybersecurity actions to detect, protect and recover the network from cyberattacks

[4] More examples of cyberattacks are discussed in Section 3.

and avoid or mitigate power outages, power quality problems and service disruptions including operations during a cyberattack.

Ponemon Institute LLC (2019) indicates that although 60% of organizations in the operational technology sector include disruptive cyberattacks among the threats which worry them most, only 48% attempt to quantify the damage a cyberattack could have on their organization and even then the estimates are not likely to reflect the full picture as they tend to consider only the direct impact based on the downtime of attacked systems. One of the reasons why organizations struggle to quantify the economic impact of cyberattacks and cybersecurity efforts is likely to be the lack of clarity in which costs and benefits should be considered as well as the lack of tools and frameworks that could be readily applied to such analysis. Thus this article discusses the types of costs that should be taken into account when deciding the level of cybersecurity efforts. It is argued that operators of critical infrastructure should not only consider the organization's private costs and benefits associated with cybersecurity efforts or flowing from cyberattacks, but should also be mindful of the external costs and benefits and how their decisions may affect other entities and individuals within the economy. In order for this to happen governments should design appropriate regulatory frameworks and incentive structures that aim at optimizing social welfare.

The discussion of the benefits and costs of cybersecurity and cyberattacks leads to the proposal of a cost-benefit analysis approach to determining the optimal level of investment in cybersecurity. In particular the Return on Security Investment (ROSI) measure is presented and it is demonstrated how it could be applied to evaluating the cybersecurity decisions. In simple terms ROSI is defined as the gain from security investment (the amount of risk reduced), less the amount spent on cybersecurity and then divided by that amount spent. Historical data is also reviewed in order to estimate the losses suffered by organizations from cyberattacks in recent years. This exercise is important for establishing the costs and consequences of cyberattacks and the first step towards obtaining results that could be generalized for a wider population of organizations and events. Nonetheless such attempts are severely limited by data availability as not many firms and organizations are willing to reveal that they were attacked or share information on the extent of the damage. Such reports reach the public domain typically when attacks are relatively large and organizations are unable to keep them secret. Furthermore national security may require a layer of secrecy around cybersecurity and cyberattacks in the case of critical infrastructure.

Finally two solutions are proposed that could improve the efficiency and effectiveness of cybersecurity efforts. First, a holistic risk and security management framework, "Identify, Protect, Detect, Respond, Recover" (IPDRR) is discussed, which guides cybersecurity activities and considers them as a part of the organization's risk management process. Its aim is to help organizations to

align their cybersecurity efforts with business requirements, risk tolerances and resources. In addition IPDRR enables organizations, regardless of size, degree of cybersecurity risk or sophistication, to apply the principles and best practices of risk management and improve the security and resilience of their critical infrastructure. The second proposed solution is the integration of blockchain technology into critical infrastructure to provide a secure and stable platform able to continuously and reliably support relevant economic and social activities. Based on the example of an electric smart grid it is argued argue that this technology has the potential to provide a high level of protection for critical infrastructure systems with added benefits of increased economic efficiency. The efficiency gains can be achieved through a development of a fully decentralized energy system in which energy supply contracts are made directly between energy producers (including small-scale owners of domestic solar panels or wind turbines) and consumers. In such an environment the blockchain technology could be a basis for metering, billing, clearing processes, documentation of ownership, asset management, guarantee of origin and renewable energy certificates.

The remainder of this article is organized as follows. Section 1 focuses on the costs and benefits of cybersecurity and difficulties in reliably capturing them. Section 2 considers tools that can be used to evaluate the worthiness of cybersecurity investments. Section 3 reviews and analyzes consequences of selected cyberattacks. Sections 4 and 5 look at potential solutions that could improve the cybersecurity and reliability of critical infrastructure. Finally, the last section summarizes these arguments and concludes.

1. Difficulties in estimating costs and benefits of cybersecurity

A comprehensive approach to the economic aspects of cybersecurity must include a thorough consideration of direct and indirect costs of cybersecurity measures and the expected damage caused by cyberattacks. The direct costs are those incurred directly by owners or providers of critical infrastructure, including repairs to damaged networks and elements. They also include losses suffered by infrastructure users whose operations are immediately affected by cyberattacks. Thus a calculation of direct costs should include losses of equipment, time, production, services, command and control and confidential information suffered by both critical infrastructure operators and its users (Fung, Roumani & Wong, 2013). In extreme cases, for example attacks on the smart grid, disruptions may result in losses of human health and life.

The indirect costs are linked to the economic concept of negative externalities and refer mostly to costs and damages incurred by third parties who are not direct victims of a cyberattack and are not responsible for the maintenance of critical infrastructure elements, but may be their users. For example, follow-

Table 1. The direct and indirect costs of cyber security attacks

Direct costs	Indirect costs
operational disruption, replacement or upgrading of damaged goods and equipment (or infrastructure) including spare parts	a decline in future revenues
a business continuity plan	insurance
cyber security service level agreements	market failures due to cyber-attacks may also impact cyber security regulations which have a consequent economic effect on the market
physical security including: security information and event management (siem), access control procedures and computer room controls	government activities associated with the cyber-attack
business income disruptions	lost productivity
insurance charges	privacy violations and future privacy protection
recruitment (because of special talent requirements potential candidates may not wish to work in a firm which has suffered a cyber-attack)	the recovery process
intellectual property (IP) losses	increased cyber security investment (such as installing additional cyber security technologies and procedures/policies, hiring cyber security experts and adding external audits)
recovery process	reduced foreign investment in the country or region which had the cyber-attack; the cyber-attack may cause investors to move out of the high-risk domain and territories
risk assessment	the economic impact of investors that may look for countries whose governments are pro-actively investing in cyber security
damage to trade name	stock market losses
lost customer relationships and contracts	
loss of human life and health	
lost revenue from disruption to an organization's internet sites/webpages	
it staff and external contractors working to bring organization systems back to full functionality (including on-line systems)	
legal complaints including privacy violation issues	
security product license fees	

Source: (Mendel, 2018).

ing an attack on the electric smart grid indirect costs could be associated with disruptions to supply chains and economic activity as well as ensuing losses of tax revenue. A response to heightened cybersecurity threats may lead to increased costs of doing business brought about by enhancement of government policies and higher electricity prices for end users due to increased security and insurance costs faced by utilities. Table 1 provides a summary of the direct and indirect costs of cyber-attacks.

The not negligible costs of cybersecurity and scarcity of resources available to an organization, as well as across a wider economy, mean that the development of a cybersecurity strategy and implementation of respective efforts should be based on a sound analysis which takes into account risks, expected costs and expected benefits of such efforts. The chief benefit is that secure critical infrastructure is reliable in providing support for the successful and continuous functioning of a modern society, enabling economic and social development. As already noted this reliability tends to be achieved by an integration of advanced Information and Communication Technologies (ICT) in order to design systems which, in addition to being secure, are flexible, efficient and sustainable. Another benefit of introducing ICT, for example in an electric smart grid, is that it enables stakeholders to monitor the performance of even the smallest infrastructure elements in real time, thus providing opportunities for efficiency gains by spotting threats and failures early or identifying and managing periods and areas of increased usage.

However as the scale and complexity of ICT-dependent critical infrastructures increase new threats arise from malicious intruders who could exploit unforeseen loopholes and unexpected system weaknesses to mount cyberattacks leading to potentially devastating effects. For example, one could imagine dire consequences of shutting down a smart grid and ensuing power shortages affecting work of hospitals, road, rail and air traffic control, communication within other infrastructure networks and disruptions to industrial production processes, among others[5]. Conversely highly secured critical infrastructure could improve efficiency and reduce costs to all stakeholders, including suppliers and customers (Fung et al., 2013).

Due to the high degree of asymmetric information and uncertainty in the area of cybersecurity any analysis of costs and benefits associated with cybersecurity and cyberattacks may rely only on approximations and estimations. The dynamic nature of the race between "protectors" and hackers as well as a virtual impossibility to foresee and measure all consequences of cyberattacks

[5] The power outage that occurred in Ukraine in 2015 was the first known power outage caused by a cyberattack. Three energy companies were affected be the event, around 30 substations were switched off and some 225,000 people were without power for one to three hours. The attack was believed to be conducted by "Sandworm", a Russian advanced persistent threat group and occurred during the ongoing conflict between Ukraine and Russia over Crimea (Vijay, Hoikka & Kenneth, 2015).

mean that analysts may base their considerations on expected costs and expected benefits. This presents a serious hindrance because, for example, how does one estimate the economic loss from reduced trust and confidence in the Internet economy due to a series of cyberattacks? Currently there are no ready answers to such questions or agreed practices. Nonetheless this presents a promising field for future research where economic theory and analytical tools are useful.

The development of a holistic economic framework for capturing costs, benefits and consequences of cyberattacks and cybersecurity is also a potentially fruitful starting point for future policymaking. That is because it will enhance the focus on market participants' incentive structures and market externalities. The wealth of opportunities presented by disruptive technologies such as artificial intelligence (AI) cannot be fulfilled without progression in other areas of knowledge, including economics and management. This is likely to be observed also in the area of critical infrastructure where governments and businesses are making major investments in new cybersecurity technologies and boosting resilience of the critical systems. Some of those solutions will prove insightful, even create new jobs and markets, whereas others will present loss in terms of costs (Evans, 2017). A reliable and comprehensive approach is needed to evaluate such investments and ensure that available resources are dedicated to solutions and activities that promise the greatest efficiency gains. The following section makes a step in that direction and discusses a tool that can be used to evaluate the return on security investment.

2. Evaluating the costs and benefits of cybersecurity efforts

Faced with hackers attempting to exploit vulnerabilities in their systems and potentially the considerable ensuing costs of cyberattacks, organizations must decide how much of their scarce resources to devote to cybersecurity. Thus they face a decision-making problem which can be solved using economic frameworks and analytical tools. The approach to the economics of cyber security proposed in the current article is rooted in the rational choice model which is well known to all students of economics.[6] This model can be used to analyze the behaviour of a wide spectrum of economic agents, including critical infrastructure providers, users, governments and regulators as well as hackers and organized crime agents. The economic analysis offers tools enabling the identification and evaluation of expected trade-offs, market failures, efficiencies, welfare effects, including those of information sharing

[6] This cyber security investment problem can be also looked at from the game theory perspective, an approach taken by Gintis (2005), Su (2006), Beasley, Venayagamoorthy and Brooks (2014) and Jentzsch (2016), among others.

among agents and the economic impact of insurance markets and regulation within cybersecurity.

2.1. An operator-centric approach

In the remainder of this article e a firm-centric, or operator-centric, approach is taken and with consideration of the expected costs and expected benefits that critical infrastructure providers derive from their investment in cybersecurity solutions. Those considerations relate not only to the question of how many resources should an operator dedicate to cybersecurity, but also which technological solutions should be chosen to maximize efficiency gains. Intrinsically private firms are likely to take a narrow approach to welfare gains and consider only private costs and benefits of their actions. Not accounting for externalities discussed in the previous section may lead to market failures where non-trivial social costs and benefits of cybersecurity provision are ignored.

The development of a comprehensive toolbox for assessing the effects and implications of various forms of cybersecurity investments requires a thorough understanding of many aspects of cybersecurity, including agents' behaviour and the extent of damages caused by attacks. Unfortunately the existing studies of economics of cyber security suffer from a number of limitations (see OECD, 2009a, for a more comprehensive review). First, they provide limited insights into how actors actually perceive expected costs and expected benefits and the incentives which they face. The difficulty of estimating tangible benefits leads to a problem of making a business case for spending on cybersecurity (Jentzsch, 2016). Second, existing literature struggles to consider dynamic and learning effects, such as how a loss of reputation changes the incentives. Third, they often treat issues of institutional design as rather trivial. Fourth, the existence of potential positive and negative externalities from cyber security efforts is too often neglected.

Nonetheless economic literature on the subject has been growing in recent years and shedding light on some important aspects of cyber security, including the drivers of organizations' investment in cyber security. According to various authors when determining the amounts of resources spent on cyber security and protection against cyber-attacks firms mainly focus on the aims of protecting customer data and privacy (Louis, Adrian & Evangelos, 2016), the protection of intellectual property, trade secrets or other business assets (Klahr et al., 2017), ensuring business continuity and preventing downtime (Bernik & Prislan, 2016), compliance with laws and regulations (Wakefield, 2012) and protecting the organization's reputation (Lloyd's, 2015).

Irrespective of their security priorities, firms, which are assumed to be rational and profit-maximizing agents, require tools to assess the efficiency of their efforts and whether their scarce resources bring the best possible return. In the following section one such tool is presented.

2.2. Return on Security Investment (ROSI)

There are several models for the calculation of the Return on Security Investment (ROSI), which are also called security metrics or cyber threat metrics. As a starting point, the Return on Investment (ROI) is defined as follows:

$$ROI = \frac{Gain\ from\ investment - Cost\ of\ investment}{Cost\ of\ investment}.$$

Senior management of any organization wants to know the impact that cybersecurity has on the organization's net income. In order to determine how much should be invested or spent they need to know the expected costs of not implementing certain cybersecurity measures, the costs and benefits if implemented and what are the most cost-effective solutions. The classical financial approach based on the ROI calculations is not particularly appropriate for answering those questions. Cybersecurity investment does not generally result in profit as it focuses mainly on loss prevention or reducing the risks. In such cases the Return on Security Investment (ROSI) allows the calculation as to how much loss is avoided thanks to the investment (ENISA, 2012). The ROSI measure provides quantitative answers to essential economic questions: Is an organization investing too much or too little in cyber security? What is the economic impact on an organization if there is no investment in cyber security? When is the cyber security investment enough?

To obtain the ROSI indicator the single loss expectancy (SLE) has to be defined as the expected amount of money that is lost when a risk occurs. In other words SLE is the total cost of an incident with a single occurrence. Due to the specific nature of cybersecurity incidents the major complexity is to consider all the asset on which s an incident has a direct or indirect impact. For example, a stolen laptop will not only result in the cost of its replacement but may also infer productivity loss, reputation loss, IT support time as well as loss of data and intellectual property. The total cost of an incident should include the cost of direct losses (e.g. website downtime, hardware replacement, data loss replacement, temporary loss of data, corruption of the system or software, permanent change of data, lost access to a third-party system, money or intellectual property stolen) as well as the cost of indirect losses (investigation time, loss of reputation and image, etc.). The ROSI calculation relies on many approximations as the cost of cybersecurity incidents and annual rate of occurrence are hard to estimate and the resulting numbers can vary significantly from one environment to another. These approximations are often subjective and biased by personal perception of the risk, meaning that the ROSI calculation can be easily manipulated. The accuracy of statistical data used in the ROSI calculation is therefore essential. However organizations tend to be reluctant to provide data on security incidents (ENISA, 2012) which means that there is an

absence of actuarial tables from which information on damages based upon real cases can be derived (Jentzsch, 2016). The lack of data makes it difficult to evaluate and justify cybersecurity investments which are often seen as costs.

Another relevant measure is the annual rate of occurrence (ARO) which is the probability that a risk occurs within a year. Combining SLE and ARO the annual loss expectancy (ALE) is obtained which is the annual monetary loss that can be expected from a specific risk on a specific asset. It is calculated as follows (ENISA, 2012):

$$ALE = ARO \cdot SLE.$$

An alternative, but nonetheless similar, approach to the calculation of ALE has been proposed by Su (2006):

$$ALE = \sum_{i=1}^{n} I(Oi)F_i,$$

where O_i represents a harmful outcome i, $I(O_i)$ is the impact of that outcome in monetary units and F_i is the frequency of occurrence of outcome i.

The calculation of ROSI combines the quantitative risk assessment and the cost of implementing security countermeasures against this risk. As such ROSI can be defined as:

$$ROSI = \frac{Monetary\ loss\ reduction - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}.$$

In practice ROSI compares ALE with the expected loss saving and is based on three variables: ALE estimated risk mitigation and cost of the solution being implemented. The latter is relatively easy to determine (provided all indirect costs are considered), while the two other variables can at best be based on estimations. Implementing an effective security solution lowers ALE; the more effective that solution is, the more ALE is reduced. The monetary loss reduction can be defined as the difference between ALE without the security solution being implemented and ALE with the relevant implementation, i.e. $ALE_{no\ security} - ALE_{with\ security}$ (Bojanc & Jerman-Blažič, 2008):

$$ROSI = \frac{(ALE_{no\ security} - ALE_{with\ security}) - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}.$$

The same result can be obtained by multiplying ALE by the risk mitigation ratio of the solution applied to obtain the value of the monetary loss reduction. In this case the ROSI formula can be written as (ENISA, 2012):

$$ROSI = \frac{ALE \cdot Mitigation\ ratio - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}.$$

Let us consider the following hypothetical example. A power utility firm is considering investing in an Intrusion Detection System (IDS). Each year the firm suffers 18 cyber-attacks (ARO = 18). The economic cost estimates of each attack are approximately $3,940 in loss of productivity (SLE = 3940). The IDS solution is expected to block 85% of the attacks (mitigation ratio = 85%) and costs $17,000 per year (due to license fees, trainings, installation, maintenance etc.). ROSI for this solution can then be calculated as follows:

$$ROSI = \frac{(18 \cdot 3{,}940) \cdot 0.85 - 17{,}000}{17{,}000} = 155\%.$$

Thus, according to this measure, the IDS solution is cost-effective because the investment is expected to generate value greater than its cost (ROSI > 100%). The higher the value of ROSI, the more worthwhile the security investment.

As previously highlighted the limits of ROSI lie in the difficulty of reliably estimating costs of cyberattacks and their annual rate of occurrence. The resulting numbers can vary highly from one environment to another. These approximations are often biased by the evaluator's perception of the risk. ROSI does not readily uncover the quantified cost-benefit of individual security countermeasures. The ALE element is also flawed in that it assumes that all security breaches carry the same cost implications. If the expected annual cost of security failures is, e.g. $10 million and the security system is thought to be 85% effective, it does not necessarily follow that the security system will save $8.5 million. If a particularly expensive type of breach falls into the 15% of incidents against which the security solution is ineffective, then the ALE estimate will be overly optimistic (Lockstep Consulting, 2004).

The following section attempts to estimate losses suffered by various organizations from cyberattacks in recent years and establish the consequences of such attacks. Given the abovementioned lack of relevant actuarial tables this exercise is the first step towards obtaining results that could be generalized for a wider population of organizations and events and thus used in the evaluation of monetary losses required to calculate ROSI.

3. The cost and impact of selected cyberattacks

The impact of security incidents can be significant for the organizations affected (Rebecca & Rob, 2019). Although in some cases the direct financial costs of the breach may be covered by cyber insurance policies the damage to the reputa-

tion, relationships within the industry and the impact on users and employees may be long lasting, hard to measure and difficult to repair. As mentioned before economic analysis should consider all expected costs and expected benefits of providing cybersecurity to critical infrastructure and the costs ought to include losses and damages from attacks which are not prevented. One of the biggest challenges in performing a systematic and robust analysis enabling researchers to generalize results is the lack of openly available and reliable information on cyberattacks as relevant organizations and governments are often reluctant to reveal information on such attacks (OECD, 2009b; Council of Economic Advisers, 2018). This can be motivated by the desire to keep evidence of an occurred incident hidden to protect the reputation of the provider or not to cause unnecessary panic when it concerns critical infrastructure networks. The sensitivity of the data is another reason as to why organizations may want to avoid further leakages of knowledge about their system's weaknesses. In some cases, for example when it comes to the smart grids, the reason for limited data availability on attacks may be the scarcity of such systems (Marotta, Martinelli, Nanni, Orlando & Yautsiukhin, 2017).

Driven by those data limitations this article analyzes historical cybersecurity incidents from a range of industries, not necessarily within the critical infrastructure domain, where more information is available. It is expected that the economic impact of those incidents should, to some extent, be a good indication of the consequences of cyber-attacks on critical infrastructure. According to OECD (2015), the digital security threat landscape continues to evolve, sustained by often profitable business models such as ransomware. The most prominent strain of ransomware is "CryptoLocker" which is spread via email attachments. Experts estimate that "CryptoLocker" infected some 234,000 computers, extracting more than $27 million in ransom payments during its first two months of operation (OECD, 2015).

The Target, Home Depot, JPMorgan Chase and Sony Pictures Entertainment breaches are examples of how destructive malware can be to organization's reputation and financial stability (Ponemon Institute LLC, 2015). Moreover the severity and frequency of malware attacks exhibits an upward tendency. In a typical week an organization can receive an average of nearly 17,000 malware alerts. The time to respond to these alerts is a severe drain on an organization's financial resources and IT security personnel. The average cost of time wasted responding to inaccurate and erroneous intelligence can average $1.27 million annually. Of those 17,000 alerts only 19% are considered to be reliable and merely 4% are investigated (Ponemon Institute LLC, 2015).

According to the findings by FireEye (2013) malware has become a multinational activity. For example in 2012 alone, callbacks were sent to Command and Control (C&C) servers in 184 countries. Whenever personal data are being collected, stored or processed, security incidents can heavily affect privacy and also generate significant costs to firms as well as to users (OECD, 2013).

When combined with the payments arising from pending lawsuits and other relevant measures taken to reduce the direct and indirect damages the cost per data entry stolen can provide a simplified measurement of the level of risks faced by companies storing personal data, standardized by the overall amount of data entries stored.

The TJX[7] data breach involving around 100 million records forced TJX to set aside $118 million to cover costs and potential liabilities in 2008, i.e. $1.18 per record. This included $11 million (9% of the total amount) in security consultancy fees and other attack-related expenses and a contingency fund of $107 million to cover liability payments arising from pending lawsuits. The impact of the intrusions was estimated to be a 57% reduction in the firm's net income compared to the earlier year (OECD, 2013). This, however, did not cover losses in reputation, impact on the brand and other indirect and opportunity costs.

Another example is the data breach at Heartland Payment Systems (HPS)[8] involving around 130 million records in 2009. As a consequence of this breach HPS agreed to set up a fund worth $105 million to cover liability payments ($0.80 per record). Of this amount $41 million (39%) was dedicated to MasterCard customers, $60 million (57%) to VISA customers and almost $4 million (4%) to American Express customers. How much HPS spent on security-related investments as well as the indirect costs remains unknown but the financial statement for 2009 revealed that the firm had a net loss of more than $52 million (compared to a net profit of $42 million a year earlier), even though the revenues increased by 7%. Furthermore its stock prices dropped from $15.44 on 16 January to $8.54 on 23 January, two days after revealing the breach (OECD, 2013).

Another high profile example of a cyberattack is the security breach in Sony's PlayStation Network and Sony Online Entertainment in 2011. It resulted in an exposure of some 103 million records and, as a consequence, a 23-day closure of the PlayStation Network. According to Sony's executives this data breach cost the company at least $171 million, or $1.7 per record (OECD, 2013). This number does not cover liability payments, as in the previous cases, but rather "includes expenses of an identity theft prevention program and promotional packages to win back customers, among other things" (Goodin, 2011). In other words, it covers (parts of) the indirect reputation and opportunity costs. Under the assumption that Sony would also have to set aside a fund worth $1 per record to cover liability payments arising from pending lawsuits an additional $103 mil-

[7] The TJX Companies Inc. is an off-price retailer of apparel and home fashions in the U.S. and worldwide, ranking number 87 in the 2017 Fortune 500 listings, with over $33 billion in revenues in 2016, more than 3,800 stores in nine countries, and three e-commerce sites (source: http://www.tjx.com/company/).

[8] Heartland Payment Systems is a Princeton (New Jersey)-based bank card payment processor for merchants in the United States (Flick & Morehouse, 2010).

lion would have had to be provided. This would still not include investments in security assessment and enhancing initiatives (e.g. security consultancy fees).

The cost of data breaches is not limited to the firms suffering from the breach but also includes the costs consumers have to pay. For example, it is estimated that 10% of Americans have had their identities stolen and each of those individuals lost around $5,000 on average (O'Dell, 2011). Similarly it is estimated that also one in ten Australians fell victim of online identity theft, losing an average of $790. In the United Kingdom almost two million people have their identities stolen every year at a cost of $3.48 billion to the national economy. With criminals gaining an average of $1,289 for each name they steal a large share of the costs suffered by the victims goes directly to the criminals, whereas the rest is made up of the resources dedicated by individuals and companies to preventing and detecting the crime and putting right the damage. In serious cases it can take more than 200 hours to resolve problems caused by identity fraud (OECD, 2013).

So far the discussion has identified a clear knowledge gap, namely, the lack of a holistic framework for the implementation and management of cybersecurity and analysis of its results and consequences within critical infrastructure. The following section proposes such a framework for organizing cybersecurity efforts.

4. The "Identify, Protect, Detect, Respond and Recover" framework

A comprehensive framework for enhanced development, implementation and management of cybersecurity should result in an increased resilience of critical infrastructure systems, but also lead to decisions that ensure the most efficient use of resources. Thus the holistic "Identify, Protect, Detect, Respond and Recover" (IPDRR) framework is suggested which focuses on using business drivers to guide cybersecurity activities and considers cyber threats as a part of the organization's risk management process. The framework consists of a set of activities and outcomes that are common across the critical infrastructure sector and provides detailed guidance for developing individual organizational profiles. Nonetheless it is not a one-size-fits-all approach to managing cybersecurity for critical infrastructure as organizations face unique risks driven by specific threats, vulnerabilities and risk tolerances. Instead the proposed framework should be perceived as a set of guidelines and principles that each organizations can adapt to its unique and specific needs. Thus organizations ought to determine activities that are important to critical service delivery and then prioritize investments to maximize the impact per dollar spent. The framework provides a common taxonomy and mechanism for organizations to: (1) describe their current cybersecurity position; (2) determine their cybersecurity

targets; (3) identify and prioritize opportunities for improvement within the context of business continuation; and (4) communicate existing cybersecurity risks to internal and external stakeholders.

The IPDRR framework consists of five concurrent and continuous functions shown in Figure 1. When considered together these functions provide a strategic view of the lifecycle of an organization's management of cybersecurity, which can help organizations to structure their risk management, cyber threat environment, legal and regulatory requirements, business objectives and organizational constraints. Figure 1 presents the aims and outcomes that are characteristic for these five functions, along with typical levels of priority assigned to each of them for maintaining continuous functioning of critical infrastructure which is disrupted as little as possible in case of a cyberattack.

The IPDRR framework organizes the risk management process into a chain of ongoing activities of identifying, assessing and responding to risks, depicted in Figure 2. To manage risks, organizations should understand the probability of an event and the likely extent of its impact. Then they can determine their risk tolerance, i.e. the acceptable level of risk for continuous delivery of services. Risks may be handled in various ways, including mitigation, transfer, avoidance or acceptance, depending on the expected impact on critical services.

Following the "road map" in Figure 2 the IPDRR framework can be used to develop an action plan to strengthen existing cybersecurity practices or to create new cybersecurity programmes. It can also be used to identify opportunities for new or revised guidelines, procedures or practices, including a common set of reporting and communication standards that could enhance the coordination of efforts across different departments of an organization or with its external stakeholders and consequently reduce the threats to the continuous delivery of essential critical infrastructure services.

5. Blockchain and cybersecurity of critical infrastructure

Since blockchain technology is considered to improve cybersecurity and provide a high level of privacy protection (Kshetri, 2017) its adoption to a critical infrastructure system could reduce the risk of breaches while being cost efficient (Rogers & Henderson, 2019) and speedy. Before discussing how this technology could be applied to securing critical infrastructure against cyber threats its basic concepts and principles will be briefly explained.

5.1. The basics of blockchain

Blockchain is a type of distributed, electronic database, a ledger, which can hold any information (e.g. user data records, critical events information, banking transactions or device service history) and set rules on how this informa-

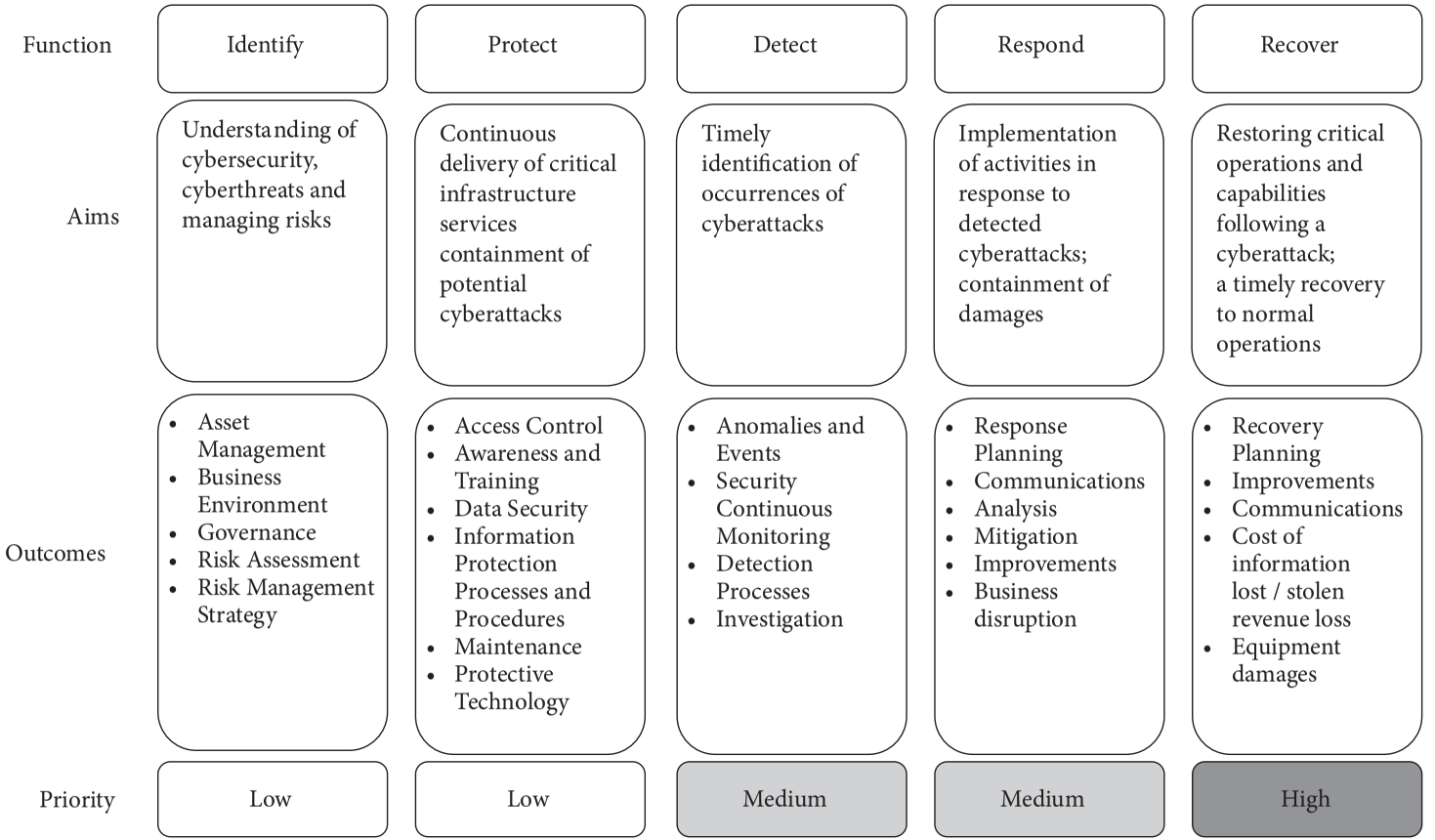

Figure 1. The "Identify, Protect, Detect, Respond and Recover" framework
Source: (Mendel, 2018).

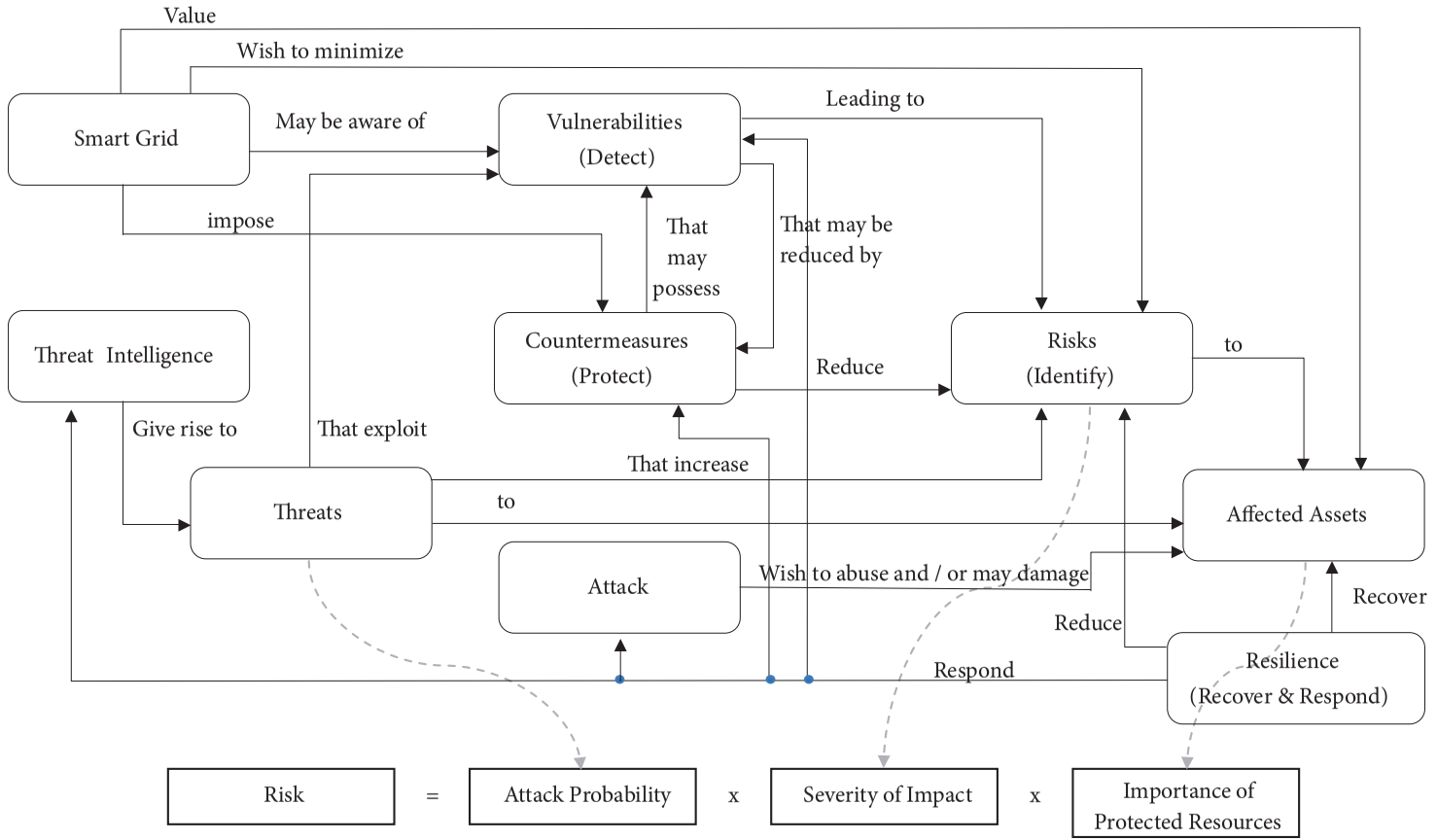

Figure 2. Operationalizing the IPDRR framework
Source: (Mendel, 2018).

[41]

tion can be updated. The blockchain continually grows as blocks of data are appended and linked (chained) to the previous block of data using a cryptographic hash function.[9] The ledger is validated and maintained by a network of participants (nodes) according to a predefined consensus mechanism so no single centralized authority is needed. Multiple (but not necessarily all) nodes hold a full copy of the entire blockchain database (Sikorski, Haughton & Kraft, 2017). This means that if an attacker tries to penetrate a blockchain network and corrupts one node there are many other redundant and identical copies of the ledger stored on different computers that can provide valid information. Arguably there is no single point of failure in the blockchain and for hacking to be successful more than 50% of nodes need to be hacked simultaneously.

The main difference between blockchain and a traditional database is the way in which records evolve over time. The blockchain system allows multiple participants to submit new data to the distributed ledger and then consensus[10] is used to determine which state of the data is valid. In a traditional database multiple participants can submit new data but only one counterparty is relied on to provide the valid state of the database. A drawback of the blockchain technology is that it consumes significant amounts of energy although a number of consensus mechanisms that lower electricity consumption has been developed in recent years (see Conti, Kumar, Lal & Ruj, 2017).

5.2. Application of blockchain in critical infrastructure

Blockchain technology has the potential to provide robust and strong cybersecurity solutions and a high level of protection for critical infrastructure systems. It can handle data in such a way that they can only be seen by users with specific permissions and proofs of identity are stored in a cryptographic format. The security is enhanced by maintaining two distinct ledgers: a ledger with individually encrypted data; and a transaction ledger which stores encryption access keys to the related data. Each access to the data is recorded and stored, it can also be timed or restricted to a certain number of attempts or entries. This means that third parties, such as other critical infrastructure providers, financial institutions or government agencies, may get permission to access only specific documents at specific times. Blockchain technology can improve the security of critical infrastructure by functioning as a cost-effective tool to

[9] The hash function is a one-way function, i.e. it is very difficult to reverse an operation and derive the original input data. Additionally it is unfeasible for two different data inputs to result in the same hash value which means that in order to alter an entry in a past block all subsequent blocks also need to be altered. If one computer's blockchain updates are breached, the blockchain system will reject this computer data.

[10] A consensus protocol is a mechanism through which all users within a blockchain system agree on the validity of the data. Importantly all parties must agree to a single "true" version of information.

track and secure the complete history of data transactions. If a security breach is discovered, thanks to its multi-node structure, the blockchain technology can facilitate data recovery and data integrity.

As an example let us consider a case of a smart grid system with decentralized energy generation, where electricity can be traded directly among network users via a blockchain system. In such a setup the blockchain can facilitate the making of smart contracts directly between energy producers and consumers while enabling the latter to also produce their own electricity and sell it within the smart grid. Thus a party that is predominantly an energy consumer, for example a household with rooftop solar panels, can also play the role of a micro-producer in such a system. The blockchain technology could ensure the efficiency of this smart grid by providing a secure basis for metering, billing, clearing, documentation of ownership, asset management, guarantee of origin and renewable energy certificates, among others. It could create a fully automated energy market with near real-time settlement, for example, if the customer fails to pay, the smart contract would automatically suspend the power supply. If all transactions are recorded on regulated ledgers it might be possible to implement prudential regulations or automatically restrict new transactions to solely green energy sources.

There are several drivers behind the adoption of distributed ledger technology in critical infrastructure systems, including the smart grid. The first of them is the pursuit of cost reductions by taking advantage of the opportunity to unplug legacy systems and reduce the number of layers required for data sharing. By ensuring that data is natively in digital format and shared at the point of transaction the transaction time will be shortened. The second one is risk-management. By providing a standardized framework for transaction recording critical infrastructure providers can make risk management much simpler and respond to changes in near real time. Regulatory compliance is the third driver where the technology can ensure that only authorized transactions are conducted in line with the rule of law.

Using blockchain technology in critical infrastructure systems could bring benefits beyond the security considerations. For example, in the case of the electric smart grid, it could result in a cost reduction to customers' energy bills due to reduced profit margins between suppliers and customers, lower operating costs for meter reading and billing and no or reduced certification costs for renewable electricity. An additional benefit of using the blockchain technology is a greater transparency for consumers who could readily track where the electricity they purchase was produced or what percentage share of energy supplied is from renewable sources.

Furthermore reduced barriers to entry, transaction costs and simpler billing processes could enable new energy providers to enter the energy markets and break predominant monopolies. The possibility of selling energy by consumers who operate their own renewable energy sources, such as rooftop solar

systems or small-scale wind turbines, would improve the economic viability of such solutions, provide a growth impulse for the green energy sector, improve market resilience and competition as well as having a positive effect on the natural environment.

In order to ensure privacy protection in critical infrastructure systems employing blockchain-based solutions the system should be designed in a way that keeps the private information visible only to authorized entities and blocks unauthorized access to transactions. In addition, the blockchain system should use multiple digital signatures for authorizing and encryption of the transactions so only the counterparties involved are able to access the whole information (the ledger can be encrypted with more than one key). Government regulation is likely to be one of the most significant factors determining whether blockchain technology will flourish within critical infrastructure systems. In many areas, including the smart grid, blockchain technology is still in its infancy, which means that it comes with a range of uncertainties, risks and problems that remain to be solved.

Conclusions

The fast pace of technological progress over recent decades has meant that the functioning of modern states, firms and individuals increasingly relies on digital or cyber technologies and this trend has also materialized in various facets of critical infrastructure. Nowadays critical infrastructure presents new cybersecurity area of attacks and threats that requires the attention of regulators, governments as well as service providers. Deploying critical infrastructure systems without suitable cybersecurity might make them vulnerable to intrinsic failures or malicious attacks, and result in serious negative consequences for a nation or firm due to, for example, instability of crucial utilities, energy fraud, loss of user information or other critical data. This means that cybersecurity efforts should focus on ensuring availability, reliability, efficiency and self-healing of critical infrastructure systems.

To date there is no agreed and uniform approach to estimating economic damage from cyberattacks against critical infrastructure or benefits of adequate cybersecurity provision. The picture is complicated by the high degree of uncertainty and asymmetric information inherent to security problems and risk management, as well as the difficulty in capturing relevant external costs and benefits of cybersecurity activities or their lack. Furthermore each sector has a different loss model requiring a special dedicated analysis, thus, one-fits-all solutions are not feasible. The danger is that if a specific problem is not assigned an accurate monetary value it may not receive an economically optimal amount of attention and resources, leading to losses in economic efficiency and welfare. This paper argues that critical infrastructure providers, and governments

should ensure that a holistic cost-benefit analysis of cybersecurity efforts, taking into account internal and external costs, should be an integral part of their decision making. This could be aided by tools such as ROSI. Nonetheless any indicator can be only as reliable as the information fed into it. Currently the lack of representative data on cyberattacks means that there are no actuarial tables from which information on damages and their probabilities could be derived. Additionally the data scarcity prevents analysts from estimating the extent of external costs and benefits associated with cybersecurity and cyberattacks thus making it difficult to design functioning mechanisms for internalizing externalities. Once these two elements are determined the proposed measure of returns on security investment could be augmented to give a more reliable tool in deciding which cybersecurity solutions are optimal.

Critical infrastructure providers often do not have sufficient incentive to scale up their cybersecurity to reflect its external impacts beyond the organization. This creates a significant space for government intervention, regulatory frameworks and legal requirements for implementing and maintaining certain cybersecurity standards. The holistic "Identify, Protect, Detect, Respond and Recover" (IPDRR) framework of organizing cybersecurity efforts within an organization as well as an illustration of how blockchain technology could be utilized to improve the security of critical infrastructure are proposed. These proposals could be used as guidance for both critical infrastructure providers in their daily operations as well as authorities in the development of appropriate regulatory frameworks. In order to ensure security of their nations governments must work closely with technology firms, including critical infrastructure operators, who are likely to act as first responders to security challenges. Recent years have shown that cyber technology has become a new battlefield and, since cyber space is often owned by private technology firms, maintaining security and peace requires that governments, private firms and organizations work together.

References

Bank of America Merrill Lynch. (2015). *Global cybersecurity primer*.

Beasley, C., Venayagamoorthy, G. K., & Brooks, R. (2014). Cyber security evaluation of synchrophasors in a power system. *IEEE Computer Society*, 1-5.

Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLOS ONE*, *11*(9), 1-33.

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413-422.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2017). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416-3452.

Council of Economic Advisers. (2018). *The cost of malicious cyber activity to the U.S. economy*. Washington, DC: The White House. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

ENISA (2012). *Introduction to return on security investment*. Athens: European Union Agency for Network and Information Security.

Evans, G. L. (2017). Disruptive technology and the board: The tip of the iceberg. *Economics and Business Review*, *3*(1), 205-223.

FireEye. (2013). *The advanced cyber attack landscape*. Milpitas, CA: FireEye, Inc.

Flick, T., & Morehouse, J. (2010). *Securing the smart grid: next generation power grid security*. Burlington, MA: Elsevier.

Fung, C. C., Roumani, M. A., & Wong, K. P. (2013). A proposed study on economic impacts due to cyber attacks in smart grid: A risk based assessment. *IEEE Power and Energy Society General Meeting*, 1-5.

Gintis, H. (2005). Behavioral game theory and contemporary economic theory. *Analyse & Kritik*, *27*(1), 48-72.

Goodin, D. (2011). *PlayStation Network breach will cost Sony $171m*. Retrieved from https://www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/

Jentzsch, N. (2016). State-of-the-art of the economics of cyber-security and privacy. *IPACSO Deliverable D*, 4.

Klahr, R., Shah, J., Sheriffs, P., Rossington, T., Pestell, G., Button, M., & Wang, V. (2017). *Cyber security breaches survey 2017. Main report.* Retrieved from http://www.ipsos-mori.com/terms

Kowalski, T. (2013). *Globalization and transformation in Central European countries: the case of Poland*. Poznan: University of Economics Press.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027-1038.

Lloyd's. (2015). *Business blackout. Lloyd's Emerging Risk Report–2015*. Cambridge: University of Cambridge Judge Business School.

Lockstep Consulting. (2004). *A guide for government agencies calculating return on security investment. Version 2.0*. New South Wales Department of Commerce, Government Chief Information Office, Sydney, Australia. Retrieved from http://nla.gov.au/nla.arc-111462

Louis, M., Adrian, B., & Evangelos, R. (2016). *Threat landscape 2015*. Athens: European Union Agency for Network and Information Security (ENISA).

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35-61.

Mendel, J. (2018). *The economic perspective on smart grid cyber security*. (Unpublished doctoral dissertation). Poznań: Wydawnictwo Uniwersytetu Ekonomicznego.

NIST. (2017). *Proposed updates to the framework for improving critical infrastructure cybersecurity*. Gaithesburg, MD: National Institute of Standards and Technology.

O'Dell, J. (2011, January 29). How much does identity theft cost?. *Mashable*. Retrieved from https://mashable.com/2011/01/28/identity-theft-infographic/

OECD. (2009a). *Computer viruses and other malicious software. a threat to the internet economy*. Paris: OECD Publishing. Retrieved from https://doi.org/10.1787/9789264056510-en

OECD. (2009b). Malware: why should we be concerned?. In *Computer viruses and other malicious software: A threat to the Internet economy*. Paris: OECD Publishing. Retrieved from https://doi.org/10.1787/9789264056510-5-en

OECD. (2013). Exploring the economics of personal data. *OECD Digital Economy Papers*, (220), 40.

OECD. (2015). *OECD digital economy outlook 2015*. Paris: OECD Publishing. Retrieved from https://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm

Ponemon Institute LLC. (2015). *The cost of malware containment*. Traverse City, MI: Ponemon Institute Research Report.

Ponemon Institute LLC. (2019). *Cybersecurity in operational technology: 7 insights you need to know*. Traverse City, MI: Ponemon Institute Research Report.

Rebecca, S., & Rob, B. (2019, January 10). America's electric grid has a vulnerable back door and Russia walked through it. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

Rogers, M., & Henderson, K. (2019, April 10). How blockchain can help the utility industry develop clean power. *Sustainability blog*. McKinsey & Company. Retrieved from https://www.mckinsey.com/business-functions/sustainability/our-insights/sustainability-blog/how-blockchain-can-help-the-utility-industry-develop-clean-power

Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, (195), 234-246.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. New York, NY: Oxford University Press.

Sobers, R. (2019). 60 must-know cybersecurity statistics for 2019. *Inside Out Security Blog*. New York, NY: Varonis. Retrieved from https://www.varonis.com/blog/cybersecurity-statistics/

Smith, B. (2018, Novemebr 18). Government and business must fight the cyber threat. *The Financial Times*.

Su, X. (2006). *An overview of economic approaches to information security management. Technical Report TR-CTIT-06-30*. Retrieved from http://www.ub.utwente.nl/webdocs/ctit/1/00000177.pdf

US Homeland Security NCCIC. (2015). *Seven strategies to defend ICSs*. Washington, DC: US Department of Homeland Security. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Vijay, S., Hoikka, H., & Kenneth, B. (2015). *Ukraine 2015 power grid cyberattack. ELEC-E7470 Cybersecurity L-Case Study*. Aalto: Aalto University. Retrieved from https://mycourses.aalto.fi/pluginfile.php/457047/mod_folder/content/0/Cyber%20Warriors.pdf?forcedownload=1

Wakefield, M. (2012). *Guidebook for cost/benefit analysis of smart grid demonstration projects*. Palo Alto, CA: Electric Power Research Institute. Retrieved from https://www.smartgrid.gov/files/Guidebook-Cost-Benefit-Analysis-Smart-Grid-Demonstration-Projects.pdf

Aims and Scope

The Economics and Business Review is a quarterly journal focusing on theoretical and applied research in the fields of economics, management and finance. The Journal welcomes the submission of high quality articles dealing with micro, mezzo and macro issues well founded in modern theories and relevant to an international audience. The EBR's goal is to provide a platform for academicians all over the world to share, discuss and integrate state-of-the-art economics, finance and management thinking with special focus on new market economies.

The manuscript

1. Articles submitted for publication in the **Economics and Business Review** should contain original, unpublished work not submitted for publication elsewhere.
2. Manuscripts intended for publication should be written in English, edited in Word in accordance with the **APA editorial** guidelines and sent to: secretary@ebr.edu.pl**.** Authors should upload two versions of their manuscript. One should be a complete text, while in the second all document information identifying the author(s) should be removed from papers to allow them to be sent to anonymous referees.
3. Manuscripts are to be typewritten in **12' font in A4 paper** format, one and half spaced and be aligned. Pages should be numbered. Maximum size of the paper should be up to 20 pages.
4. Papers should have an abstract of not more than 100 words, keywords and the Journal of Economic Literature classification code (**JEL Codes**).
5. Authors should clearly declare the aim(s) of the paper. Papers should be divided into numbered (in Arabic numerals) sections.
6. **Acknowledgements** and references to grants, affiliations, postal and e-mail addresses, etc. should appear as a separate footnote to the author's name a, b, etc and should not be included in the main list of footnotes.
7. **Footnotes** should be listed consecutively throughout the text in Arabic numerals. Cross-references should refer to particular section numbers: e.g.: See Section 1.4.
8. **Quoted texts** of more than 40 words should be separated from the main body by a four-spaced indentation of the margin as a block.
9. **References** The EBR 2017 editorial style is based on the **6th editio**n of the Publication Manual of the American Psychological Association (**APA**). For more information see APA Style used in EBR guidelines.
10. **Copyrights** will be established in the name of the **E&BR publisher**, namely the Poznań University of Economics and Business Press.

More information and advice on the suitability and formats of manuscripts can be obtained from:

Economics and Business Review
al. Niepodległości 10
61-875 Poznań
Poland
e-mail: secretary@ebr.edu.pl
www.ebr.edu.pl

Subscription

Economics and Business Review (E&BR) is published quarterly and is the successor to the Poznań University of Economics Review. The E&BR is published by the Poznań University of Economics and Business Press.

Economics and Business Review is indexed and distributed in Claritave Analytics, DOAJ, ERIH plus, ProQuest, EBSCO, CEJSH, BazEcon, Index Copernicus and De Gruyter Open (Sciendo).

Subscription rates for the print version of the E&BR: institutions: 1 year – €50.00; individuals: 1 year – €25.00. Single copies: institutions – €15.00; individuals – €10.00. The E&BR on-line edition is free of charge.