European Journal of Sustainable Development (2018), 7, 4, 171-178 ISSN: 2239-5938
Doi: 10.14207/ejsd.2018.v7n4p171

Cybersecurity as an Essential Sustainable Economic Development Factor

Ioana Vasiu[1], Lucian Vasiu[2]

ABSTRACT
Technological developments facilitated an impressive growth in international trade; however, organizations are facing numerous risks, resulting from their reliance on digital services and complex supply chains. One of the most notable risks concerns cybersecurity, which can take numerous forms and can have very significant negative consequences for the victims. This reality makes cybersecurity a major differentiator for organizations and an essential sustainable economic development factor. This paper employs an empirically-informed theoretical approach, and, based on a large corpus of data, consisting essentially of cases brought to courts, cybersecurity reports, and press releases, examines the main cybersecurity risks, grouped in three broad categories: damage, theft of trade secrets, and payment fraud. In each category, the main issues are illustrated with real case examples. The findings of this study underline the need for improved cybersecurity strategies, policies, and programs. The paper proposes a number of measures that must be taken, in order to provide conditions for a safer and better economic development environment.

Keywords: Cybersecurity, E-Commerce, Sustainable Development, Damage, Trade Secret, Fraud, Loss

1. Introduction

Impressive leverages of information and communication technologies (ICT) allow efficient exchanges of data, streamlining of operations, virtualization of numerous products and services, and the adoption of diverse electronic payment methods. These, in turn, create conditions for the emergence of new trade approaches, models, functionalities, and, potentially, new sales channels and markets.

Creative business models are constantly remodeling or reshaping the business strategy, making it increasingly "modular, distributed, crossfunctional, and global business processes that enable work to be carried out across boundaries of time, distance, and function" (Bharadwaj et al., 2013: 472). These developments continuously change the value creation process, enabling new, innovative approaches to international trade, ranging from expanded e-service functions and personalization to higher business process integration and digitization of supply networks or chains.

The expanding capabilities, innovation orientation, and value offerings (Chuang & Lin, 2017), created ideal conditions for electronic commerce (e-commerce) to take the forefront role, now representing an important and continuously expanding part of the international trade. The figures published recently strongly support this assertion: in the European Union (E.U.), for instance, the percentage of e-shoppers reached 55% and, during 2016, one out of five enterprises in the E.U. made electronic sales, the annual e-sales turnover amounting to 18% of the total turnover of organizations with at least 10

| [1] Prof. Dr., Faculty of Law, Babeş-Bolyai University. Corresponding Author.
| [2] Independent Information Systems Security Expert.

employees (European Commission, 2017). In the United States (U.S.), the retail e-commerce sales for the first quarter of 2017 amounted to $105.7 billion (U.S. Census Bureau, 2017). Worldwide-figures are even more impressive, business-to-consumer (B2C) sales reaching close to $2.3 trillion (eMarketer, 2017), while according to estimates by the United Nations Conference on Trade and Development (UNCTAD, 2016), between 2013 and 2015 the value of online trade accelerated upwards, from $16 trillion to $25.3 trillion.

Clearly, e-commerce, by allowing the broadening or diversification of exports, fosters inclusion, facilitates access by micro, small and medium enterprises (MSMEs) to the international trade (OECD/WTO, 2017), and has the potential to act as a major economic development component. In fulfilling this potential, e-commerce could play an important role in validating United Nations' 2030 Sustainable Development Goals (SDGs) approach, according to which the international trade "is an engine for inclusive economic growth and poverty reduction, and contributes to the promotion of sustainable development." (U.N. General Assembly, 2015). However, to make this tremendous promises come to fruition, the role played by ICT and the potential risks associated could be very well understood and effectively managed.

The ICT role with respect to development (ICT4D) is commonly discussed along ecological, social, and economic dimensions (Hilty & Hercheui, 2010). This paper takes a different approach, and discusses cybersecurity challenges that could negatively impact e-commerce and, by consequence, the sustainable economic development. The paper aims to provide an understanding of the main cybersecurity risks, identify their actual or potential effects, and outline the main aspects that should be considered, from a prevention and recovery perspective.

Specifically, based on a large corpus of data, consisting of cases brought to courts, cybersecurity reports, and official press releases, this paper outlines some of the main cybersecurity risks faced by e-commerce organizations: damage, trade secret theft, and payment fraud, all presenting a global dimension or reach. In each category, the main issues are illustrated with real case examples, then the implications of this study are presented.

2. Cybersecurity Risks

There are numerous risks that organizations engaged in e-commerce face, such as financial, legal, supply chain, safety, and security. The security risk presents several components or dimensions, one of the most concerning is the cybersecurity risk.

The high level of inter-connectivity, which characterizes modern society and the international trade, has opened many avenues for cyber attacks, rendering cybersecurity an issue of major concern for all organizations (World Economic Forum, 2018; Günther, 2017; Baesens et al., 2014). Even though, in recent years, there were notable advances in the understanding and mitigation of cyber risks, as empirical data shows, the number of incidents augmented and continued to grow in sophistication, becoming more thorough and inflicting often major losses (IDG, 2017). Through advanced tools, tactics and procedures (TTP), such as SQL injection; malware infection; advertisement click fraud; business e-mail compromise (BEC); and exploitation of zero-day vulnerabilities, used in

watering hole attacks, cyber criminals pose major threats to organizations and citizens.
Cyber incidents have the potential to very negatively affect organizations' activity, economic development, and users' privacy and other fundamental rights. With that in mind, it comes as no surprise that cybersecurity, according to a recent survey of IT Leaders' Personally Most Important/Worrisome IT Management Issues, is now the number one concern for managers (Kappelman et al., 2017), consequently regarded as critical to all e-commerce organizations (Rothrock, Kaplan & Van Der Oord, 2018).

In order to outline the complexity and magnitude of the problem, the next subsections discuss some of the most important facets of cybersecurity risk, underlining essential aspects, such as victimization and incidence, losses involved, and consequences for victims.

2.1 Damage

Computer data is essential for the proper functioning of organizations. Successful damage or impairment attacks can negatively impact the integrity and availability of data and/or information systems. Whether in the form of impairment, sabotage, subversion, or intrusion, these attacks can inflict direct and proximate harm on a significant scale. This fact is reflected in a recent survey of business continuity professionals from 80 countries, which identified "cyber attacks" as the fourth most significant cause of business disruption, while "data breach" was ranked the ninth most important source of disruption (Business Continuity Institute, 2017).

While the intent and motive that drive damage attacks vary significantly, often the motivation is represented by revenge or retaliation (Vasiu & Vasiu, 2014). Such malicious acts or actions, nevertheless, can have behind hacktivism, the perpetration of other crimes, usually to derive profit, or the attempt to cover, render untraceable or unrecoverable incriminating evidence of previously perpetrated offenses (Vasiu & Vasiu, 2014).

The examination of cases in this category revealed the prevalence of attacks aiming to hinder data availability (Vasiu & Vasiu, 2014). However, the survey of cases also uncovered a significant number of attacks where system resources were exhausted or data was corrupted, with certain notable instances of disk-wiping malware usage (Symantec Corporation, 2017).

Major cybersecurity incidents, such as, for instance, the ones occurred at Target, Equifax, Yahoo!, or Home Depot, can result in exposure of personally identifiable information (PII) of many millions of consumers, including dates of birth, cell phone numbers, zip codes, or method of payment details, some posted subsequently on the Darkweb, for sale (In Re Equifax, 2018; In Re Yahoo!, 2018).

Recent cases show that insider sabotage, which can result in unavailable services or servers, or loss of connectivity to certain data centers (United States v. Brown, 2018; United States v. Shahulhameed, 2018), or infiltration of organizations, through malware implants into the supply chain, is on the increase (Symantec Corporation, 2017).

An important subcategory here is represented by the Distributed Denial of Service (DDoS) attacks. These attacks, often difficult to block, send requests which aim to overwhelm the victim's system, exhausting resources and rendering it inaccessible or incapable to properly respond to legitimate requests. Even more difficult to counteract are the DDoS attacks that employ simultaneously multiple attack vectors (for example, the Operation Ababil, which employed three attack strategies).

To maximize the impact on victim's system, perpetrators often employ botnets, which can consist of millions of computers. For instance, the Sirefef botnet (aka ZeroAccess), contained about 2 million infected computers, with over 800,000 active on any given day (Microsoft, 2013). Another recent prominent example is Mirai, made up of numerous Internet of Things (IoT) devices, used in several major DDoS attacks (Symantec Corporation, 2017).

More and more concerning are the DDoS-for-hire attacks, advertised in criminal forums and available on dark webmarkets. These attacks are often carried out via cybercrime tools, especially botnets, phishing, or spear-phishing emails, false websites, and deceptive telephone numbers. The aim of such attacks is to infect victim's systems with malicious code, to remotely control victims' computers and capture victims' keystrokes (United States v. Yücel, 2015), or to make the affected systems part of botnets; to steal confidential information or property from victims; to misappropriate intellectual property; or to undertake other types of activity, that aims to harm the victims (Microsoft Corporation v. Does 1-8, 2015; United States v. Panin, 2013). Spam botnets-for-hire, such as Necurs, for example, allowed ransomware groups to launch massive e-mail campaigns (Symantec Corporation, 2017).

2.2 Theft of Trade Secrets

In today's economy, information and know-how, usually the result of very significant research and development investments, creativity, and initiatives, are often essential factors in the development and preservation of competitive advantages.

Trade secret protection broadly encompasses the following categories: technical data; confidential business information, including clients' contact information, pricing information, prior purchase history, product preferences and habits; and know-how. The theft of trade secrets is wide-spread, overall, according to estimates, the theft of trade secrets costs up to $300 billion per year (Almeling et al., 2010).

Misappropriation of trade secrets can take the form of economic espionage, which benefits a foreign state or instrumentality, and theft for pecuniary gain, which benefits an individual or an organization (Vasiu & Vasiu, 2017). This threat come from numerous sources, such as current or former employees, competitors, clients, suppliers, and hackers (Vasiu & Vasiu, 2017).

As numerous cases demonstrate, insiders pose a significant concern in this regard. In United States v. Pani (2013), for instance, the defendant, already working for a competitor of the victim company, downloaded files containing top secret information, valued at about $1 billion. In another high profile case (United States v. Aleynikov, 2010), the defendant, close to the end of his employment with the victim company, misappropriated computer source code valued at $500 million.

The theft of trade secrets affects all major economic sectors, and can result in very significant economic and other harm to the owner of the trade secret, as well as to others. Successful or attempted trade secret theft may result in loss of sales, costs for internal investigation, negotiating settlements, prosecution and litigation, and higher disbursement for security measures. In United States v. Sinovel (2015), for instance, the defendant misappropriated source code from the victim company, then used it in the operation of wind turbines. As consequences of the trade secret theft, victim's annual turnover fell by 75%, the stock price dropped by 90% and it was forced to reduce its workforce by 70% (Vasiu & Vasiu, 2017).

2.3 Payment Fraud

"The main category of proceeds-generating crime on the Internet – as in the real world – is fraud, that is, the intentional deception causing loss of property to another person for economic gain." (Council of Europe, 2012: 21). Financial gain is by far the most powerful motivation behind payment frauds, however, these offenses can also be encountered as hacktivism (Vasiu & Vasiu, 2014).

Financial losses, due to cyber heist or fraud, can be massive, and can affect organizations from all industries, particularly the banking sector. For instance, the Carbanak group, targeted hundreds of banks, in several countries, the total amount stolen being estimated at $1 billion (Symantec Corporation, 2017). The Banswift group, by exploiting weaknesses in bank's security, infiltrated the network and obtained transaction credentials, managing to steal $81 million from Bangladesh's central bank (Symantec Corporation, 2017). In another recent major case, roughly 500,000 computers were infected globally with malware, conceived to obtain victims' sensitive banking credentials, with a view to conduct fraudulent wire transfers (U.S. Department of Justice, 2016).

The U.S. Federal Reserve (2017) payments study supplement reveals an accelerated use of credit cards. This payment method, however, is very vulnerable to a variety of frauds (Vasiu & Vasiu, 2015). Moreover, the criminal proceeds in credit card fraud cases can be very large (Federal Trade Commission, 2018), with massive actual or potential losses of many millions of dollars. This aspect is very concerning, as a high level of credit card fraud can negatively impact consumers trust.

There are scores of cases in which massive credit card details were obtained illegally. In United States v. Watt (2010), for example, the conspirators have stolen the details of 40 million credit cards; the Target data breach resulted in 40 million customers' credit card details stolen and made available on the web (Internet Society, 2016); in United States v. Miralles (2013), the defendant downloaded from the Internet 26,418 stolen credit card numbers.

These cases often present trans-border aspects. In United States v. Ivanov (2001), for example, the perpetrator hacked from a remote jurisdiction into the computer system of an e-commerce firm and obtained credit card numbers and merchant account numbers. Even more concerning are the global cybercriminal enterprise cases. The highly anonymized underground market (Darknet) is host to "hidden services", such as underground forums and criminal marketplaces. A number of cases show perpetrators trading card numbers through dedicated sites. The Infraud Organization, for example, engaged in the dissemination of stolen identities, credit cards numbers, and other financial data, inflicted approximately $2.2 billion in intended losses, and more than $530 million in actual losses (U.S. Department of Justice, 2018).

3. Implications for Organizations

The most obvious results of cybersecurity incidents are financial losses, however, cyber incidents can also result in costly recovery or remediation and, in certain cases, litigation; serious harm to consumers' privacy, resulting in potential fines, imposed on the basis of regulations, such as the General Data Protection Regulation (GDPR), which can amount to 20 million euros or 4% percent of an organization's worldwide turnover; impaired organizational operational integrity, infringement of intellectual property rights, and bad reputation.

Cyber incidents can also very negatively affect "trust", a very important social capital indicator and an determining factor of economic growth (Hamilton, 2006). As Oliveira et al. (2017: 161) explain, "firm characteristics (reputation and brand recognition), lack of integrity, privacy and security and likability (website infrastructure), and interactions (service quality and customer satisfaction), are the major sources of trust that influence the three dimensions of consumer trust, namely: competence, integrity and benevolence; which explains that overall trust has a direct effect on intention to purchase online."

The causes of cybersecurity incidents, as made clearly in the previous section, are numerous, multifaceted, and, often, intricated. Successful cyber attacks are usually the result of various problems, such as software vulnerabilities, poor authentication, exploitation of trust mechanisms, insufficient awareness of cybersecurity risks, or administrative errors.

The ability to manage the cybersecurity risk is essential for organizations' success. In order to effectively be part of the solution to cyber risks, it is imperative that organizations make extensive vulnerability or weakness analysis mandatory (Savaglia & Wang, 2017). Cybersecurity measures must commensurate with the level of risks identified. Risk assessment should identify essential data and functions, as well and their importance to the organization, paying particular attention to high-value assets.

In designing responses to the cybersecurity risks, organizations must address factors such as vulnerability assessments; threat level; human aspects; and physical environment security. Cybersecurity should comprise technical, operational, and administrative controls. These controls must include clear policies and procedures regarding the protection of and access to valuable data, activity logging, and restoring of the normal state or functioning of systems after cyber incidents; software updating; encryption of data at rest and in transit; behavior analytic systems; periodic evaluation of access lists and rights, and of incident response and recovery plans; confidentiality agreements; adequate training and awareness programs regarding the cybersecurity risks, for all those in charge of protecting the data and systems; adequate contracts with all ICT suppliers. The effectiveness of controls in place must be reassessed regularly, with respect to the identified risks.

Conclusion

The adoption of ICT is changing virtually every aspects of our lives. ICT and connectivity can drive up productivity, innovation, and growth in the international trade, hence significantly contributing to the achievement of the United Nations' 2030 SDGs.

However, these benefits come at a cost, namely the cybersecurity risk.
Organizations face numerous types of cybersecurity incidents. This paper outlined some of the main cybersecurity risks faced by e-commerce organizations. Cyber attacks can very negatively impact the fundamental security attributes of integrity, availability, and confidentiality, resulting in disrupted or delayed services or activities, financial loss, and overall distrust in electronic transactions. Cyber attacks continue to evolve and, in order to keep data and systems in a protected state, significant and effective measure must be taken.
Measures that aim to control the cybersecurity risk are not just of a technical nature. Legal, regulatory, and organizational measures must also be considered, in order to have a truly effective approach. These measures must include adequate laws; mandatory legal or industry standards; awareness-raising programs and public service announcements; skills development programs; dissemination of best practices; establishment of specialized agencies; and effective forms of international law enforcement cooperation.

References

Almeling, D.S., Snyder, S.W., Sapoznikow, M., McCollum, W.E., & Weader, J. (2010). A Statistical Analysis of Trade Secret Litigation in Federal Courts. *Gonzaga Law Rewiew, 45*, 291-334.

Baesens, B., Bapna, R., Marsden, J.R., Vanthienen, J., & Zhao, J.L. (2014). Transformational issues of big data and analytics in networked business. *MIS Quarterly, 38 (2)*, 629–632.

Bharadwaj, A., El Sawy, O.A., Pavlou, P. A., & Venkatraman, N. (2013). Introduction: Digital Business Strategy. *MIS Quarterly, 37(2)*, 471-482.

Business Continuity Institute (2017). Horizon Scan Report 2017.

Chuang, S.-H. & Lin, H.-N. (2017). Performance implications of information-value offering in e-service systems: Examining the resource-based perspective and innovation strategy. *Journal of Strategic Information Systems, 26,* 22–38.

Council of Europe (2012). Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction, *MONEYVAL 6*.

eMarketer (2017). Worldwide Retail and Ecommerce Sales: eMarketer's Estimates for 2016–2021. Retrieved from https://www.emarketer.com/Report/Worldwide-Retail-Ecommerce-Sales-eMarketers-Estimates-20162021/2002090

European Commission (2017). E-commerce Statistics. Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics

Federal Trade Commission (2018). Consumer Sentinel Network Data Book 2017.

Günther, W.A. (2017). Debating big data: A literature review on realizing value from big data. *Journal of Strategic Information Systems, 26*, 191–209.

Hamilton, K. (2006). Where is the wealth of nations?: Measuring capital for the 21st century. World Bank Publications.

Hilty, L.M., & Hercheui, M.D. (2010). ICT and sustainable development. In What kind of information society? Governance, virtuality, surveillance, sustainability, resilience (pp. 227-235). Springer, Berlin, Heidelberg.

IDG (2017). 2017 U.S. State of Cybercrime.

In Re Equifax, Inc., Customer Data Security Breach Litigation, MDL No. 2800 (Judicial Panel Mar. 20, 2018).

In Re Yahoo! Inc. Customer Data Security Breach Litigation, No. 16-MD-02752-LHK (N.D. Cal. Mar. 9, 2018).

Internet Society (2016). Global Internet Report 2016.

Kappelman, L., Nguyen, Q., McLean, E., Maurer, C., Johnson, V., Snyder, M., and Torres, R. (2017). The 2016 SIM IT Issues and Trends Study. *MIS Quarterly Executive, 16:1*, 47-80.

Microsoft Corporation v. Does 1-8, Civil No. 1: 14-cv-811 (E.D. Va. Aug. 17, 2015).

Microsoft (2013). Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet.

OECD/WTO (2017). Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development, WTO, Geneva/OECD Publishing, Paris.

Oliveira, T., Alhinho, M., Rita, P., & Dhillon, G. (2017). Modelling and testing consumer trust dimensions in e-commerce. *Computers in Human Behavior, 71*, 153-164.

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The Board's Role in Managing Cybersecurity Risks. *MIT Sloan Management Review, 59 (2)*, 12-15.

Savaglia, J. & Wang, P. (2017). Cybersecurity vulnerability analysis via virtualization. *Issues in Information Systems 18(4)*, 91-98.

Symantec Corporation (2017). Internet Security Threat Report.

UNCTAD (2016). UNCTAD B2C E-commerce Index 2016, UNCTAD Technical Notes on ICT for Development N°7. TN/UNCTAD/ICT4D/07, United Nations, http://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d07_en.pdf

U.N. General Assembly (2015). Transforming our world: the 2030 Agenda for Sustainable Development, A/RES/70/1.

U.S. Census Bureau (2017). Quarterly Retail E-Commerce Sales 1st Quarter 2017.

U.S. Department of Justice (2016). Avalanche Network Dismantled in International Cyber Operation. Retrieved from https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation

U.S. Department of Justice (2018). Thirty-Six Defendants Indicted For Alleged Roles In Transnational Criminal Organization Responsible For More Than $530 Million In Losses From Cybercrimes. Retrieved from https://www.justice.gov/usao-nv/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organizationf

U.S. Federal Reserve (2017). Federal Reserve Payments Study.

United States v. Aleynikov, 737 F. Supp. 2d 173 (S.D.N.Y. 2010).

United States v. Brown, No. 16-11340 (5th Cir. Mar. 1, 2018).

United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001).

United States v. Miralles, No. 12-14603, 521 F. App'x 837 (11th Cir. June 6, 2013).

United States v. Shahulhameed, Criminal Action No. 5: 12-CR-118-KKC-REW (E.D. Ky. Jan. 8, 2018).

United States v. Sinovel Wind Grp. Co., Ltd., 794 F.3d 787, 789 (7th Cir. 2015).

United States v. Pani, 2013 U.S. 1st Cir. Briefs Lexis 362 (2013) (No. 12-2054).

United States v. Panin, No. 1:11-CR-0557-AT-AJB (N.D. Ga. June 26, 2013).

United States v. Watt, 707 F. Supp. 2d 149, 152 (D. Mass. 2010).

United States v. Yücel, 97 F. Supp. 3d 413 (S.D.N.Y. 2015).

Vasiu, I., & Vasiu, L. (2017). Backdoor Man: A Radiograph of Computer Source Code Theft Cases. *Journal of High Technology Law, 18 (1)*, 1-37.

Vasiu, I. & Vasiu, L. (2015). Riders on the Storm: An Analysis of Credit Card Fraud Cases. *Suffolk Journal of Trial & Appellate Advocacy, 20*, 185-218.

Vasiu, I., & Vasiu, L. (2014). Break on Through: An Analysis of Computer Damage Cases. *Pittsburgh Journal of Technology Law & Policy, 14*, 158-201.

World Economic Forum (2018). The Global Risks Report 2018. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.