STRATEGIC ASSESSMENT OF CYBER CRIMES CONTROL THROUGH CYBER SECURITY AND RESILIENCE BY CYBER SECURITY CENTER, A CASE STUDY OF THE NIGERIA EXPERIENCE

By

Dr AKPAN, E. Ebenezer, *FCICN, AP, PPGDCA, PHDCDPM*
Corporate Institute of Research and Computer Science
140 Ikot Ekpene Road
Uyo, Akwa Ibom State.

ABSTRACT

This study assessed "Strategic assessment of cyber crimes control through cyber security and resilience by Cyber Security Center. A case study of the Nigeria experience", Two specific research objectives were formulated to guide the study. The research design was descriptive survey design. 200 respondents comprising all professionals in computer science, computer engineering and security agents who have been exposed to computer science were randomly selected for the study, using stratified random sampling technique. The instrument known as "Cyber Security and Resilience Questionnaire" (CSRQ)." was used to collect the data. The instrument used for the research was made to pass through face and content validation using experts in computer, Cronbach Alpha reliability technique to measure level of reliability of the instrument and it produced high average reliability coefficient of 0.92 to justify the use of the instrument. The findings revealed that there is significant difference in the perception of people as regards the effect of cyber security and cyber resilience in reducing cyber risk in Nigeria. It was concluded that Nigeria as other parts of the world, has suffered greatly in Cyber attack and that cyber security and resilience has become useful tool to checking and stopping cyber risks and with Cyber security and resilience our society is protected against cyber risk., one of the recommendation was that Countries should build upon the work of the Global Community Engagement and Resilience Fund (GCERF) which supports local, community-level initiatives aimed at strengthening resilience against cyber attacks.

Key Words: Cyber security, cyber attack, cyber risks, cyber resilience, Social studies

INTRODUCTION

Technology adoption is driving business growth and innovation in Nigeria, at the same time it is exposing the country to new and emerging threats. Cyber-terrorists, spies, hackers and fraudsters are increasingly motivated to target our ICT infrastructure due to the increasing value of information held within it, and the perceived lower risk of detection and capture in conducting cybercrime as compared to more traditional crime. According to Global Commission on Internet Governance (2015), internet usage has been rapidly rising in Africa, as more people connect to the inter-web mostly through their mobile phones. This increased use has created a new challenge for the continent in potential attack vectors at both individual and organizational level. Juwah (2015) opine that with the increasing availability and utilisation of internet facilities, threats in the cyber space have also escalated dramatically. Criminals are invading homes and offices not by breaking doors and windows but by breaking into laptops, Personal Computers

and wireless devices through the internet. The global economic loss due to cybercrimes and cost of systems repairs as a result of cyber attacks runs into billions of naira every year.

According to Kaplan, James and Tucker (2015), the global digital economy, democracy and the public sphere now completely depend upon the stability and security of cyberspace. Encryption technologies are necessary to protect data privacy, authenticate websites and secure online transactions. Security problems such as consumer data breaches and denial-of-service attacks disrupt the digital economy and the public sphere. They also can have chilling effects on speech and online behaviour. Perlroth and Nicole (2016) asserts that as everyday physical objects from cars to home appliances increasingly become internet-connected, human safety in the real world also depends upon cyber security. Trust in digital infrastructure is now necessary for the capacity to communicate, access knowledge, use one's banking system, drive a car and buy products through an online commerce site such as Amazon. Democracy also depends upon cyber security, considering the stunning admission by United States intelligence agencies about Russia's influence campaign, probing of voter rolls and hacking of Democratic National Committee emails during the 2016 presidential campaign.

Cyber security is one of the great human rights issues of our time. Cyber security is not only an issue for "Internet users" but for all citizens. Even someone who has never been online is directly affected when a retail company they frequent (for example, Target or Home Depot) experiences a massive consumer data breach, when their television potentially becomes a surveillance tool or when they are denied medical care because of a ransomware attack that cryptographically locks medical records and otherwise disables health care provider systems. All people and all societies are now directly affected by the security of digital systems (Schneier and Bruce, 2016).

Debates on cybercrime and cyber security tend to concentrate around dramatic events such as the defacement of popular online spaces, sensitive information leaks or diffusion of particularly infectious malware (Schneier and Bruce, 2016). Less attention has been paid to broader issues of cyber resilience, that is, an organization or government's capability "to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain, and unexpected threats from activities in cyberspace" (ISACA, 2014). Cyber Resilience refers to the idea that failures will inevitably occur, but promotes the adoption of holistic, cooperative measures that ensure a system does not wholly collapse.

The EVC have noted that if users are to benefit from the full advantages of the internet, confidence in the information infrastructure is of utmost importance. "Cyber threats such as malware, cyber harassment, spoofing, phishing, spam, hacking, viruses, Trojans, worms, child online pornography and spyware are becoming extremely sophisticated. This is especially true with increased presence of organised online criminal groups. The internet has long ceased to be the exclusive domain of the technically savvy users. User friendly software and interfaces enable all types of users including novices and children to interact remotely. This new territory contains a goldmine of valuable information and potential victims. The complicated infrastructure of the internet, also makes it more difficult to track down criminals".

Juwah (2015) revealed that the commission receives complaints frequently from International Criminal Investigation Organisation (ICIO), Police and EFCC on cybercrimes committed by some Nigerians on the internet both locally and abroad. He opined that though, national measures are being taken by individual nations, cyber threats remain basically an international problem. "The internet is a borderless communication tool and consequently, any solution to secure it must involve global collaborations. Loopholes in legal framework are being

exploited by perpetrators as harmonization between existing laws across nations is far from satisfactory. Cross border investigation and prosecution are difficult if categorization of crimes differ from country to country. This study therefore seeks to assess cyber security and resilience in Nigeria.

Statement of Problem

The current security framework and the threat landscape detrimental to National Security and economic development have grown beyond the contemporary domain of land, sea, air, and space. Cyberspace have ushered in new opportunities with its security challenges. The role of sovereign nation-states in addressing cyber security is in a state of flux. On the one hand, these states have an interest in preserving the security of critical infrastructure. On the other hand, they are not cyber resilient enough. Studies have shown that the internet has overtaken the television in the number of audience at prime time, totaling over two billion users worldwide with well over 200 million websites. Despite the growing number of Nigerian users running into millions, the country's leaders are not paying enough attention to various activities in the cyberspace. As cyber threats become more complicated, the role of institutions such as computer security incident response teams (CSIRTs) become more important. This study therefore assesses cyber security and cyber resilience in Nigeria.

Objectives of the study

The following specific objectives were formulated for this work:

1. To determine the strategies used in strengthening Cyber Security and Resilience against Cyber Risk in Nigeria.
2. To find out the extent Cyber Security and Cyber Resilience help in reducing cyber risk in Nigeria.

Research Questions

1. What are the strategies used in strengthening Cyber Security and Resilience against Cyber Risk in Nigeria?
2. To what extent have Cyber Security and Cyber Resilience helped in reducing cyber risk in Nigeria?

Research Hypothesis

1. There is no significant difference in the perception of people as regards the effect of cyber security and cyber resilience in reducing cyber risk in Nigeria.

Significance of the Study

This study will enhance security services in their battle to tackle cyber risks, threats and crime in the nation. The findings will expose people to various cyber security activities and threats as well as create a plat form to the public for the awareness of cyber resilience and strengthening of cyber resilience. It is also obvious that the study will be useful to the businesses and organizations in that they will know how to effectively combat this menace of cyber-attacks in the country by enforcing cyber security measures to protect sensitive information of clients as well as safeguard national security.

Policy makers and government will gain insight on cyber threats proffer the expected remedy. The study will also provide basis for reference in future research. Teachers and students

will find this study valuable as they will gain knowledge and carry out further security studies on the topic.

LITERATURE REVIEW

Concept of Cyber Resilience

According to Cassim (2011), the concept of cyber resilience underlines the need for broad, concerted and comprehensive approaches to cyber security, but in reality, the implementation of measures to curb cyber attacks has been selective and driven by narrower agendas. Cyber resilience refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events and that with it risk is certainly reduced (Howell and Lind, 2009). Ploch (2010) assert that cyber resilience is an evolving perspective that is rapidly gaining recognition. The concept essentially brings the areas of information security, business continuity and (organizational) resilience together. Entities with potential need of cyber resilience abilities include; IT systems, critical infrastructure, business processes, organizations, societies and nation-states. Adverse cyber events are those that negatively impact the availability, integrity or confidentiality of networked IT systems and associated information and services. These events may be intentional (e.g. cyber attack) or unintentional (e.g. failed software update) and caused by humans or nature or a combination thereof (Greenwald, 2014).

The objective of cyber resilience is to maintain the entity´s ability to deliver the intended outcome continuously at all times. This means even when regular delivery mechanisms have failed, such as during a crisis and after a security breach. The concept also includes the ability to restore regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of new risks. Backups and disaster recovery operations are part of the process of restoring delivery mechanisms. The objective is therefore maintaining as much normalcy as possible or returning to that level as quickly as possible following a cyber attack (Stremlau and Osman, 2015). Resilience, as defined by Presidential Policy Directive PPD-21, is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Cyber resilience focuses on the preventative, detective, and reactive controls in an information technology environment to assess gaps and drive enhancements to the overall security posture of the entity.

The African Union Convention on Cyber Security and Personal Data Protection, which offers continental reference to improve cyber preparedness in Africa, has also raised concerns that in the charged political climate characterizing many countries on the continent, the heightened emphasis on security and state-led responses may impact free speech and privacy as governments that have been criticized for their abuses gain enhanced abilities to police the cyber world (Macharia, 2014). The possibility that personal data could be processed without subjects giving free and informed consent delineate scenarios where users may be stripped of their ability to be in control of their data and, on the contrary, be controlled in the name of agendas they had little voice in shaping (Access, 2014).

Concept of Cyber Security

Ravi (2003) asserts that cyber security is the protection of systems, networks and data in cyberspace and is essential even as more people get connected to the internet across the world. The International Telecommunications Union [ITU] defines Cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber

environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."

The ITU also notes that the three broad security objectives are ensuring Availability; Integrity (which may include authenticity and non-repudiation), and Confidentiality. While these are the bedrock of a secure network, achieving these three objectives is no mean feat as it requires the integration of various functions such as robust systems engineering and configuration management; effective cyber security or information assurance policy and comprehensive training of personnel. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment - the internet (Steffani, 2006). Cyber Security can also be described as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access (Thilla, 2012).

Functions of a Cyber Security Center:

Ideally, a Cyber Security Center should strive to ensure a secure and resilient cyber and communications infrastructure that supports national/ regional security, a vibrant economy, and the health and safety of all citizens. To achieve this, a Cyber Security Center ought to:

- Serve stakeholders as a national center of excellence and expertise for cyber and telecommunications security issues.
- Focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the Nation;
- Pursue whole-of-nation operational integration by broadening and deepening engagement with its partners through information sharing to manage threats, vulnerabilities, and incidents.
- Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact.
- Maintain a sustained readiness to respond immediately and effectively to all cyber and telecommunications incidents of national security.
- Protect the privacy and constitutional rights of the citizens in the conduct of its mission.

Concept of Cyber Risk

Cyber risk can be defined as the risk connected to activity online, internet trading, electronic systems and technological networks, as well as storage of personal data. According to Deloitte Advisory Cyber Risk Services (2013), the fundamental things that organizations undertake in order to drive performance and execute on their business strategies happen to also be the things that actually create cyber risk. This includes globalization, mergers and acquisitions, extension of third-party networks and relationships, outsourcing, adoption of new technologies, movement to the cloud, or mobility.

Cyber risk is an issue that exists at the intersection of business risk, regulation, and technology. Events covered by this more comprehensive definition can be categorized in multiple ways. One is intent. Events may be the result of deliberately malicious acts, such as a hacker carrying out an attack with the aim of compromising sensitive information, but they may

also be unintentional, such as user error that makes a system temporarily unavailable (www.reuters.com). Risk events may come from sources outside the organization, such as cybercriminals or supply chain partners, or sources inside the organization such as employees or contractors. Combining these two dimensions leads to a practical framework for inventorying and categorizing cyber risks into:

Internal Malicious: Deliberate acts of sabotage, theft or other malfeasance committed by employees and other insiders. For example, a disgruntled employee deleting key information before they leave the organization.

Internal Unintentional: Acts leading to damage or loss stemming from human error committed by employees and other insiders. For example, in 2013, NASDAQ experienced internal technology issues that caused backup systems to fail.

External Malicious: The most publicized cyber risk; pre-meditated attacks from outside parties, including criminal syndicates, hacktivists and nation states. Examples include network infiltration and extraction of intellectual property, and denial-of-service (DoS) attacks that cause system availability issues, business interruptions, or interfere with the proper performance of connected devices such as medical devices or industrial systems.

External Unintentional: Similar to the internal unintentional, these cause loss or damage to business, but are not deliberate. For example, a third party partner experiencing technical issues can impact system availability, as can natural disasters.

Difference between Cyber Security and Cyber Resilience

According to Ravi (2012) Cyber security consists of technologies, processes and measures that are designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyber attack and protects entities, organisations and individuals from the deliberate exploitation of systems, networks and technologies while Cyber resilience looks at a wider scope where it comprises cyber security and business resilience. Greenwald (2014) asserts that Cyber security is effective without compromising the usability of systems and there is a robust continuity business plan to resume operations, if the cyber attack is successful.

Ploch (2010) is of the view that Cyber resilience helps businesses to recognize that hackers have the advantage of innovative tools, element of surprise, target and can be successful in their attempt. This concept helps business to prepare, prevent, respond and successfully recover to the intended secure state. This is a cultural shift as the organization sees security as a full-time job and embeds best security practices in day-to-day operations. In comparison to cyber security, cyber resilience requires the business to think differently and be more agile on handling attacks.

Thomas, Karas, Lori, Parrott (2008) assert that while the term “cyber security” is as old as the hills in the security world, the term “cyber resilience” has been gaining momentum. This is a good thing as cyber security management is complex and always changing. Focusing on security alone simply isn’t enough – organizations need a more comprehensive strategy. The best approach for IT security is to have a balanced, resilient approach that encompasses threat prevention and adaptability to new types of threats combined with built-in durability and fast recovery. This is the approach organizations should focus on for all business-critical IT systems, especially their most mission-critical business application.

According to a research from Vanson and Bourne (2012), only 30 percent of organizations surveyed have adopted a cyber resilience strategy, and only one-third of those are

in the early stages of development or planning. Too many organizations are leaving themselves exposed to the unknown – but it doesn't have to be this way. By developing a more holistic approach organizations can safeguard against email-borne cyber attacks, business disruption, data loss and human error.

Strategies to Strengthen Cyber Security and Cyber Resilience in Nigeria

Based on the World Economic Forum (2012) research findings, most Nigerian organisations are ill-equipped to respond to information security threats. Although there are different initiatives (regulators, government and private organisations) in place set out to address information security issues in Nigeria, these initiatives cannot adequately address the current information security issues. Public and private organisations need to rethink their whole approach to information security and establish security practices needed to protect critical IT infrastructure. They also need to train and grow security experts needed to secure this infrastructure. Most organisations now recognize that it is imperative that local organizations take action before the situation worsens and the cost of inaction becomes even greater (World Economic Forum, 2012).

Lamorde (2015) maintained that just as it is with the European Union, North America and several countries in Asia have come up with National Strategy on Cyber security. The Nigerian National Cyber security framework should consider internet security as vital to a vibrant digital society. It should set out action plans to improve cyber security readiness and provide response and management of breaches for all internet users.

Lamorde (2015) suggested that the strategy should include the establishment of a well-functioning network of Computer Emergency Response Team at the national level. The organisation of cyber incidents simulations, putting in places a well-defined policy on Critical Information Infrastructure Protection (CIIP) with the aim of strengthening the security and resilience of ICT Infrastructure. He advised that in order to ensure a safer internet for our kids and young persons, the framework should create a strategy that will provide a safer and more secured cyber space for our young ones.

Juwah (2015) assert that countries need to step up; work together to build and provide information security services that enables Nigeria to address these challenges. Nigerians need to leverage their local presence and understanding of the environment to provide a clear indication of the security problems on the ground. This local presence combined with partnerships with regional and global players will provide globally tested solutions and approaches to address identified security problems.

METHODS

The researcher adopted a descriptive survey design. This type of design creates a platform for the researcher to make full description of the causes, effect and extent of the effect caused by the variables. The study area for this study was Nigeria. The population of this study consisted of all professionals in computer science, computer engineering and security agents who have been exposed to computer science. The researcher adopted a stratified random sampling technique. This method was used in selecting the 200 respondents for the study.

The main instrument used in this study was questionnaire titled "Cyber Security and Resilience Questionnaire" (CSRQ). The questionnaire comprised sections A and B. Section A contained information on personal data of the respondents while section B of the questionnaire

contained three variables such as strengthening Cyber Security and Resilience against Cyber. The instrument used for the research was made to pass through face and content validation using experts in computer science. The researcher used Cronbach Alpha reliability technique to measure level of reliability of the instrument, using 40 respondents who were not used for the main study. The test produced reliability coefficient of (0.92) and this proved that the instrument remarkable reliability for the study. With the help of the letter of introduction the respondents gave the researcher audience. The collected data were subjected to percentage analysis and chi-square analysis. For the hypothesis, the test for significance was done at 0.05 alpha levels.

RESULTS AND DISCUSSIONS

Research Question One

The research question sought to find out the strategies used in strengthening Cyber Security and Resilience against Cyber Risk in Nigeria. In order to answer the question, percentage analysis was used. (See table 1)

Table 1

Percentage analysis of the strategies used in strengthening Cyber Security and Resilience against Cyber Risk in Nigeria.

PERCENTAGE ANALYSIS	FREQ	%	Remark
Public and private organisations rethinking and building their whole approach to information security and establishing security practices needed to protect critical IT infrastructure.	18	9*	5th
Training and growing security experts needed to secure this infrastructure	38	19	4th
Taking action before the situation worsens and the cost of inaction becomes even greater	45	22.5	2nd
The establishment of a well-functioning network of Computer Emergency Response Team at the national level with strong internet security meant for vibrant digital society	42	21	3rd
The organisation of cyber incidents simulations, putting in places a well-defined policy on Critical Information Infrastructure Protection (CIIP)	57	28.5**	1st
Total	**200**	**100%**	

**** The highest percentage frequency**

*** The least percentage frequency**

SOURCE: Field survey

From the result of the above table 1, it was observed that the mostly used strategies in strengthening Cyber Security and Resilience against Cyber Risk in Nigeria was " The organisation of cyber incidents simulations, putting in places a well-defined policy on Critical Information Infrastructure Protection (CIIP)" (28.5%), while the least used strategy was "Public

and private organisations rethinking and building their whole approach to information security and establishing security practices needed to protect critical IT infrastructure".

Research Question 2

The research question sought to find out extent to which Cyber Security and Cyber Resilience helped in reducing cyber risk in Nigeria. To answer the research question, see table 2.

Table 2

Percentage analysis of the extent of help rendered by Cyber Security and Cyber Resilience in reducing cyber risk in Nigeria.

Cyber Security and and Cyber Resilience	FREQ	PERCENTAGE
VERY HIGH EXTENT	119	59.5**
HIGH EXTENT	65	32.5
LOW EXTENT	11	5.5
VERY LOW EXTENT	5	2.5*
TOTAL	**200**	**200**

**** The highest percentage frequency**

***** The least percentage frequency**

SOURCE: Field survey

From the result of the above table 2, it was observed that 59.5% of the respondents stated that Cyber Security and Cyber Resilience have helped in reducing cyber risk in Nigeria to a very high extent. 32.5% stated it to be of high extent. The third category of people affirmed it to be 5.5% while the least percentage of the respondents (2.5%) stated that Cyber Security and Cyber Resilience have helped in reducing cyber risk in Nigeria to a very low extent.

Hypothesis 1

1. The null hypothesis states that there is no significant difference in the perception of people as regards the effect of cyber security and cyber resilience in reducing cyber risk in Nigeria. (see table 3)

Table 3

Chi-square analysis of extent of the help of Cyber Security and Cyber Resilience on cyber risk in Nigeria.

Effect	Observed Freq	Expected Freq	X^2
VERY HIGH EXTENT	119	50	
HIGH EXTENT	65	50	
LOW EXTENT	11	50	170.64*
VERY LOW EXTENT	5	50	
TOTAL	**200**	**200**	

***Significant at 0.05 level; df = 3; Critical = 7.82**

Table 3 shows the calculated X^2-value as (170.64). This value was tested for significance by comparing it with the critical X^2-value (7.82) at 0.05 levels with 3 degree of freedom. The calculated X^2-value (170.64) was greater than the critical X^2-value (7.83). Hence, the result was significant. The result therefore means there is significant difference in the perception of people as regards the effect of cyber security and cyber resilience in reducing cyber risk in Nigeria. The result therefore was in agreement with the research findings of Howell and Lind, (2009), who opined that the cyber resilience is an entity's ability to continuously deliver the intended outcome despite adverse cyber events and that with it risk is certainly reduced. The significance of the result caused the null hypothesis to be rejected while the alternative one was accepted.

Conclusions

Based on the findings of the research work, it was concluded that Nigeria and other parts of the world, has suffered greatly from Cyber attack. Cyber Security Center has striven hard to ensure a secure and resilient cyber and communications infrastructure that supports national/ regional security, a vibrant economy, and the health and safety of all citizens. This is done by a Cyber Security Center serves stakeholders as a national center of excellence and expertise for cyber and telecommunications security issues, focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the Nation, etc. finally, cyber security and resilience have become a useful tool in checking and stopping cyber risks, and with Cyber security and resilience our society is protected against cyber risk.

Recommendations

1. Countries should build upon the work of the Global Community Engagement and Resilience Fund (GCERF) which supports local, community-level initiatives aimed at strengthening resilience against cyber attacks.
2. Organizations should build awareness of security issues across the internet community and promote cyber security awareness.
3. To improve cyber security posture over the years, companies should invest in enabling technologies and staffing.

REFERENCES

Access, A. (2014). "African Union Adopts Framework on Cyber Security and Data Protection." www.accessnow.org/blog/2014/08/22/African-union-adopts-framework on- cyber-security-and-data-protection.

Cassim, F. (2011) "Addressing the growing specter of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players" *CILSA* XLIV 123-138

Deloitte Advisory Cyber Risk Services (2013) Information Security: A Strategic Approach. IEEE Computer Society, Hoboken, NJ.

Governance (2015) Cybersecurity Strategy. Ministry of Information Communications and Technology

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books/Henry Holt.

Howell, J. & Lind, J. (2009). *Counter-Terrorism, Aid and Civil Society: Before and After the War on Terror*. Basingstoke, UK: Palgrave Macmillan. ISACA, 2014).

Juwah, M. (2015) *Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability.* Information System Front 8 (5), 339–349.

Kaplan, B., James, D. and Tucker (2015) Theory of deterrence and individual behavior. Can lawsuits control file sharing on the Internet? *Review of Law and & Economics* 3 (3), 693–714.

Wiley, D. (2015) Towards cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security* 10 (1–2), 5–22.

Lamorde, F. (2015) Education, poverty, political violence, and terrorism: is there a connection? *Journal of Economic Perspectives* 17 (4), 119–144.

Macharia, D. (2014) Theory of deterrence and individual behavior. Can lawsuits control file sharing on the Internet? *Review of Law and & Economics* 3 (3), 693–714.

Perlroth, G. & Nicole, E. (2016) Perlroth, Nicole, "Hackers use new weapons to disrupt major websites across U.S.", The New York Times, 21 October *http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.*

Ploch, D. (2010) The Information System and the Global Terrorism. SSRN: <*http://www.ssrn.com/abstract=906289*> (retrieved 2008).

Ravi, V. (2003) Toward an integration of criminological theories. *Journal of Criminal Law and Criminology* 76 (1), 116–150.

Ravi, D. (2012) How optimal penalties change with the amount of harm. *International Review of Law and Economics* 15 (1), 101–108.

Schneier, D. & Bruce, C. (2016). Schneier, Bruce, "Lessons from the Dyn DDoS Attack", Schneier on Security Blog, 8 November 2016, *https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html*

Steffani, H. (2006). Do ''bad boys'' really get the girls? Delinquency as a cause and consequence of dating behavior among adolescents. *Justice Quarterly* 21 (2), 355–389.

Stremlau, D. & Osman, E. (2015) A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: *An Exploratory Study*. University of Manitoba, Winnipeg, Manitoba.

Thilla, D. (2012) The economics of crime and punishment: an analysis of optimal penalty. *Economics Letters* 68 (2), 191–196.

Thomas, T., Karas, D., Lori, P. & Parrott, D. (2008) A framework for predicting security and dependability measures in real-time. *International Journal of Computer Science and Network Security* 7 (3), 169–183.

Vanson, H. & Bourne, M. (2012) A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency* 34, 495–518.

World Economic Forum (2012) "Convergence on the outcome economy", http://reports.weforum.org/industrial-internet-of-things/3-convergence-on-the-outcome-economy/3-2-the-emergence-of-the-outcome economy/? doing_wp_cron=1463567483.8225409984588623046875