Exploring the New Era of Cybersecurity Governance

Petac Eugen
"Ovidius" University of Constanța, Faculty of Mathematics and Computer Science
epetac@univ-ovidius.ro
Duma Petruţ
Technical University "Gh. Asachi" of Iaşi
Faculty of Electronics, Telecommunications and Information Technology
pduma@etti.tuiasi.ro

Abstract

In a digital world, cybersecurity has become very important for companies, government agencies or organizations, as well as for end-users. With its components, Data Governance (DG) and Information Technology Governance (ITG), Information Governance (IG) is a key element of Corporate Governance (GC). The characteristics and the relationships between them are analysed in the second part of the paper. The subject of cybersecurity as part of Information Governance is addressed in the third part of the paper, discussing issues such as attack types, the relationship attack sophistication versus intruder technical knowledge and a security framework for identification and prevention of cyber-attacks. In the fourth part, the best practices for Cybersecurity Governance are synthesized. As cyber threats are scarcely diversifying and becoming more and more sophisticated, affecting an increasingly number of users and organizations, the solution is a unified and coordinated approach at the organizational, regional and global level.

Key words: Cybersecurity, Information Governance, CIA triad, CSIRT.
J.E.L. classification: L8, M1, M3

1. Introduction

We will refer to cyber environment and cybersecurity from the perspective provided by the International Telecommunication Union in the document ITU-T X.1205: "Cyber environment includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks (ITU, 2008)."; "Cybersecurity is 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. Cybersecurity 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 general security objectives comprise the following: Availability, Integrity (which may include authenticity and non-repudiation) and, Confidentiality (ITU, 2008)."

ISO/IEC 17799 (ISO, 2005) treats information security through the prism of three important attributes, known as the CIA triad: Confidentiality – the information is only accessible to authorized persons; Integrity – ensuring the accuracy and completeness of the methods by which information is processed; and Availability – authorized users have access to information and associated assets at opportune times.

This paper has two main objectives. The first objective is to contribute to an important and current discussion about the meaning and importance of cybersecurity for the Corporate

Governance. The relationships between Data Governance, Information Technology Governance, Information Governance and Corporate Governance, and the role of cybersecurity are analyzed in the second part of our paper. The second main objective of the paper is to analyze and to propose best practices for Cybersecurity Governance. The structure of cyber-attacks is analyzed in the current work through the intrusion framework Cyber Kill Chain (Lockheed Martin, 2018), presented in the third part. The framework provides an insight into the attack and allows a very good understanding of the attacker's strategy, mechanisms, methods and procedures to reduce the attacker's chances. Proper prevention and security against cyber-attacks is no longer an option but a necessity. The consequences of computer security incidents can be disastrous, but they can be avoided. In the fourth part of our paper we mention best practices that provide protection against most of all security threats.

2. Theoretical background. What is Cybersecurity Governance?

The Federal Information Security Management Act (FISMA) defines CIA triad objectives for information and information systems (Taylor, 2013): CONFIDENTIALITY "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information. INTEGRITY "Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information. AVAILABILITY "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to or use of information or an information system.

Confidentiality, integrity, availability, possession or control, authenticity and utility, also known as the Parkerian hexad (Parker, 1998), is another model designed to guide policies for information security within an organization.

As an in-depth analysis, developed by European Union Agency For Network And Information Security (ENISA), the study "Definition of Cybersecurity Gaps and overlaps in standardization" (ENISA, 2015) provides an essential context needed to understanding the cybersecurity term and to use these in a variety of fields. According to this study the different domains of Cybersecurity are: communications security, operations security, information security, physical security, public/national security. The CSG takes these domains into account. Organizing the activity of IG bodies only from the perspective of information security is not enough. International Organization for Standardization (ISO), International Telecommunication Union (ITU), National Institute of Standards and Technology (NIST), Committee on National Security Systems (CNSS), National Cybersecurity and Communications Integration Center's (NCCIC), NATO and ENISA are some of the organizations that have adopted the term cybersecurity.

Corporate Governance (CG) represents the area for achieving a company's goals and in this sense it encompasses any management domain that can sustain the company's long-term success. "Corporate governance can be accepted as an art of management, which provides a well organized top-down communication between all abovementioned participants in a company (Sonmez and Yildırım, 2015)." Including the global policies and processes for optimizing and using the data, Information Governance (IG) is a core element of the CG.

IG is defined by Gartner as "the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals (Proença, Vieira and Borbinha, 2016)." Data Governance (DG) and Information Technology Governance (ITG) constitute a global IG program. Establishing the frameworks and the best practices for achieving the desired business objectives based on information technology investments is the main focus of ITG. The DG approach to governance focuses on processes, methods, tools, and techniques to ensure that data is of high quality, reliable and unique. DG is the lower level at which to implement IG. However, DG including elements of data quality, data management, IG policy development, business process improvement, and compliance and risk

management, DG will be the core of Data Stewardship considering topics such as metadata management, data security and authentication, setting of Data Quality rules and policies and data integration. In an analysis regarding the Effective Data Governance, Infosys shows the following statistics regarding the data: "the size of global data will reach 40 zettabytes by 2020; structured data grows at a rate of 40% each year; the volume of structured and unstructured data grows at a constant rate of about 80% per year; machine-generated data will increase 15 times by 2020 (Infosys, 2018)." These statistics are meant to provide a new dimension for DG, as well as for Data Management (DM), as processes of creating, obtaining, transforming, sharing, protecting, documenting and preserving data.

The Information Management (IM) at an organization is completed by the IG with the integration of ITG and DG, creating a balance between the usage and the security of information. The data management is a subset of IM. The processes that enable organizations to systematise, manage and understand all types of data, including integration of IP device discovery, data sharing, infrastructure databases, events and alarms, third-party integration, automated patching, and applications are attributes of Intelligent Information Management (IIM). The main objective of CG is an effective and secure business performance.

By incorporating it into IG, information security is an integral part of CG. But is not IS a relative term? Because IG includes "information security and protection, compliance, data governance, electronic discovery, risk management, privacy, data storage and archiving, knowledge management, business operations and management, audit, analytics, IT management, master data management, enterprise architecture, business intelligence, big data, data science, and finance (IGI, 2014)", we consider the term cybersecurity to be more appropriate.

Defining risk posture , balancing global and local requirements, managing data , responding to change and applying relevant metrics are some reasons for which cybersecurity becomes an integral part of CG and we can discuss about a new era for CyberSecurity Governance (CSG).

3. Cybersecurity: challenges and opportunities

In addition to technology, cybersecurity also refers to the fact that people have access to data and processes involved. The access may be authorized or unauthorized. Cyber-attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain by performing malicious activities. Grouped in amateurs, hackers (white, gray, or black hats) and organized hackers (cyber criminals, hacktivists, terrorists, and state sponsored hackers), depending on their intentions of destruction, cyber-attackers target is both large and small businesses and organizations. The threats can also come from within organizations, from privileged users or end-users. The main objectives of cyber-attackers are manipulated, destroy, disrupt and steal. The estimated Cyberattack fallout cost to Global Economy by 2020 is $3 Trillion (Chinn, Kaplan and Weinberg, 2014).

Among the factors that contributed to this we can mention: corporate and social media security breaches, explosive growth of computer, mobile systems and Internet availability, increase in broadband availability, low priority of security for software developers, difficulty patching vulnerabilities on all systems, graphical user interface based tools that exploit known software vulnerabilities, tools that try to exploit multiple vulnerabilities, availability of malicious software authoring and editing tools, spear phishing (hackers target employees through emails that appear to be from colleagues within their own organizations, allowing cyber criminals to steal personal information), advanced employee training (can form insider cyber-attackers), hacktivism, botnets (as a number of computers set up to forward malicious information to other computers).

Developed by Lockheed Martin as a security framework for identification and prevention of cyber-attacks, Cyber Kill Chain (Lockheed Martin, 2018) is an ordered list of seven stages of a cybernetic APT (Advanced Persistent Threat) attack that allows cybersecurity experts to understand the type of cyber-attack. The Cyber Kill Chain stages are:

- Reconnaissance - The attacker gathers information about the target;
- Weaponization - The attacker creates an exploit and malicious payload to send to the target;

- Delivery - The attacker sends the exploit and malicious payload to the target by email or other method;
- Exploitation - The exploit is executed; Installation - Malware and backdoors are installed on the target;
- Command and Control - Remote control of the target is gained through a command and control channel or server;
- Action - The attacker performs malicious actions like information theft or executes additional attacks on other devices from within the network by working through the Cyber Kill Chain stages again.

This framework is purpose to provide insight into an attack and great understanding the attacker's strategy, mechanisms, methods and procedures to decrease chances said adversary accomplish their desired outcome. But Cyber Kill Chain is not infallible. Manny attack strategies are changing and follow their own rules. This is the case with web application attacks: a good approach consists to take advantage of a vulnerability in the application itself. The solution is the new security technology named Runtime application self-protection (RASP) (Gartner, 2018).

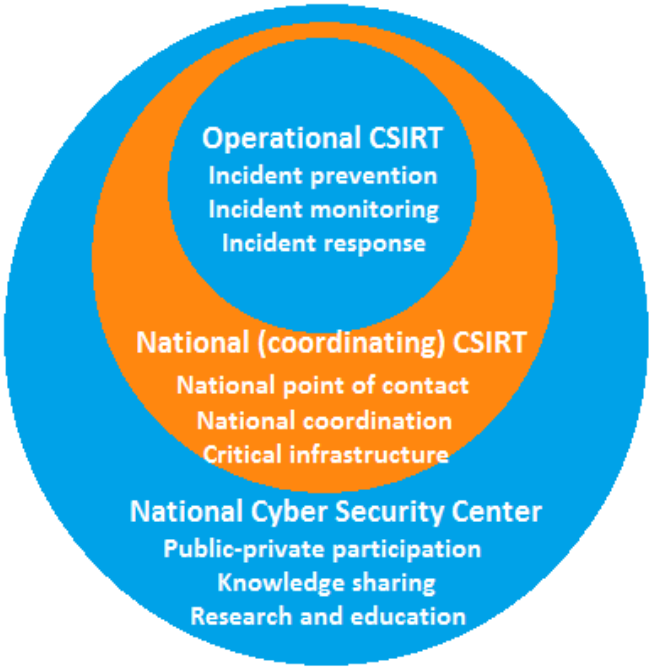
4. Best practices for Cybersecurity Governance

Cybersecurity best practices and ways to protect data are found in lists of professional organizations. Some of the best practices are: employ a risk-based approach to security; create a hierarchical cybersecurity policy; maintain security patches and updates; accomplish and test backups; use the principle of least privilege; use two-factor authentication; handle passwords securely; change default passwords for the IoT (Internet of Things) devices; physical security measures; human resource security measures; educate users; encrypt data; employ access controls regularly test incident response; implement a network monitoring, analytics and management tool; implement network security devices; implement a comprehensive endpoint security solution.

In the CSG, cybersecurity best practices list setting is one of the objectives of a Computer Security Incident Response Team (CSIRT), especially established at an organization level, such as a corporation, institution, educational or government network, region or country. The main objectives of a CSIRT are: define the incident response policies, procedures and services provided by identifying the risks; create an incident reporting capability; identify, contain and eradicate the incident; recover from the incident; investigate the incident; assist in the prevention of a reoccurrence of the incident; integrating lessons learned. CSIRT services generally grouped into three categories: reactive (e.g. vulnerability alerts, incident handling); proactive (e.g. intrusion detection, auditing and information dissemination) and security quality management (e.g. risk analysis, disaster recovery planning, and education and training). Mitigation planning, incident trend analysis, and security architecture review are the mains proactive threat assessments for prevent cybersecurity incidents. Mostly embedded within a government authority or ministry, such as the telecommunications or network information security authority, though some reside in an interior or defense ministry, the national CSIRTs provides a reliable and trusted single point of contact for reporting computer security incidents worldwide by any user, company, government agency or organization. The relationships between Operational CSIRT, National (coordinating) CSIRT and National Cyber Security Center are shown in figure 1.

Forum of Incident Response and Security Teams (FIRST- www.first.org) as a global association of CSIRTs (421 Teams in 86 different countries) enables incident response teams to more effectively respond to security incidents reactive as well as proactive and brings together a variety of computer security incident response teams from government. With similar activities, there are the following organizations as a regional association of CSIRTs: ENISA-European Network and Information Security Agency (Regional Europe Union), TF-CSIRT – Task Force Collaboration of Computer Security – Incident Response Team in Europe, APCERT–Asia Pacific Computer Emergency Response Team (Regional Asia Pacific), OIC-CERT– Organization of Islamic Conference – Computer Emergency Response Team, ANSAC-ASEAN Network Security Action Council.

Figure no. 1. CSIRTs relationships



Source: Clark et al., (2014)

Originally used by the Carnegie Mellon University (CMU), the term Computer Emergency Response Team (CERT) is used by some large organizations as well to CSIRT, as it is about the same objectives and functions (CMU, 2018). The National Cybersecurity and Communications Integration Center (NCCIC - https://www.us-cert.gov) is the USA's flagship cyber defense, incident response, and operational integration center, with the mission to reduce the USA's risk of systemic cybersecurity and communications challenges. NCCIC share information for industrial control systems owners, operators, and vendors (control system users), resources for information sharing and collaboration among government agencies (government users) and information for system administrators and technical users about latest threats (home and business). The EU Institutions have decided to set up a permanent Computer Emergency Response Team (CERT-EU - https://cert.europa.eu) for the EU institutions, agencies and bodies and has good cooperation with other CERTs in the Member States and beyond as well as with IT security companies and professionals.

5. Conclusions

The compromise of information security may affect the ability of an organization to provide services, and may lead to fraud or destruction of data, non-contractual clauses, disclosure of confidential information, impairment of credibility, etc. The cyber threats are scarcely diversifying and becoming more and more sophisticated, affecting an increasingly number of users and organizations. A coordinated approach at the organizational, regional and global level allows the prevention of cyber risks and threats. Our work provides a comprehensive overview of existing discussion about the meaning and importance of cybersecurity. Communication security, operation security, information security, physical security, and public/national security are identified areas by ENISA (ENISA, 2015) for cybersecurity. Any security system must ensure confidentiality, integrity and availability of information. Changes in paradigm and technology evolution have brought new concepts such as: security without frontiers, cloud computing, fog computing, big data, mobile computing, etc. The information is perishable, volatile and often uncertified by multiple sources, which is why the processing power for filtering and analyzing large volumes of data is steadily increasing. Cybersecurity becomes an integral part of the corporate governance and we are discussing a new era for cybersecurity governance.

National authorities established at an organization level, such as a corporation, institution, educational or government network, region or country, CSIRTs provides consistent support to the end users, companies, government agencies or organizations in the fight with cyber-enemies. CSIRTs stand out through efficiency, competence and efficiency. The weaknesses of not having a CSIRT structure within an organization are obvious. The incapacity to contain an incident can lead to repeated incidents, in a continuous cycle that can only lead to disaster. The protection of critical national infrastructures in financial, banking, transport, medical, education, energy, eGovernment and intelligent public administration, education and cyber security culture are some of the cybersecurity governance challenges.

6. References

- Chinn, D., Kaplan, J. and Weinberg, A., 2014. *Risk and responsibility in a hyperconnected world: Implications for enterprises, Report - January 2014*. [online] Geneva: Word Economic Forum. Available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/risk-and-responsibility-in-a-hyperconnected-world-implications-for-enterprises, [Accessed 28 Apr. 2018].
- Clark, K., Stikvoort, D., Stofbergen, E. and Heuvel, E., 2014. "A Dutch Approach to Cybersecurity through Participation". *IEEE Security & Privacy*, 12(5), pp. 27-34.
- CMU.edu, 2018. *Carnegie Mellon University, The CERT Division*, [online] Available at: https://www.sei.cmu.edu/about/divisions/cert/index. cfm. [Accessed 28 Apr. 2018].
- Dragomir, C., Utureanu, S. and Manole, I. C., 2017. *Computer Science within the Academic Curriculum Used in Maritime Training*. "Ovidius" University Annals, Economic Sciences Series 17.2, pp. 402-406.
- ENISA, 2015. *Definition of Cybersecurity Gaps and overlaps in standardization V1.0 December 2015*. [online] Attiki: ENISA. Available at: https://www.enisa.europa.eu/publications/definition-of-cybersecurity, [Accessed 28 Apr. 2018].
- Gartner.com, 2018. *Gartner IT Glossary, Runtime Application Self-Protection (RASP)*, [online] Available at: https://www.gartner.com/it-glossary/runtime-application-self-protection-rasp. [Accessed 20 Apr. 2018].
- IGI, 2014. *IGI Publishes 2014 Annual Report*. [online] Available at: http://iginitiative.com/igi-publishes-2014-annual-report/ [Accessed 28 Apr. 2018].
- Infosys.com, 2018. *Effective Data Governance*. [online] Available at: https://www.infosys.com/data-analytics/ insights/Documents/effective-data-governance.pdf, [Accessed 28 Apr. 2018].
- ISO, 2005. *Information technology --Security techniques -- Code of practice for information security management, ISO/IEC 17799:2005*, [online] Available at: https://www.iso.org/standard/39612.html, [Accessed 28 Apr. 2018].
- ITU, 2008. *Overview of cybersecurity, ITU-T X.1205*. [online] Available at: https://www.itu.int/rec/T-REC-X. 1205-200804-I/en [Accessed 28 Apr. 2018].
- Lockheedmartin.com, (2018). *The Cyber Kill Chain® framework*. [online] Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, [Accessed 28 Apr. 2018].
- Parker, D., 1998. *Fighting Computer Crime.* New York: John Wiley & Sons.
- Proença, D., Vieira, R. and Borbinha, J., 2016. "A maturity model for information governance". In: *International Conference on Theory and Practice of Digital Libraries*. Cham: Springer, pp. 15-26.
- Sonmez, M. and Yildırım, S., 2015. "A Theoretical Aspect on Corporate Governance and Its Fundamental Problems: Is It a Cure or Another Problem in the Financial Markets?". *Journal of Business Law and Ethics*, [online] Volume 3 (No. 1 & 2), pp. 20-35. Available at: http://jblenet.com/journals/jble/Vol_3_No_1_June_ 2015/2.pdf [Accessed 28 Apr. 2018].
- Taylor, L., 2013. *FISMA Compliance Handbook.* 2nd ed. New York: Elsevier.