Enfoque UTE, V.9-N.1, Mar.2018, pp. 127 - 137
http://ingenieria.ute.edu.ec/enfoqueute/
e-ISSN: 1390-6542 / p-ISSN: 1390-9363

Recibido (Received): 2017/11/23
Aceptado (Accepted): 2018/03/30

Un modelo práctico para realizar auditorías exhaustivas de Ciberseguridad

(A Practical Model to Perform Comprehensive Cybersecurity Audits)

Regner Sabillon[1]

Resumen:
En la actualidad, las organizaciones se enfrentan continuamente a ser blanco de ciberataques y amenazas cibernéticas; la sofisticación y complejidad de los ciberataques modernos y el modus operandi de los ciberdelincuentes, incluidas las Técnicas, Tácticas y Procedimientos (TTP), continúan creciendo a un ritmo sin precedentes. Los ciberdelincuentes siempre están adoptando nuevas estrategias para planificar y lanzar ataques cibernéticos basados en las vulnerabilidades de ciberseguridad existentes y explotar a los usuarios finales mediante el uso de técnicas de ingeniería social. Este artículo presenta un modelo de auditoría de ciberseguridad innovador e integral. El Modelo de Auditoría de Ciberseguridad (CSAM) se puede implementar para realizar auditorías de ciberseguridad internas o externas. Este modelo se puede usar para efectuar auditorías únicas de ciberseguridad o puede ser parte de cualquier programa de auditoría corporativa para mejorar los controles de ciberseguridad. Cualquier equipo de auditoría de seguridad de la información o ciberseguridad tiene la opción de aplicar una auditoría completa para todos los dominios de ciberseguridad o seleccionando dominios específicos para auditar ciertas áreas que necesitan verificación y fortalecimiento del control. El CSAM tiene 18 dominios; el Dominio 1 es específico para Estados y los dominios 2-18 se pueden implementar en cualquier organización. La organización puede ser cualquier empresa pequeña, mediana o grande, el modelo también es aplicable a cualquier organización sin fines de lucro (OSFL).

Palabras clave: ciberseguridad; auditoría de ciberseguridad; modelo de auditoría de ciberseguridad; aseguramiento de ciberseguridad; controles de ciberseguridad.

Abstract:
These days organizations are continually facing being targets of cyberattacks and cyberthreats; the sophistication and complexity of modern cyberattacks and the modus operandi of cybercriminals including Techniques, Tactics and Procedures (TTP) keep growing at unprecedented rates. Cybercriminals are always adopting new strategies to plan and launch cyberattacks based on existing cybersecurity vulnerabilities and exploiting end users by using social engineering techniques. Cybersecurity audits are extremely important to verify that information security controls are in place and to detect weaknesses of inexistent cybersecurity or obsolete controls. This article presents an innovative and comprehensive cybersecurity audit model. The CyberSecurity Audit Model (CSAM) can be implemented to perform internal or external cybersecurity audits. This model can be used to perform single cybersecurity audits or can be part of any corporate audit program to improve cybersecurity controls. Any information security or cybersecurity audit team has either the options to perform a full audit for all cybersecurity domains or by selecting specific domains to audit certain areas that need control verification and hardening. The CSAM has 18 domains; Domain 1 is specific for Nation States and Domains 2-18 can be implemented at any organization. The organization can be any small, medium or large enterprise, the model is also applicable to any Non-Profit Organization (NPO).

Keywords: cybersecurity; cybersecurity audit; cybersecurity audit model; cybersecurity assurance; cybersecurity controls.

[1] Internet Interdisciplinary Institute, Universitat Oberta de Catalunya, Calgary – Canada (regners@athabascau.ca).

1. Introduction

This article is an extended version of the paper entitled “A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)”, that was presented at the “2nd. International Conference on Information Systems and Computer Science - INCISCOS 2017” on November 24, 2017.

The initial paper introduced the CyberSecurity Audit Model (CSAM) and its design to the global scientific community. Furthermore, we now present the methodology of our case study research and the results from our Canadian post-secondary institution case study research.

Organizations are trying to protect cyber assets and implement cybersecurity measures and programs, but despite this continuing effort it is unavoidable to evade cybersecurity breaches and cyberattacks.

According to the Information Systems Audit and Control Association (ISACA), the origin of cybersecurity was published in a journal article in the early eighties, presenting the first proof of the concepts of self-replicating/self-propagating code linked to a computer worm. Pursuant to the fundamentals of the discipline defined by ISACA, cybersecurity is *“The protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems”* – cybersecurity and information security are often mentioned interchangeably but cybersecurity is a component of information security. Proaño et al. (2017) highlight that IT auditors deal with subjectivity issues involved with emotions, technical skills or abilities in order to report audit findings and recommend the future implementation of knowledge-based systems for computer audits.

Our proposed CyberSecurity Audit Model (CSAM) has been designed to address the limitations and inexistence of cybersecurity controls to conduct comprehensive cybersecurity or domain-specific cybersecurity audits.

2. Methodology

In our previous paper, we reviewed relevant literature related to general cybersecurity, cybersecurity best practices, cybersecurity audits and cybersecurity frameworks from Protiviti, Deloitte, ISACA, ISO 27001, ISO 27001, NIST Cybersecurity Framework, Donaldson et al., Hollingsworth, Ross and Khan.

The CyberSecurity Audit Model (CSAM) has been tested, implemented and validated along with the Cybersecurity Awareness TRAining Model (CATRAM) in a Canadian higher education institution. The research project assessed the cybersecurity organizational strategy, implemented the CyberSecurity Audit Model (CSAM) and delivered cybersecurity awareness training to more than one hundred participants based on the Cybersecurity Awareness TRAining Model (CATRAM).

The case study research included several phases like plan, design, preparation, collection, analysis, sharing and dissemination. We intended to perform qualitative research by utilizing interpretive material practices such as online and paper surveys, interviews, classroom and online training and analysis of documentation, processes and procedures of the target institution. The organization provided their staff time to support the case study research, resources to conduct the cybersecurity audit, the provision of classroom space and time, computer use, Internet access for the delivery of the cybersecurity awareness training courses, the access to their computer systems to conduct the research and to design the online courses in their Learning Management System (Moodle).

3. The Cybersecurity Audit Model (CSAM)

The CyberSecurity Audit Model (CSAM) proposed in this article, is a new exhaustive model that encloses the optimal assurance assessment of cybersecurity in any organization and it can verify specific guidelines for Nation States that are planning to implement a

National Cybersecurity Strategy (NCS) or want to evaluate the effectiveness of its National Cybersecurity Strategy or Policy already in place. The CSAM can be implemented to conduct internal or external cybersecurity audits, this model can be used to perform single cybersecurity audits or can be part of any corporate audit program to improve cybersecurity controls. Any audit team has either the options to perform a full audit for all cybersecurity domains or by selecting specific domains to audit certain areas that need control verification and hardening. The CSAM has 18 domains; domain 1 is specific for Nation States and domains 2-18 can be implemented at any organization. The organization can be any small, medium or large enterprise, the model is also applicable to any Non-Profit Organization (NPO).

The CyberSecurity Audit Model (CSAM) contains overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessments and an evaluation scorecard.

Overview

This section introduces the model organization, the working methodology and the possible options for implementation.

Resources

This component provides links to additional resources to help understanding some of the cybersecurity topics:

- Cybersecurity: NIST Computer Security Resource Center, Financial Industry Regulatory Authority (FINRA) cybersecurity practices and Homeland Security cybersecurity.
- National Cybersecurity Strategy (NCS): North Atlantic Treaty Organization (NATO) cybersecurity strategy, European Union Agency for Network and Information Security (ENISA) cybersecurity strategy and Organisation for Economic Co-operation and Development (OECD) comparative analysis of national cybersecurity strategies.
- Governance: PricewaterhouseCoopers Board cybersecurity governance and MITRE cybersecurity governance.
- Cyber Assets: NERC critical cyber assets.
- Frameworks: Foresite common cybersecurity frameworks, United States Computer Emergency Readiness Team (US-CERT) framework and ISACA's implementing the NIST cybersecurity framework.
- Architecture: Trusted Computer Group (TCG) architect's guide and US Department of Energy's IT security architecture.
- Vulnerability Management: SANS vulnerability assessment and Homeland Security vulnerability assessment and management.
- Cyber Threat Intelligence: SANS – Who's using cyberthreat intelligence and how?
- Incident Response: Computer Security Incident Response Team (CSIRT) frequent asked questions.
- Digital Forensics: SANS forensics whitepapers.
- Awareness: National Cyber Security Alliance – Stay safe online and PCI DSS -Best practices for implementing security awareness program.
- Cyber Defense: SANS- The sliding scale of cybersecurity.
- Disaster Recovery: Financial Executives International (FEI) Canada – Cybersecurity and business continuity.
- Personnel: Kaspersky – Top 10 tips for educating employees about cybersecurity.

Domains

The CSAM contains 18 domains. Domain 1 has been designed specifically for Nations States and domains 2-18 are applicable to any organization.

Sub-domains

All domains have at least one sub-domain but in certain cases there might be several sub-domains per domain.

The sub-domains are:

- Cyberspace
- Governance
- Strategy
- Legal and Compliance
- Cyber Asset Management
- Cyber Risks
- Frameworks and Regulations
- Architecture
- Networks
- Information
- Systems
- Applications
- Vulnerability Management
- Threat Intelligence
- Incident Management
- Digital Forensics
- Awareness Education
- Cyber Insurance
- Active Cyber Defense
- Evolving Technologies
- Disaster Recovery
- Onboarding
- Hiring
- Skills
- Training
- Offboarding

Controls

Each domain has sub-domains that are assigned a reference number. Controls are identified by clause numbers and an assigned checklist. In order to verify the control evaluation, the cybersecurity control is either in place or inexistent.

Checklists

Each checklist is linked to a specific domain and the subordinated sub-domain. The checklist verifies the validity of the cybersecurity sub-controls in alignment with a control clause. The cybersecurity auditors have the option to collect evidence to verify the sub-control compliance.

Sub-Controls

The Sub-Controls are evaluated using the checklists.

The assessment of each sub-control can be in compliance, with a minor nonconformity or with a major nonconformity:

-Compliant: The cybersecurity sub-control is active and aligned with the specific requirements.

-Minor Nonconformity: The cybersecurity sub-control has not been fulfilled and it represents a minor risk.

-Major Nonconformity: The cybersecurity sub-control does not exist or it is a complete failure and it represents an unacceptable risk.

Guideline Assessment

The guideline assessment only applies to the Nation States domain. The guidelines are evaluated for cybersecurity culture, National Cybersecurity Strategy (NCS), cyber operations, critical infrastructure, cyber intelligence, cyber warfare, cybercrime and cyber diplomacy.

Evaluation Scorecard

The control, guideline and sub-control evaluation is calculated after the audit has been completed. The evaluation consists in assigning scores and ratings for each control, guideline and sub-control.

We calculate the final cybersecurity maturity rating of the Nation States domain by using the following criteria. The score can be mapped to a specific maturity level:

Immature (I): 0-30

The Nation State does not have any plans to manage its cyberspace. A National Cybersecurity Strategy (NCS) or Policy is inexistent.

Developing (D): 31-70

The Nation State is starting to focus on national cybersecurity. If technologies are in place, the Nation State needs to focus on key areas to protect cyberspace.

Mature (M): 71-90

While the Nation State has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.

Advanced (A): 91-100

Nation State has excelled in national cybersecurity and cyberspace practices. There is always room for improvement. Nation State could become an international leader and help other Nation States with cybersecurity and cyberspace matters.

And for domains 2-18, we calculate the final cybersecurity maturity rating of any organization by using the following criteria. The score can be mapped to a specific maturity level:

Immature (I): 0-30

The organization does not have any plans to manage its cybersecurity. Controls for critical cybersecurity areas are inexistent or very weak. The organization has not implemented a comprehensive cybersecurity program.

Developing (D): 31-70

The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations.

Mature (M): 71-90

While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses.

Advanced (A): 91-100

The organization has excelled in implementing cybersecurity best practices. There is always room for improvement. Keep documentation up-to-date and continually review cybersecurity processes through audits.

Cybersecurity Readiness Evaluation

We calculate the overall organizational cybersecurity readiness by using the following criteria. The score can be mapped to a specific cybersecurity readiness level:

Immature (I): 0-30

The organization does not have any plans to manage its cybersecurity. Controls for critical cybersecurity areas are inexistent or very weak. The organization has not implemented a comprehensive cybersecurity program. The Cybersecurity readiness is inexistent at this level.

Developing (D): 31-70

The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations. The Cybersecurity readiness is developing at this stage.

Mature (M): 71-90

While the organization has a mature environment. Improvements are required to the key areas that have been identified with weaknesses. The Cybersecurity readiness is at a mature level.

Advanced (A): 91-100

The organization has excelled in implementing cybersecurity best practices. There is always room for improvement. Keep documentation up-to-date and continually review cybersecurity processes through audits. The Cybersecurity readiness is at an advanced level, but the organization must continually update its cybersecurity strategy at all times.

4. Results

The research results were measured based on the implementation outcome of the CSAM and CATRAM models in our target institution. The organizational cybersecurity audit results are presented as an overall cybersecurity rating classified by the model's domains.

The organization is starting to focus on cybersecurity matters. If technologies are in place, the organization needs to focus on key areas to protect cyber assets. Attention must be focused towards staff, processes, controls and regulations. The final cybersecurity maturity rating is positioned at the "Developing" level with a score of 51% (Table 1).

In addition, the radar chart (Figure 1) presents the domain evaluation results in order to provide the overall organizational cybersecurity readiness.

5. Discussion

This study presents the design of the CyberSecurity Audit Model (CSAM). The aim of this model is to introduce a cybersecurity audit model that includes all functional areas, in order to guarantee an effective cybersecurity assurance, maturity and cyber readiness in any organization or any Nation State that is auditing its National Cybersecurity Strategy (NCS). This model was envisioned as a seamless and integrated cybersecurity audit model to assess and measure the level of cybersecurity maturity and cyber readiness in any type of organization, no matter in what industry or sector the organization is positioned. Moreover, by adding guidelines assessment for the integration of a national cybersecurity policy, program or strategy at the country level.

Table 1. Final Cybersecurity maturity rating table

Cybersecurity Audit Model (CSAM)						
No.	**Domain**	**Ratings**				**Score**
		I	D	M	A	
2	Governance and Strategy	☐	☒	☐	☐	35%
3	Legal and Compliance	☐	☐	☒	☐	90%
4	Cyber Assets	☒	☐	☐	☐	30%
5	Cyber Risks	☐	☒	☐	☐	60%
6	Frameworks and Regulations	☒	☐	☐	☐	30%
7	Architecture and Networks	☐	☒	☐	☐	67%
8	Information, Systems and Apps.	☐	☒	☐	☐	55%
9	Vulnerability Identification	☒	☐	☐	☐	30%
10	Threat Intelligence	☐	☒	☐	☐	60%
11	Incident Management	☒	☐	☐	☐	10%
12	Digital Forensics	☒	☐	☐	☐	30%
13	Awareness Education	☐	☒	☐	☐	60%
14	Cyber Insurance	☐	☐	☒	☐	90%
15	Active Cyber Defense	☒	☐	☐	☐	5%
16	Evolving Technologies	☐	☐	☐	☒	100%
17	Disaster Recovery	☒	☐	☐	☐	30%
18	Personnel	☐	☐	☒	☐	77%
Final Cybersecurity Maturity Rating		☐	☒	☐	☐	**51%**

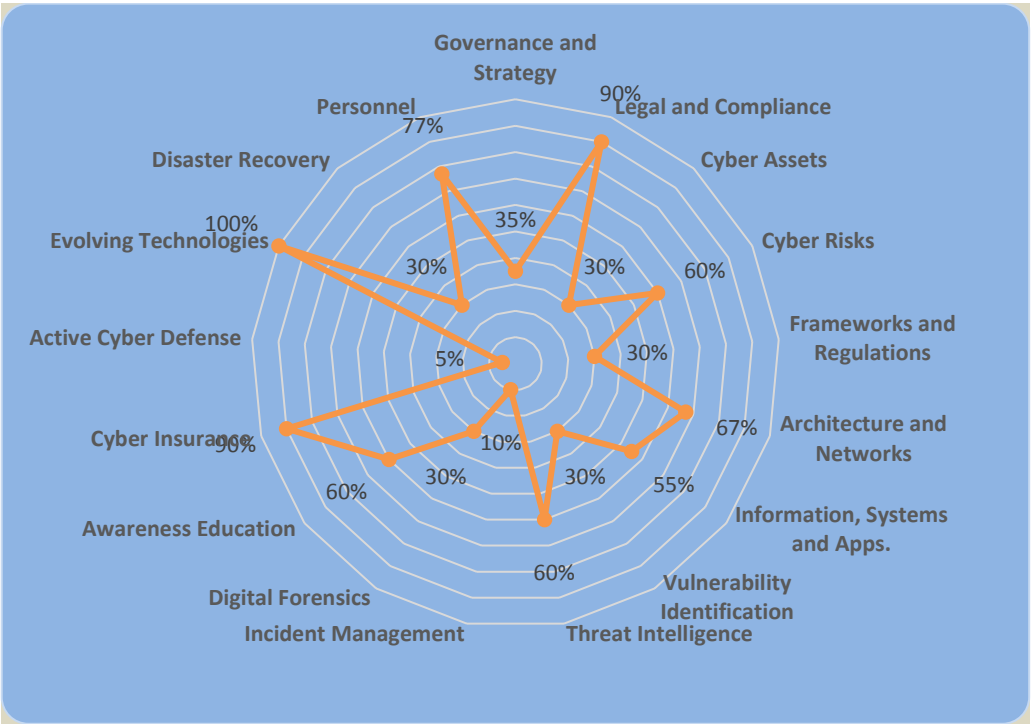

Figure 1. Final Cybersecurity Readiness Chart

Many cybersecurity frameworks are mostly oriented towards a specific industry like the *"PCI DSS"* for credit card security, the *"NERC CIP Cyber Security"* for the bulk power system or the *"NIST Cybersecurity Framework"* for protecting national critical infrastructure. But, all the existing frameworks do not provide a one-size fits all for planning and conducting cybersecurity audits. The necessity to mapping against specific cybersecurity frameworks is because of regulatory requirements, to satisfy the demands of industry regulators, to comply with internal or external audits, to satisfy business purposes and customer requirements or simply by improving the enterprise cybersecurity strategy.

Table 2. Comparison of some cybersecurity audit models

Audit Model or Framework	Description
The Cybersecurity Framework (CSF) Version 1.1: NIST (2017)	The initial version was conceived in 2014 to improve cybersecurity of critical infrastructure. The version 1.1 manages cybersecurity risks for critical infrastructure. It is composed of the Framework Core, the Framework Implementation Tiers and the Framework profiles. The Framework Core includes five functions – Identify, Protect, Detect, Respond and Recover; then each of these functions have categories and subcategories. In addition, the Core contains Informative resources like cybersecurity standards, guidelines and best practices. The Tiers define cybersecurity context organized from partial to adaptive tier. The Profile presents the outcomes based on organizational needs. The current profile can later be compared with a target profile.
The Audit First Methodology: Donaldson et al. (2015)	This methodology considers other cybersecurity controls and leaves preventive control execution until the end. This audit includes five different phases: 1. Threat analysis: This phase identifies Confidentiality, Integrity and Availability (CIA) threats that may impact IT and corporate data. Threat impact and indicators are defined. 2. Audit controls: It includes the design of threat audit controls. 3. Forensic controls: This phase helps to implement the required forensic controls for the enterprise cybersecurity functional areas: 1) Systems administration 2) Networks 3) Applications 4) Endpoints, servers and devices 5) Identity, authentication and access 6) Data protection and cryptography 7) Monitoring, vulnerabilities and patch management 8) Availability, disaster recovery and physical protection 9) Incident management 10) Supply chain and asset management 11) Policy, audit, e-Discovery and training 4. Detective controls: Detective controls are designed to alert, detect, stop and repel cyberattacks. 5. Preventive controls:These controls block undesired activities and stop them from ocurring.
The CyberSecurity Audit Model (CSAM): Sabillon et al. (2017)	The CSAM comprises overview, resources, 18 domains, 26 sub-domains, 87 checklists, 169 controls, 429 sub-controls, 80 guideline assessments and an evaluation scorecard. Domain 1-Guideline assessment are specific for Nation States and domains 2-18 are applicable to any type of organization. Certain domains have specific sub-domains where controls are evaluated. Then the checklists verify compliance about specific sub-controls based on domain/sub-domain. The scorecard results determine the domains rating and score that will produce the overall cybersecurity maturity rating.

We compared our model in *Table 2* to highlight the main features against *"The Cybersecurity Framework (CSF) Version 1.1: NIST (2017)"* and *"The Audit First Methodology: Donaldson et al. (2015)".* The CSAM is not for a specific industry, sector or organization – On the contrary, the model can be utilized to plan, conduct and verify cybersecurity audits everywhere. The CSAM has been designed to conduct partial or complete cybersecurity audits either by a specific domain, several domains or the comprehensive audit for all domains.

6. Conclusions

This study introduces the CyberSecurity Audit Model (CSAM) design and all its components, the aim of this model is to evaluate and measure the cybersecurity assurance, maturity and cyber readiness in any organization. In addition, the model can evaluate the effectiveness of cybersecurity guidelines for any Nation State linked to its national cybersecurity strategy or policy.

The CSAM was tested, implemented and validated along with the Cybersecurity Awareness TRAining Model (CATRAM) in a Canadian higher education institution. A research case study is being conducted to validate both models and the findings will be published accordingly.

Since there aren't universal acceptance or standardization in terms of defining cybersecurity audit scopes, aims and domains, further research is required and encouraged in the cybersecurity areas of assurance and audits.

References

Bodeau, D., Boyle, S., Fabius-Greene, J., and Graubart R. (2010). "Cyber Security Governance", *MITRE*. Retrieved January 24, 2018, from https://www.mitre.org/sites/default/files/pdf/10_3710.pdf.

Boyce, R. (2001). *"Vulnerability Assessment: The Pro-Active Steps to Secure your Organization"*, SANS Institute. Retrieved January 24, 2018, from https://www.sans.org/reading-room/whitepapers/threats/vulnerability-assessments-pro-active-steps-secure-organization-453.

CERT Division. (2017). *"CSIRT Frequently Asked Questions*", Carnegie Mellon University. Retrieved January 24, 2018, from https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm.

Department of Homeland Security. (2012). "*Vulnerability Assessment and Management*", NICSS. Retrieved January 24, 2018, from https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/vulnerability-assessment-and-management.

Donaldson, S., Siegel, S., Williams, C., and Aslam, A. (2015). "*Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*". New York: Apress, pp. 201-204.

Financial Executives International – FEI. (2014). "*Financial Executives, Cyber Security & Business Continuity*", Canadian Executives Research Foundation (CFERF). Retrieved January 24, 2018, from https://www.feicanada.org/enews/file/CFERF%20studies/2013-2014/IBM%20Cyber%20Security%20final3%202014.pdf.

Financial Industry Regulatory Authority – FINRA. (2015). "*Report on Cybersecurity Practices*", pp 1- 46. Retrieved January 24, 2018, from https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

Foresite. (2016). "*Quick guide to common Cybersecurity Frameworks*". Retrieved January 24, 2018, from https://www.foresite.com/blog/quick-guide-to-common-cybersecurity-frameworks/.

ISACA. (2014). *Implementing the NIST Cybersecurity Framework*. Rolling Meadows: ISACA.

ISACA. (2013). Transforming Cybersecurity. Rolling Meadows: ISACA.

ISACA. (2015). Cybersecurity Fundamentals. Rolling Meadows: ISACA

Karspersky Lab. (2015). "*Top 10 Tips for Educating Employees about Cybersecurity*", AO Kaspersky Lab. Retrieved January 24, 2018, from http://go.kaspersky.com/rs/kaspersky1/images/Top_10_Tips_For_Educating_Employees_About_Cybersecurity_eBook.pdf.

Lee, R. (2015). "*The Sliding Scale of Cybersecurity*", SANS Institute. Retrieved January 24, 2018, from https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240.

Ministry of Economic Affairs and Communication. (2017). "2014-2017 Estonia Cybersecurity Strategy", *ENISA*. Retrieved January 24, 2018, from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf.

National Cyber Security Alliance. (2017). "*Stay Safe Online*", NCS. Retrieved January 24, 2018, from https://staysafeonline.org/ncsam/.

National Institute of Standards and Technology - NIST. (2017). *"Framework for Improving Critical Infrastructure Cybersecurity*", version 1.1.

National Institute of Standards and Technology – NIST. (2017). "*NIST Special Publications SP*". Retrieved January 24, 2018, from http://csrc.nist.gov/publications/PubsSPs.html.

NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE. (2015). *"Cyber Security Strategy Documents*". Retrieved January 24, 2018, from https://ccdcoe.org/strategies-policies.html.

North American Electric Relaibility Corporation – NERC. (2010). "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets", *NERC*. Retrieved January 24, 2018, from <www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf.

Organisation for Economic Co-Operation and Development – OECD. (2012). "Cybersecurity Policy Making at a Turning Point", *OECD*. Retrieved January 24, 2018, from http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

PCI Security Standards Council. (2014). "Best Practices for implementing a Security Awareness Program", *PCI DSS*. Retrieved January 24, 2018, from <https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.

Pricewaterhouse Coopers - PwC. (2016). "PwC's Board Cybersecurity Governance Framework", *PwC*. Retrieved January 24, 2018, from <https://www.pwc.com/ca/en/consulting/publications/20160310-pwc-reinforcing-your-organizations-cybersecurity-governance.pdf.

Proaño, R., Saguay, C., Jacome, S. and Sandoval, F. (2017). "Knowledge based systems as an aid in information systems audit". *Enfoque UTE*. V.8 Sup. 1, Feb 2017, pp.148-159. https://doi.org/10.29019/enfoqueute.v8n1.122

Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Cano, J. (2017). "A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)". *2017 Second International Conference on Information Systems and Computer Science* (INCISCOS), Quito, Ecuador.

SANS Institute. (2017). "SANS Forensics Whitepapers", *SANS Institute*. Retrieved January 24, 2018, from https://digital-forensics.sans.org/community/whitepapers.

Shackleford, D. (2015). "Who's using Cyberthreat Intelligence and how?",SANS Institute. Retrieved January 24, 2018, from https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767.

Trusted Computing Group. (2013). "*Architect's Guide: Cybersecurity*". Retrieved January 24, 2018, from https://www.trustedcomputinggroup.org/wp-content/uploads/Architects-Guide-Cybersecurity.pdf.

United States Computer Emergency Readiness Team - US-CERT. (2017). "Cybersecurity Framework", *US-CERT.* Retrieved January 24, 2018, from https://www.us-cert.gov/ccubedvp/cybersecurity-framework.

U.S. Department of Homeland Security. (2016). "*Cybersecurity*". Retrieved January 24, 2018, from https://www.dhs.gov/topic/cybersecurity.

U.S. Department of Energy. (2007). "*IT Security Architecture*". Retrieved January 24, 2018, from https://energy.gov/sites/prod/files/cioprod/documents/DOE_Security_Architecture.pdf.