International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.109-120
http://dx.doi.org/10.14257/ijsia.2017.11.1.10

A Classification Scheme for Cybersecurity Models

Issa Atoum[1] and Ahmed Otoom[2]

[1]*Faculty of Information Technology, The World Islamic Sciences & Education University, Amman, Jordan*
[1]*Issa.Atoum@wise.edu.jo,* [2]*otoom@hotmail.com*
[2]*Independent Researcher, Amman, Jordan*

Abstract

Cybersecurity is important for information dissemination, privacy and the human life. Managing cybersecurity related issues (such as banking hacks or phishing scams) during development, operation, and maintenance of cybersecurity models is a challenging task. Nearly no guidance is available on how to select, adapt, combine, and evolve cybersecurity models. This problem is due to the nature of cybersecurity models that are highly context-dependent. Therefore, cybersecurity models need to be adaptable and in accordance with the respective project goals. Consequently, encouraging decision makers to assign and plan human resources and technologies, and to enhance communication between relevant stakeholders. We defined a classification scheme, a global criterion for any cybersecurity model and then used it to compare a large set of cybersecurity models. Results showed that our scheme is able to identify cybersecurity models based on organizational needs. Furthermore, we found a research gap in regard to cybersecurity models that need to be implemented internationally.

Keywords*: cybersecurity implementation frameworks, cybersecurity strategy, threat analysis.*

1. Introduction

Cybersecurity is used to refer to the integrity of our personal privacy, to security of our critical infrastructure, to military threats and to the protection of intellectual property [1]. The cyber attacker has the lead in digital realms while the defender has the advantage as he knows details of used cybersecurity models; thus he/she is able to setup adequate defenses ahead of time. Recently, many breaches and incidents were reported: Qatar National Bank has suffered a massive breach involving 1.4 GB of sensitive internal files being dumped online by unknown attackers in April 2016, Bangladesh Bank attackers hacked SWIFT Software on April 2016, TalkTalk in October 2015, and email disclosure by the Bank of England in May 2015. 50% of world breaches in the last year were caused by inadvertent human error, the main actor in cybersecurity models.

The cybersecurity problem is challenging due to inability to create a fully real-world settings [2]. This could be due to improper adaptation of diverse cybersecurity models. Typical cybersecurity models focus on traditional information security aspects[3] [4], adherence to security policies [5] [4], defensive decision support models[6] [7]. Each of these models usually supports only a limited set of application purposes. Some of these models are deemed to be used at the organization level[8] while others could be used at the country level[9]. Several cybersecurity models are suitable for prediction[10] and decision making[11] [12].

The multitude of cybersecurity models available and the lack of guidance for selecting and adapting these models implies a need for getting a structured classification of available cybersecurity models. Therefore, supporting higher-level cybersecurity goals of an organization. Currently, it is not obvious for which usage purposes the cybersecurity

ISSN: 1738-9976 IJSIA

models are suitable, in which contexts they can be applied, and how to customize them. Moreover, the evaluation of many models are limited to specific contexts and is difficult to find in the literature. Consequently, cybersecurity decision makers have significant problems in identifying the appropriate set of cybersecurity models that is relevant to them. Furthermore, the lack of a uniform classification of cybersecurity models aggravates the communication regarding cybersecurity issues.

This article creates a structured classification and overview of available cybersecurity models. The reference [13] shed the light on a possible direction towards resolving this problem. He identified six factors that determine a good cybersecurity strategy which are: purpose and role of information security, societal trends, human elements, interaction and complexity, information security management and changing technologies. Literature proposed many models in in different contexts; network infrastructure[14], security standards [15], and decision support systems[16]. The reference [17] proposed a comparison of several cybersecurity frameworks , however their work is limited. This article classifies cybersecurity models in order to achieve several objectives. These objectives are believed to enhance communication between related cybersecurity stakeholders, supports the identification of gaps, support the selection and adaptation of several cybersecurity models.

Figure 1. Proposed Classification Scheme

First, we deduce a comparison criterion. Then we review a few cybersecurity models. Next, we evaluate studied modules. Finally, we conclude this paper.

2. Proposed Cybersecurity Classification Scheme

To the best of our knowledge, there are no specific guidelines of the best aspects of cybersecurity models. cybersecurity goes beyond the boundaries of traditional information security[61] to include the person him/herself [60]. The reference [62] defined 100 requirements when considering end-to-end cybersecurity models. They discussed several questions to design a strong cybersecurity program that includes, among others; strategy, governance and control, standards and processes, laws and regulations, human resources and research and development. Recently, the reference [63] identifies different angles on which to see cybersecurity; technical and conceptual issues , cyberspace as a domain of content, and even the cybersecurity context.

Figure 1 shows the proposed classification scheme. First, we studied a large set of cybersecurity models. Then, we elicit common cybersecurity features among studied works. Next, we generalize features such that more abstract features cover the low level features (e.g. confidentiality covers encryption techniques features, etc.). After that, we added other features that could be added to enhance our classification scheme in regard to cybersecurity models research gaps. Finally, our rules(constraints) converts features to a list of criterion. Therefore, we devise the top 10 criterion based on studied works and proposed by this work.

1. Basic security principles: cybersecurity model should support the heart of information security; confidentiality, integrity, and availability.
2. Defense depth: information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information.

3. Defense strategy: proactive models should take proactive decisions in regard to possible incidents such as legislation and proper guidelines and recovery plans. Preventive models trigger prevention actions one a threat is detected.
4. Cybersecurity controls coverage: selecting proper controls and implementing them will help an organization to bring down risk to acceptable levels. The ISO/IEC 27001:2005 model defines 133 controls. A good cybersecurity model should contain risk, administrative, logical and physical control components.
5. Resilience: the ability of the model to be flexible with unseen changes in technology, environment, attack methods, etc.[64], [65]. Resilient management systems and processes will provide greater protection against multidimensional attacks [66].
6. Compliance: a compliance model follows a security standard or a best practice in a cybersecurity domain. Thus, allowing the cybersecurity model to make portable changes between security related standards or cybersecurity models. [67] .
7. Tracking: the model should be able to detect if further modification is needed in security models or cybersecurity strategies. The tracking could be at the packet level up to the organizational level.
8. Performance measurement: the ability to measure performance of security initiatives effectively at various organizational levels. It also should audit whether the security policy and strategies are being effectively implemented.
9. Information classification: an important aspect of information security and the risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information.
10. Cybersecurity implementation level: the level which security measures are being measured; the enterprise, national, or international level. The reference [66] indicated that security should be placed in a holistic setting. The reference [68] pointed out that cybersecurity requires a holistic approach. The references [17], [69]–[71] showed that holistic approaches must be considered to cover various aspects of cybersecurity.

3. Landscaping Cybersecurity Models

There exist a variety of different cybersecurity models for different application scenarios, and it is a challenging task to create a landscape of existing models. The below gathered related literature is grouped into the following logical categories to facilitate a structured reading and analysis.

3.1. Standard Models

Security Maturity models are used to ensure that an organization has adopted a set of procedures or standards in the security domain. The Security Engineering Capability Maturity Model (SSE-CMM) is used to ensure that an organization applies in practice security engineering principles [3]. The SSE-CMM model has been approved as the ISO/IEC 21827 International Standard and henceforth, its certification is maintained by the International Systems Security Engineering Association (ISSEA). The ISO/IEC 21827 additionally covers areas of concurrent interaction within the organization and other organizations, and the security project execution cycle [18]. The Information Security Program Maturity Grid (ISPMG) is a tool composed of five stages of security maturity and five measurement categories that may be used by management in evaluating an enterprise's maturity from the perspective of information security [19]. The Fraunhofer Institute for Software and Systems Engineering (ISST) has developed SMM to assess a company's IT security [20]. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) is a risk-based information security strategic assessment and

planning. In OCTAVE® model, the organization could set the security strategy based on the current evaluation of organizational risks[21].

Security metrics are often qualitative methods to measure how an organization is secured. There are many guiding standards and good experiments of security metrics. The Federal Information Processing Standards Publication (FIPS PUB) FIPS 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements for cryptographic module to protect sensitive information within computer and telecommunications systems[4]. The Information Technology Security Evaluation Criteria (ITSEC), Trusted Computer System Evaluation Criteria ITSEC is a structured set of criteria for evaluating computer security within products and systems used in Europe. The ITSEC criterion is currently superseded with the Common Criteria (CC) which is an ISO/IEC 15408 standard. The ISO/IEC 15408 computer security certification standard is a framework to specify security functional and assurance requirements. The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) is a combination of the TCSEC and ITSEC, a computer security standard published by the Communications Security Establishment to provide evaluation criteria for IT products. The Special Publications of the 800 series present documents of general interest to the computer security community and is based on ITIL's research, and governmental organizations. [22]

The ISO/IEC 27001 is considered the key security standard for information security management. The ISO 22301 suggests to consider business continuing as well as availability. The ISO/IECC 20000-1:2011 information technology service management covers management aspects, such as change management, release management and asset management. The BS 10012 personal information management develops information for personal in accordance with data protection legislation. The Cybersecurity Information Exchange Framework (CYBEX) was proposed to provide a framework for information exchange on a global scale. It has five functional components; the information description block, discovery block, query block, assurance block, transport block. Several works [23] [21] found that the current standards are broad and not effective for cybersecurity.

Standard models are very generic; thus suitable customization should be applied to be accepted in certain organizational context.

3.2. Decision Support Models

In this category cybersecurity models could be grouped into three groups: the governance and management models, business alignment models, and optimization models. Many Information security models target the management perspective of information security. The reference [6] suggested a conceptual framework for information security management, which is composed of two major components: information security framework and the information security management program. The reference [7] proposed to manage security of an enterprise using a set of defined activities mapped to system security engineering maturity model. In the same category , proper controlling is suggested to ensure security governance[24], and information security management system evaluation [25] are being continuously explored to their crucial importance to cybersecurity.

Many governments deploy Enterprise Architectures (EA) solutions to align between different IT projects (e.g. e-government projects) and government business, to ensure interoperability, avoid duplication, and identify Business-IT gaps. The reference [26] suggested a National EA framework composed of architectures , principles and standards to compare the architecture of Denmark and the Netherlands. The EA initiatives face complicated governance and insufficient support for the development, according to a case study by [27].

Several cost estimation models were proposed in order to find the optimum invest to mitigate possible threats. The reference [11] suggested a framework for valuation of IT security based on business process. The approach makes a trade-off comparison between

the cost of losing business opportunity and the cost of ensuring security to a specific level. The decision maker could be able to decide which security level to select according to cost benefit analysis. The reference [16] employed the game theory and the knapsack approach in order to highlight the weakness and strengths of different investment approaches in cybersecurity. By comparing the budget and the expected damage after conducting cybersecurity risk assessment, and optimal amount of investment could be obtained. The reference [28] provided a model to the key requirement in security planning for any threat scenario and apply specific countermeasures. The reference [10] proposed Risk Assessment and Optimization Model (RAOM) to solve the security countermeasure selection problem, where variables such as financial cost and risk may affect the final decision of risk level. The reference [12] optimized countermeasures in IT security planning to prevent or mitigate cyber-threats and a mixed integer programming approach is proposed for the decision making. The reference [29] provides a mathematical model to suggest the best amount of investment in order to quantify potential damages to cyber space. The model makes a trade-off between cost of investment and the expected benefits. The model showed that an organization should not invest more than 37% of expected loss.

Decision support models target higher management and may lose proper communication with lower levels of cybersecurity systems.

3.3. Privacy Models

The Innovation Framework for Privacy and Cybersecurity Market Opportunities (IPACSO) model supports an innovation framework to enhance the overall innovation, engagement for industry and the research community, as well as management and deployment activities. It aims to support ICT Security innovators with State of the Art methodologies and best practices in their innovation process [30]

The reference [1] showed the complexity of integrating the private and public in cybersecurity activities. There are many parameters that need to be taken into consideration, including legislation, responsibility and accountability. It founds that there is fundamental disjuncture between the expectation of the two partners. Many models showed that not only technical issues affect the cybersecurity, but also human aspects. The human reliability and statistical quality control must be considered for better quality assurance [31] [9]. The references [5] [4] showed that several human factors such as behavioral, knowledge and situational characteristics affect human trust and thus the cybersecurity system. They build a risk assessment model based on the user, information technology analyst, defender and attacker in order to predict potential threats.

Although privacy is one goal of a good cybersecurity model, privacy models of its own has conflicting goals with requested highly secured systems.

3.4. Infrastructure Models

Grid communications nowadays supports self-healing, energy reliability and security. Therefore, they are vulnerable to cybersecurity threats. Smart grids require high performing networks and connectivity and sophisticated protocols to support cybersecurity. The North American Electric Reliability Corporation (NERC) and the ISO/IEC 17799 specify guidelines for power systems. The Supervisory Control and Data Acquisition (SCADA) [32] systems are widely used in the industry for monitoring and controlling power grids. The Process Control System (PCS) implanted with a closed loop for ongoing tasks. Distributed control systems (DCS) are the complex combination of PCS and SCADA. A cyber impact analysis framework for electric smart grid using directed graph was proposed by [33]. Their model has three stages; synthesis, system analysis, and system validation. The reference [34] model provides control and data acquisition framework. It has three phases; real time monitoring, anomaly detection,

impact analysis and mitigation strategy. The model of [34] provides a vulnerability assessment model using attack trees to protect SCADA systems. Using the mathematical model probabilities could be calculated and thus countermeasures will be enforced.

Although the infrastructures cybersecurity model saves cybersecurity systems' ground, they are too detailed and they might need additional resources for unneeded cybersecurity feature that does not support cybersecurity project goals.

3.5. Enterprise Frameworks

These models are proposed to be used at the organization level. The IBM® Center for the Business of Government reports that there is a need of CIO at the state level [35] . The IBM® security framework consists of five components: data, people, network, infrastructure, and process. The IBM® framework influence governance, risk management and compliance through complete IBM® solutions. The IBM® Framework and IBM® blueprint suggest a secure-by-design approach which means that implementation of this framework will need to use IBM® software and hardware solutions which finally limits the user needs in terms of costs and needed customization at the national level [36].

Oracle® has a set of library guidelines and reference architectures called Oracle Reference Architecture (ORA) that can be used by organizations to plan and execute their IT initiatives. They suggest a conceptual architecture to show how architectural concepts are associated with information security within the ORA.[8]

In addition, there are various available Enterprise Architecture (EA) frameworks vary in: completeness, visual aspects, simplification, and representation. The reference [37] define a matrix of stakeholders' viewpoints, and six main abstractions in describing information security. It does not consider explicitly security concerns. The Federal Enterprise Architecture Framework (FEAF) is a structure for organizing Federal resources. Security standards are part of FEAF components [38]. The Department of Defense Architecture Framework (DoDAF) focus is to understand complex EA models to facilitate decision making [2]. The Open Group Architecture Forum (TOGAF) describes guidelines, models and methods of developing EA[39].

The EA frameworks help to answer 'what' questions not 'how' questions as indicated by EA consultant company [40]. Moreover, most of the EA frameworks are used in financial and insurance sectors and to our knowledge they have been never used specifically for cybersecurity on a national level [41].

3.6. Generic Frameworks

A generic framework for strategy implementation was suggested in [42]. It includes these components: devising rewards and incentives, shaping the corporate culture, and strategic leadership. Their framework is abstract and is more suitable to business strategies.

The reference [9] suggested a generic cybersecurity framework consisting of a cybersecurity Management Framework (CSMF) overseen by a Security Framework for Protecting Business, Government and Society (SFPBGS). The CSMF provides a linkage between outputs of Social, Legal, Economic, Political, Technological (SLEPT) analysis and Strengths, Weaknesses, Opportunities and Threats (SWOT). The main goal of Trim's work is to allow mangers to incorporate counter intelligence and places risk in a manageable context. The McCumber Cube model is a conceptual model indicating assurance requirements [43]. It shows that the education, training and assurance should be in-line with information states and information characteristics.

The U.S Computer Emergency Readiness Team (US-CERT) start cybersecurity threat prevention since 1980. At the same level, the EU cybersecurity strategy [44] is coupled with Europe 2020 strategy. International Telecommunication Union (ITU) suggests a

management framework for Organizing national cybersecurity. The ITU model depends on five factors: national strategy, government industry collaboration, deterring cybercrime, incident management capabilities, and culture of cybersecurity [45]. Each element of the ITU framework recommends a policy, a goal and a specific step. An application of the ITU framework has been applied to other countries (e.g. Morocco [46]). The ITU framework is a step by step management plan and is very abstract in the sense that no security engineering components are identified.

Generic frameworks could be applied to many cybersecurity contexts; however, a proper cybersecurity strategy implementation must be in place.

3.7. National Frameworks

According to a recommendation by the European Network and Information Security Agency (ENISA), the ICT systems must be secured in Europe coherently across geographical borders and should be followed consistently over time [47]. The Agency helps in identification and analysis of threat trends over time, suggests policy implementation and infrastructure protection, but does not identify a specific framework.

Most of the international information security strategies include guidelines in order to facilitate their implementation [48]–[52]. The reference [53] suggested an Awareness Toolkit as an approach to implement the strategy of South Africa. The Department of Defense [54] has suggested the implementation of the strategy in phases to be executed by security implementation vendors coordinating with various related government organizations. Unfortunately, these strategies do not provide a clear implementation or performance controls to holistically monitor the implementation. The reference [55] proposed a model to align the Taiwanese national policy with standards of the ISO/IEC 27001 and the BS 7799. Recently provide a holistic model cybersecurity model of multi-tier missions comprised of multiple craft with heterogeneous movement and sensing capabilities [56]. A suggested implementation framework for Jordan was presented in [57]. Their framework is targeting Jordan only, needs a validation model, suggests a very high level organizational structure and does not widely address performance measures that monitor and control the implementation process.

Table 1. Cybersecurity Models' Comparison. Numbers in Columns Indicate Studied Models' Sections

Model # / Criterion	2.1	2.2	2.3	2.4	2.5	2.6	2.7
1	*High*	*average*	*high*	*high*	*Average*	*high*	*high*
2	*High*	*high*	*high*	*low*	*high*	*average*	*high*
3	*Both*	*both*	*preventive*	*preventive*	*proactive*	*both*	*proactive*
4	*Average*	*average*	*low*	*low*	*high*	*average*	*high*
5	*Low*	*low*	*high*	*high*	*high*	*average*	*high*
6	*High*	*low*	*low*	*low*	*high*	*high*	*high*
7	*Low*	*average*	*low*	*low*	*high*	*average*	*high*
8	*Average*	*average*	*high*	*high*	*high*	*average*	*high*
9	*Average*	*average*	*high*	*high*	*high*	*average*	*high*
10	*National*	*enterprise/ national*	*enterprise/ national*	*enterprise*	*national*	*enterprise*	*enterprise / national*

The Integrated Governance, Risk and Compliance (iGRC) Consortium is doing an on-going research program to protect the UK. The iGRC is using their integrated Enterprise information security management system, extended with the open interoperability

protocol (GRCiP) along with network sensor technologies from participating companies. The goal is to automatize threat level and control status changes in real-time so that critical information infrastructure is made more resilient and be able to withstand the increasing number of attacks. We consider this framework a mixed between management and technology however it is specialized in UK.[58]. The research on iGRC framework is still on-going and it does not address holistic performance controls.

In the same category, the German IT protection Manual is a collection of huge documents (more than 3000 pages) from the German Federal Office for Security in Information Technology (BSI) that provide useful information for detecting weaknesses and combating attacks in IT environment [59].

National frameworks protect the cyberspace at the country level, but leaves risks of potential threats that could come from outsiders. They may be also subject to legacy and political issues in other countries in the cyberspace.

4. Evaluation and Discussion

We evaluate the models discussed in Section 3 using the proposed criteria in Section 2. Unfortunately, we cannot judge whether a cybersecurity model satisfies a certain criterion completely. Therefore, we grade the models as *low*, *average* and *high* to indicate the level of criterion satisfaction. From Table 1, decision support models (i.e. Section 3.2) are *low* in resilience criterion because it is deemed for optimizing cost and benefits. However, national models are *high* in several criteria because it has the ability to integrate with systems worldwide thus, they are sophisticated systems. Standard (i.e. Section 3.1) and generic (i.e. Section 3.6) models are considered guidelines; thus they have *average* controls. Standard models need further customization to be accepted in a certain country, or a domain while generic models are abstract. Privacy models (i.e. Section 3.3) are provided to protect the privacy of information, thus they got *high* in performance criterion. Infrastructure models (i.e. Section 3.4) provides preventive actions, thus they have *low* controls and compliance, and does not necessarily track possible change at higher cybersecurity strategies. Generally, national models (Section 3.7) have the *highest* performance among compared models. Although many models are proposed as part of the vision of the Europe 2030, or US, we did not come across a model that is found to be used internationally.

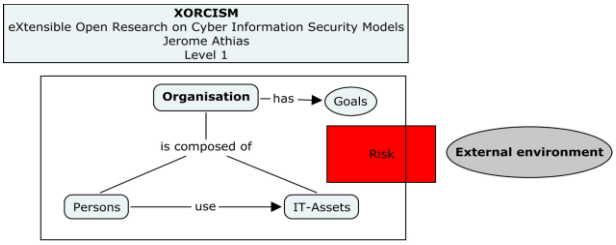

Figure 2. Link between Management and Technical

	Dimention		
Purpose	Product	Resource	Project
Controling	[17]		
Compliance		[26]	
Implementation Level	[32]		
Performance	[69]		

Figure 3. A Ssample Cybersecurity Landscape

Furthermore, we found that in many cases models are very technical and do not consider management dimensions of cybersecurity (Section 3.1 versus Section 3.2). Therefore, we found a *linkage* between *management* and *technical* levels. The previous

finding is also acknowledged by the XORCISM (eXpandable Open Representation of Cyber Information Security Management) framework. The XORCISM Model is built around various open information security data models, specifications, standards, frameworks, guidelines, architectures, best practices, protocols and vocabularies. Figure 2 shows that in order to achieve an organization's goals the persons and IT assets should be harmonized. Risks are potentially related to IT assets, persons or the external environment.

Figure 3 shows a sample cybersecurity landscape. It shows the relationship between the purpose of cybersecurity models and the dimension (or object) that the model covers. The reference [17] was proposed for the purpose of controlling cybersecurity models, yet it covers the product (partially), the resources (data and human), and the project goals. However, the reference [32] covers the product and the resource dimensions.

Our evaluation deduced several implications. There is no complete cybersecurity model. A good cybersecurity model is a one that supports project and organization goals. Adapting various cybersecurity models requires diverse experts in different domains. One of major cybersecurity issues that remains open; the human who selects and adapts cybersecurity models.

5. Conclusion

This paper presents the first step towards developing a classification scheme landscaping cybersecurity models. We studied various cybersecurity models, ranging from infrastructure models till generic national models, and then built a comparison criterion for studied models. Results showed that our scheme is able to identify cybersecurity models based on organization needs. We found that there is no comprehensive cybersecurity model. Moreover, we found that there is an immense need for cybersecurity models at the international level. Future work will be in the area of refining and empirically evaluating the proposed classification. We recommend to build up a database of existing cybersecurity models based on our proposed classification scheme.

References

[1] M. Carr, "Public–private partnerships in national cyber-security strategies," *Int. Aff.*, vol. 92, no. 1, pp. 43–62, 2016.
[2] L. J. Hoffman, T. Rosenberg, R. Dodge, and D. Ragsdale, "Exploring a national cybersecurity exercise for universities," *IEEE Secur. Priv.*, vol. 3, no. 5, pp. 27–33, Sep. 2005.
[3] Carnegie Mellon University, "Systems Security Engineering Capability Maturity (SSE-CMM®) Model Document Ver 3.0," 2010.
[4] National Institute of Standards and Technology (NIST), "Security Requirements For Cryptographic Modules," Gaithersburg, 2001.
[5] D. Henshel, M. G. Cains, B. Hoffman, and T. Kelley, "Trust as a Human Factor in Holistic Cyber Security Risk Assessment," *Procedia Manuf.*, vol. 3, pp. 1117–1124, 2015.
[6] A. L. Nnolim, "A framework and methodology for information security management," Lawrence Technological University, 2007.
[7] A. Zuccato, "Holistic security management framework applied in electronic commerce," *Comput. Secur.*, vol. 26, no. 3, pp. 256–265, May 2007.
[8] Oracle®, "Information Security: A Conceptual Architecture Approach [White Paper]," 2011.
[9] P. R. J. J. Trim and Y.-I. Lee, "A security framework for protecting business, government and society from cyber attacks," *2010 5th Int. Conf. Syst. Syst. Eng.*, pp. 1–6, Jun. 2010.
[10] V. Viduto, C. Maple, W. Huang, and D. López-Peréz, "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem," *Decis. Support Syst.*, vol. 53, no. 3, pp. 599–610, 2012.
[11] T. Neubauer, M. Klemen, and S. Biffl, "Business process-based valuation of IT-security," in *ACM SIGSOFT Software Engineering Notes*, 2005, vol. 30, no. 4, pp. 1–5.
[12] T. Sawik, "Selection of optimal countermeasure portfolio in {IT} security planning," *Decis. Support Syst.*, vol. 55, no. 1, pp. 156–164, 2013.

[13] K. Fielden, "An Holistic View of Information Security : A Proposed Framework," *Int. J.*, vol. 4, no. 1, pp. 427–434, 2011.
[14] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Trans. Syst. Man, Cybern. - Part A Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.
[15] E. Humphreys, *S27 Platinium Book Twenty Years of ISO/IEC JTC 1/SC27 Information Security Standardisation*. ISO/IEC JTC 1/SC27, 2008.
[16] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decis. Support Syst.*, p. , 2016.
[17] I. Atoum, A. A. Otoom, and A. Abu Ali, "A Holistic Cyber Security Implementation Framework," *Int. J. Inf. Secur.*, vol. 22, no. 3, pp. 251–264, 2014.
[18] A. Tsohou, S. Kokolakis, C. Lambrinoudakis, and S. Gritzalis, "Information Systems Security Management: A Review and a Classification of the ISO Standards," in *Next Generation Society. Technological and Legal Issues SE - 21*, vol. 26, A. Sideridis and C. Patrikakis, Eds. Springer Berlin Heidelberg, 2010, pp. 220–235.
[19] T. R. Stacey, "Information security program maturity grid," *Inf. Syst. Secur.*, vol. 5, no. 2, pp. 22–33, 1996.
[20] H. Kurrek, "SMM - Assessing a Company's IT Security," *ERCIM News*, Apr-2002.
[21] C. J. Alberts and A. J. Dorofee, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional, 2003.
[22] A. J. A. Wang, "Information security models and metrics," *Proc. 43rd Annu. southeast Reg. Conf. - ACM-SE 43*, vol. 2, p. 178, 2005.
[23] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance amp; Security," in *International Conference on Availability, Reliability and Security (ARES), 2013 Eighth*, 2013, pp. 546–555.
[24] R. Von Solms, K. L. L. Thomson, and P. M. M. Maninjwa, "Information security governance control through comprehensive policy architectures," in *Information Security South Africa (ISSA), 2011*, 2011, pp. 1–6.
[25] H. Jo, S. Kim, and D. Won, "Advanced Information Security Management Evaluation System," *KSII Trans. Internet Inf. Syst.*, vol. 5, no. 6, pp. 1192–1213, 2011.
[26] M. Janssen and K. Hjort-Madsen, "Analyzing enterprise architecture in national governments: The cases of denmark and the netherlands," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, 2007, p. 218a–218a.
[27] V. Seppanen, J. Heikkila, and K. Liimatainen, "Key Issues in EA-implementation: Case study of two Finnish government agencies," in *2009 IEEE Conference on Commerce and Enterprise Computing*, 2009, pp. 114–120.
[28] T. R. Rakes, J. K. Deane, and L. Paul Rees, "IT security planning under uncertainty for high-impact events," *Omega*, vol. 40, no. 1, pp. 79–88, 2012.
[29] L. A. Gordon, M. P. Loeb, and L. Zhou, "Investing in Cybersecurity: Insights from the Gordon-Loeb Model," *J. Inf. Secur.*, vol. 7, no. 2, p. 49, 2016.
[30] Z. Dooly, S. Galvin, J. Power, B. Renard, and U. Seldeslachts, "IPACSO: towards developing an innovation framework for ICT innovators in the privacy and cybersecurity markets," in *Cyber Security and Privacy*, Springer, 2014, pp. 148–158.
[31] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human Behaviour as an aspect of Cyber Security Assurance," *CoRR*, vol. abs/1601.0, 2016.
[32] A. G. Bruce and R. Lee, "A framework for the specification of SCADA data links," *Trans. Power Syst.*, vol. 9, no. 1, pp. 560–564, 1994.
[33] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010, pp. 244–249.
[34] C. W. Ten, C. C. Liu, and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," in *Power Engineering Society General Meeting*, 2007, pp. 1–8.
[35] M. Goodyear, H. T. Goerdel, S. Portillo, and L. Williams, "Cybersecurity Management in the States : The Emerging Role of Chief Information Security Officers," *IBM Cent. Bus. Gov.*, 2010.
[36] A. Buecker, M. Borrett, C. Lorenz, and C. Powers, "Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security," *IBM Redguides Bus. Leaders REDP-4528-01*, vol. 4528, no. 1, 2010.
[37] Zachman International®, "Zachman Framework 3.0," 2012. [Online]. Available: http://www.zachman.com/.
[38] Office of Management and Budget, "Federal Enterprise Architecture (FEA)," *The White House*, 2012. [Online]. Available: http://www.whitehouse.gov/omb/e-gov/fea.
[39] The Open Group, "Open Group Architecture Forum," 2012. [Online]. Available: http://www.opengroup.org/architecture/.
[40] EAdirections, "EA Frameworks : Pros and Cons – Inventory and Insights," 2013.

[41] S. M. Oda, H. Fu, and Y. Zhu, "Enterprise information security architecture a review of frameworks, methodology, and case studies," in *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 2009, pp. 333–337.
[42] R. Barnat, "Strategic Management : The Nature Of Strategy Implementation," 2005. [Online]. Available: http://www.strategy-implementation.24xls.com/en100. [Accessed: 03-Feb-2012].
[43] J. McCumber, "Information systems security: A comprehensive model," in *Proceedings of the 14th National Computer Security Conference*, 1991.
[44] EC, "Cyber Security Strategy of the European union: An Open Safe and Secure Cyberspace," 2013.
[45] International Telecommunication Union(ITU), "Management Framework for Organizing National Cybersecurity / CIIP Efforts," 2008.
[46] M. D. E. D. E. el Kettani and T. Debbagh, "NCSec: a national cyber security referential for the development of a code of practice in national cyber security management," in *Proceedings of the 2nd international conference on Theory and practice of electronic governance*, 2008, pp. 373–380.
[47] European Network and Information Security Agency (ENISA), "Cyber security : future challenges and opportunities," 2011.
[48] The White House, "The Comprehensive National Cybersecurity Initiative," 2009.
[49] U.S. DoD, "Department of defense Strategy for operating in cyberspace," 2011.
[50] HM Government, *A strong Britain in an age of uncertainty: the national security strategy*. The Stationery Office, 2010.
[51] Government of Australia, "Cyber SeCurity Strategy," 2009. [Online]. Available: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG Cyber Security Strategy - for website.pdf.
[52] R. V. A. N. Suid-afrika, "South African National Cybersecurity Policy," 2010.
[53] L. J. Phahlamohlaka, J. C. Jansen van Vuuren, and A. J. Coetzee, "Cyber security awareness toolkit for national security: an approach to South Africa's cyber security policy implementation," in *Proceedings of the first IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW)*, 2011, pp. 1–14.
[54] Estonia Department of Defence, "Cyber Security Strategy -Estonia," 2008. [Online]. Available: http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf. [Accessed: 01-Feb-2012].
[55] C.-Y. Ku, Y.-W. Chang, and D. C. Yen, "National information security policy and its implementation: A case study in Taiwan," *Telecomm. Policy*, vol. 33, no. 7, pp. 371–384, Aug. 2009.
[56] J. Straub, "Cybersecurity Methodology for a Multi-Tier Mission and Its Application to Multiple Mission Paradigms," in *Proceedings of the 2016 IEEE Aerospace Conference*, 2016.
[57] A. Otoom, "A Proposed Implementation Framework (PIF) for the National Information Assurance and Cyber Security Strategy (NIACSS)," in *Conference on Security and Saftey in the Cyberspace*, 2011.
[58] IGRC, "The integrated governance, risk and compliance (iGRC) Consortium," 2011. [Online]. Available: http://www.informationsecurityprotection.com/. [Accessed: 01-Apr-2012].
[59] D. Henze, "IT baseline protection manual," *Fed. Agency Secur. Inf. Technol. Ger.*, 2000.
[60] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013.
[61] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, no. October 2015, pp. 1–13, 2016.
[62] J. Suffolk, "Cyber Security Perspectives," *Huawei Publ.*, no. October, 2013.
[63] B. Gier, B. Z. Yuan, and B. Gier, "Perspectives on Cybersecurity: A Collaborative Study," *MIT Polit. Sci. Dep. Res. Pap. No. 2016-2*, 2016.
[64] A. Rashid, W. Joosen, and S. Foley, "Security and resilience of cyber-physical infrastructures," in *Proceedings of the First International Workshop with the International Symposium on Engineering Secure Software and Systems*, 2016.
[65] O. Erol, B. J. Sauser, and M. Mansouri, "A framework for investigation into extended enterprise resilience," *Enterp. Inf. Syst.*, vol. 4, no. 2, pp. 111–136, 2010.
[66] P. Trim and Y.-I. Lee, "A security framework for protecting business, government and society from cyber attacks," *5th Int. Conf. Syst. Syst. Eng.*, pp. 1–6, Jun. 2010.
[67] IsecT Ltd, "Information security compliance," *Inf. Secur. Aware. Serv.*, no. March, pp. 1–10, 2011.
[68] D. Dasgupta and M. Rahman, "A Framework for Estimating Security Coverage for Cloud Service Insurance," *Proc. Cyber Secur.*, p. 1, 2011.
[69] I. Atoum and A. Otoom, "Holistic Performance Model for Cyber Security Implementation Frameworks," *Int. J. Secur. Its Appl.*, vol. 10, no. 3, pp. 111–120, 2016.
[70] I. Atoum and A. Otoom, "Effective Belief Network for Cyber Security Frameworks," *Int. J. Secur. Its Appl.*, vol. 10, no. 4, pp. 221–228, 2016.
[71] I. Atoum, "Requirements Elicitation Approach for Cyber Security Systems," *i-manager's J. Softw. Eng.*, vol. 10, no. 3, pp. 1–5, 2016.

