Surveying the Incorporation of IoT Devices into Cybersecurity Risk Management Frameworks

Aaron J. Pendleton
Graduate Cyber Operations
Air Force Institute of Technology
Dayton, United States
email: Aaron.Pendleton@afit.edu

Richard Dill
Assistant Professor
Dept of Electrical & Computer Engineering
Air Force Institute of Technology
Dayton, United States
email: Richard.Dill@afit.edu

Dillon Pettit
Graduate Cyber Operations
Air Force Institute of Technology
Dayton, United States
email: Dillon.Pettit@afit.edu

***Abstract*—This paper reviews the state of the art for incorporating Mobile Devices, Industrial Control Systems, and Internet of Things systems into present risk analysis framework models. Internet of Things devices present unique risks to a network due to their highly connective and physically interactive nature. This physical influence can be leveraged to access peripherals beyond the immediate scope of the network, or to gain unauthorized access to systems which would not otherwise be accessible. A 2017 Government Accountability Office report on the current state of Internet of Things device security noted a lack of dedicated policy and guidance within the United States government cybersecurity risk assessment construct and similar private sector equivalents. Surveyed in this paper are 28 original frameworks designed to be implemented in enterprise networks. In this research the comparison of frameworks is analyzed to assess each system's ability to provide risk analysis for Internet of Things devices. The research categories are level of implementation, quantitative or qualitative scoring matrix, and support for future development. This survey demonstrates there are few risk management frameworks currently available which attempt to incorporate both cyber-physical systems and enterprise architecture in a large scale network.**

Keywords*— *IoT; RMF; cybersecurity; risk; ICS.

I. Introduction

Industrial Control Systems (ICS) and Internet of Things (IoT) devices have infiltrated most networks that would traditionally be classified as enterprise networks. Their unprecedented rise in popularity has made it challenging for companies to assess and mitigate the additional risk.

IoT devices present unique risks to a network due to their highly connective and often cyber-physical nature. This physical influence can be leveraged to gain unauthorized access to systems which would not otherwise be accessible.

The United States (U.S.) Government Accountability Office (GAO), an independent and nonpartisan U.S. Congressional watchdog organization, provides objective and reliable information to the government regarding work and spending practices. GAO focuses on identifying problems and proposes solutions [32]. In July 2017, GAO released a report titled *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD* in order to highlight shortcomings in most current operational risk assessment frameworks to include those implemented by the U.S. Department of Defense (DOD). The report includes security concerns with Mobile Devices, Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLC), and Remote Terminal Units (RTU) in the U.S. DOD [32].

GAO noted a lack of dedicated policy and guidance within the U.S. government cybersecurity risk assessment construct and similar private sector equivalents. In the report, GAO defines IoT devices as any personal wearable fitness device, portable electronic device, smartphone, or infrastructure device related to industrial control systems [32].

Present DOD Instructional Guidance does not address IoT devices sufficiently [32]. Furthermore, no single DOD entity is responsible for the security of IoT systems, and the primary guidance on IoT security is the strategic directive to establish an operations security program. This paper furthers the research done by GAO in order to expand the scope of analysis beyond the U.S. DOD and into the greater field of published cyber risk solutions.

A risk analysis methodology must account for more than just traditional enterprise network components in order to mitigate the risks presented by an unregulated or loosely defined set of devices on an otherwise secure network. The purpose of this survey is to analyze the pace of development and compare the strengths and weaknesses of each analyzed framework with regard to IoT and ICS devices. 27 original cyber risk assessment and management models will be compared based on their method of risk scoring, level of implementation, and future development plans. These metrics will be used to gauge the effectiveness of a framework when accounting for devices which may not be consistently part of the secure baseline, or may not be commonly patched and secured. The ability of a risk analysis model to incorporate these common, but otherwise difficult to attribute systems will be compared in order to determine the state of the art. Frameworks published from as early as 2002 were identified and assessed for their ability to adapt to IoT devices. This paper analyzes the extent that network risk analysis and management frameworks have adapted to this evolving threat terrain. Section II outlines the risk framework models and their attributes, Section III presents the methods used to analyze and evaluate the frameworks in order to make appropriate comparisons, and Section IV provides an assessment of the current state of the art in order to then make recommendations for future research. We conclude

 ISBN: 978-1-61208-746-7

this work in Section V.

II. Related Work

A. Risk Management Framework (RMF)

The primary risk assessment and management framework used by the U.S. Military and DOD to conduct mission assurance is the cybersecurity Risk Management Framework (RMF) developed by the National Institute of Standards and Technology (NIST). NIST RMF is a 6 step qualitative analysis method for assessing risk. It establishes a secure baseline through identifying controls that are to be updated as changes are detected [1]. Common NIST RMF implementation policy requires end users to disable the impertinent network components of most IoT devices, but this can encourage subversion of the RMF process for personal and government devices by dis-associating some capabilities from the network and the secure baseline. This presents heightened risk levels that are left unaccounted for in the overall assessment [32]. Qualitative frameworks such as RMF rely on scanning tools and strict Information Assurance (IA) policy to prevent unauthorized activity. These security measures can be subverted by IoT devices because they often have limited up-time, minimal support, a notable lack of associated scanning tools, and a smaller footprint for vulnerability testing [32]. Note: The NIST Cybersecurity Framework (CSF) and RMF are different, and CSF is directed at a higher level of protection specific to Critical Infrastructure (CI) not analyzed in this paper.

B. Control Objectives for Information and related Technology (COBIT) 5

COBIT 5 is the latest COBIT version analyzed. It was developed by the Information Systems Audit and Control Association (ISACA) and is a qualitative framework designed to provide top-down security of a business sized network. It relies on control objectives to build out the security requirements, and the level of security is assessed by maturity models. COBIT follows a purpose built model which is intended to allow for only necessary systems to be on the network in order to minimize risk [2] [34] . COBIT 2019 has been announced and is expected to address IoT more directly [22].

C. ISO27K Series

Published the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the ISO/IEC 27000 series is a large framework of best practices. It provides a security control based qualitative framework with significant modularity for varying levels of implementation similar to the NIST RMF and COBIT. The strength of this model is its inherent ability to scale to the needs of the network, but allows for weaknesses where the framework is not fully implemented. It is currently in extensive use [3] [19].

D. Information Security Maturity Model (ISMM) (2011)

The ISMM model was created by analyzing eight existing models: NIST, Information Security Management Maturity Model (ISM3), Generic Security Maturity Model (GSMM), Gartner's Information Security Awarness Maturity Model (GISMM), SUNY's Information Security Initiatives (ISI), IBM Security Framework, Citigroup's Information Security Evaluation Maturity Model (ISEM), and Information Security Management System (ISMS) Maturity Capability Model. ISMM assesses the security requirements of an organization and then assigns a maturity level that will provide the correct balance of security and accessibility. They propose a method of quantifying risk at a very abstracted level, but the model itself is primarily a qualitative system to initiate compulsory levels of security [21].

E. Information Security Maturity Model (ISMM) (2017)

This ISMM model was also created following a comparison of several current implementations of risk modeling frameworks to include NIST RMF, COBIT, and ISO 27001. ISMM attempts to directly map each capability provided by current models to determine the most mature framework. The findings discovered weaknesses in all frameworks, and a single composite framework was introduced as a solution which provides all capabilities of currently implementations in one system. The framework is still at a theoretical stage of implementation, but has the potential to create a more complete qualitative solution [1].

F. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

1) OCTAVE (original): OCTAVE is a self directed risk management solution for large enterprises. It relies on the network staff's knowledge of critical systems and components to create a secure baseline. The weakness of this system is it is outdated (2003) and reliant on having an expert team with significant resources. There have not been significant updates to OCTAVE following the release of OCTAVE-Allegro and it could now be considered a legacy framework [4].

2) OCTAVE-S: OCTAVE-S is designed as a smaller scale implementation of OCTAVE, but suffers from several similar pitfalls. A manually created baseline that is updated as changes are observed cannot be easily adapted. OCTAVE-S provides additional structure for a less experienced team, but at the expense of significant system constraints as the implementation matures [4].

3) OCTAVE-Allegro: Allegro attempts to make risk management system more approachable than the original models. The complexity level of OCTAVE Allegro is lowered and the system is shifted to a more information-centric container based approach. Allegro is one of the first qualitative systems to incorporate an abstracted level of quantitative analysis using the containers as network elements. Due to the still largely

 ISBN: 978-1-61208-746-7

qualitative nature of Allegro, it can have issues with implementation consistency. This can be especially challenging when accounting for IoT devices [10].

G. Holistic Cyber Security Implementation Framework (HCS-IF)

Atoum introduces HCS-IF in an attempt to create a more complete approach to risk management that avoids the fragmented stovepipe nature that developed over several iterations of abstracted quantification in many risk management frameworks. The HCS-IF has not yet been tested, but has potential value to be assessed in future studies [6].

H. IoT/M2M

Cisco introduces the IoT/M2M framework in order to address the rising challenge of securing networks saturated with relatively insecure IoT devices. The downside to this otherwise very effective model is the cost and difficulty in building a network from essentially the ground up as opposed to introducing new security measures to an existing network. It is a qualitative zero trust approach to security that attempts to limit the access of IoT devices in order to prevent them from being leveraged to influence otherwise secure devices. Live network evaluation has not yet been published [14].

I. Mobius

Mobius creates a quantifiable model which allows for risk calculations to be made using custom designed profiles for each device. The weakness is in the scaling and implementation relative to more modern tools. It requires extensive expertise to properly employ, and additional development to account for IoT devices [12].

J. Online Services Security Framework (OSSF)

The OSSF framework is designed to manage risk in an enterprise network offering online services. It provides the structure to create a secure baseline for both the provider and the consumer, but inherently must be configured by the end user. It accounts for broadly connected devices like IoT well, but it is limited in its application until it can be expanded to more diverse networks [24].

K. The CORAS Method

The CORAS approach is an 8 step model-based solution which allows a great deal of flexibility in implementation. A risk evaluation matrix is populated using CORAS that provides both high and low level analysis, but at the cost of significant labor as the baseline is constantly redefined when IoT devices are introduced [23].

L. Threat Agent Risk Assessment (TARA) (2009)

TARA was created by Intel and uses a calculation matrix to predict which agents pose the highest risk to the network. The output is then cross-referenced with known vulnerabilities and controls to mitigate risk. A meaningful published application of the TARA system has not been identified during this survey [26].

M. Threat Assessment & Remediation Analysis (TARA)(2011)

The MITRE Corporation created the TARA system to secure specific networks known to be of interest to potential actors. TARA uses a scoring model to identify probability of attack and potential attack vectors. It is difficult to scale, but can provide very sophisticated assessments if the cybersecurity budget is sufficiently large [35].

N. CCTA Risk Analysis and Management Method (CRAMM)

CRAMM is a framework designed by the United Kingdom (UK) Central Computer and Telecommunications Agency (CCTA). It is a relatively outdated method of providing qualitative analysis across multiple asset groups and requires them to be built out on a per-network basis. This makes the modular construction useful, but at the cost of significant overhead to implement. It has been implemented in many countries, but has not been updated since CRAMM 5 in 2003 [36].

O. Cyber Assessment Framework (CAF) 2.0

Created by the UK National Cyber Security Centre (NCSC), the CAF is a model based risk assessment system similar to NIST RMF which provides extensibility across many devices and network types including SCADA [33]. The framework is very new without published academic assessment, but has been adopted at an international level with a particular focus on SCADA and business IT systems [31].

P. Cyber Risk Scoring and Mitigation (CRISM)

CRISM uses Bayesian graphs to build an end-to-end automated capability which can provide security scores and prioritized mitigation plans. A high level of automation is achieved which makes implementation much simpler for small teams. Additional testing and development has the potential to create a powerful tool [29].

Q. Network Security Risk Model (NSRM)

NSRM relies on establishing a secure baseline and comparing risk levels after the introduction of each new device. This method is relatively outdated and labor intensive, but can provide good results if it is effectively implemented. It is targeted at Process Control Networks (PCN) which have less variance, and is not suitable for a large enterprise network [18].

R. Cyber Physical Systems Security (CPSS)

DiMase identified the need for a Cyber-Physical System (CPS) centric risk framework to account for the rise in CPS devices across enterprise networks. It relies on a heuristics based approach rather than a secure baseline to provide an initial level of security, and over time creates an operational baseline. Extensive future development is required before fielding on a large network [13].

 ISBN: 978-1-61208-746-7

S. Harmonized Threat & Risk Assessment (HTRA)

Published by the Canadian Government, HTRA provides a risk management framework which expounds rapid adjustments to account for quickly evolving threat terrain, but still implements a traditional secure baseline structure. HTRA suffers from the same pitfalls of most large frameworks in that the size of the network often determines how effectively the model is implemented [17].

T. System-Fault Risk (SFR)

The qualitative framework created by Ye accounts for several layers of interconnection by creating multiple attack origin classification models. It is modular and capable of extension into nearly any device that operates on a network, but at extreme cost. It is not primarily intended to be used as a full enterprise solution [37].

U. Hierarchical Model Based Risk Assessment

Baiardi introduces a framework based on security dependency hypergraphs which have the capability to identify attack paths which an analyst may miss in a qualitative assessment. Tools for basic implementation were developed but not widely tested in a live network [7].

V. Patel & Ziveri Model

The model is a quantitative system which depends on predetermined types of attacks and devices. Additional research would be required in order to account for anything outside of the current scope of the model. It is presently designed for implementation in SCADA networks, and does not account well for IoT or any attack that is not within the matrix [25].

W. IBM Security Framework

The IBM security blueprint stovepipes security into domains which are broken down further into distinct objectives and services. Each sub-domain is then to be implemented according to industry best practices [8]. An update in 2014 showed successful results in several live networks [9].

X. Information Security Risk Analysis Method (ISRAM)

ISRAM is an attempt to bridge the gap between the overwhelming challenge of implementing a quantitative model on a complex network and the inconsistencies of a qualitative model. While sound in theory, the product still suffers from the extensibility issues faces by quantitative models [20].

Y. Amin Cyber-Physical Security (CPS) Model

Amin attempts to create a quantitative framework to address the risks presented by cyber-phsyical systems on a network, but struggles to account for all components simultaneously in a large composite model [5].

Z. Cybernomics

Cybernomics is an attempt to incorporate cyber risk management and economic modeling to build a quantifiable framework which can be scaled to a larger enterprise network. It provides a more network centric portfolio, and in turn may be capable of providing sound IoT accountability. Live network testing is anticipated in a future publication [28].

III. Methodology

Four primary elements common to each framework are evaluated. This establishes a basic standard used to make comparisons, and highlights several key differences between otherwise similar methods. These attributes are mapped and graded to determine the level of efficacy provided. It is challenging to conduct a full pairwise comparison between any two models due to their inability to target IoT devices at all. Nearly all models surveyed neglected to take special measures towards securing IoT devices versus other enterprise components. This led to a largely qualitative analysis of the merits of each model, with models that have a particularly outstanding system being highlighted in Section IV.

A. Quantitative vs. Qualitative

Each framework surveyed was classified as either primarily qualitative, or quantitative. The constraints of the quantitative model are similar to the strengths of a qualitative model, and vice versa. Quantitative models often provide unparalleled modeling at the expense of scalability. In order to classify a framework as quantitative, it needed to exhibit device based calculations. Any framework which used only abstractions for a quantitative analysis was relegated to the qualitative category.

B. Level of Implementation

Models are assigned an implementation score of high, low, or N/A in order to account for the broad range of real-world testing frameworks have received. A framework with hundreds of implementations and years of feedback will have more data points to evaluate than a network which is conceptual or in its first live network test. Many surveyed frameworks that are recently published have not yet been employed in a significant capacity on a live network.

C. Age and Support Level

Risk assessment frameworks which no longer have a robust implementation or supporting entity may no longer be viable. It is important to consider that legacy models may no longer provide adequate security.

D. Overall Rating

The current standard for a risk assessment framework is a qualitative model which relies on robust security policy and patching processes alongside vulnerability scanning and security controls. These methods are suitable for securing a traditional enterprise network, but fall short when IoT devices are introduced. Any framework that meets, but does not have the potential to exceed this baseline is rated “Yellow”. Yellow

 ISBN: 978-1-61208-746-7

rated models are relatively good assessments of cyber risk, but do not manage IoT devices well. Any framework which is unable to achieve the same level of network protection as the current generation of frameworks are rated "Red". Models which have made a meaningful step towards properly accounting for IoT devices within enterprise networks will be rated "Green". The rating of green does not mean that they have fully accounted for IoT devices, but that it is an advancement over most currently implemented models.

IV. Analysis of Risk Assessment Frameworks

TABLE 1. RISK FRAMEWORK COMPARISON

Reviewed Framework	Framework Analysis		
	Rating	*Implementation*	*Year*
*Amin CPS Model [5]	Red	N/A	2013
†CAF [33]	Yellow	High	2018
†COBIT 5 [3] [34]	Yellow	High	2012
†CORAS [30]	Red	Low	2003
†CPSS [13]	Red	N/A	2015
*CRAMM [36]	Red	Low	2003
*CRISM [29]	Green	N/A	2018
*Cybernomics [28]	Green	N/A	2017
†HCS-IF [6]	Green	N/A	2014
†*Hierarchical Model [7]	Red	N/A	2009
†HTRA [17]	Yellow	High	2007
†IBM Framework [8]	Yellow	Low	2010
†IoT/M2M [14]	Green	N/A	2016
†ISO27K [3] [19]	Yellow	High	2005
*ISRAM [20]	Red	N/A	2005
†ISSM [1]	Green	N/A	2017
†ISSM [21]	Yellow	Low	2011
*Mobius [12]	Red	N/A	2002
†NIST [27]	Yellow	High	2015
*NSRM [18]	Red	N/A	2009
†OCTAVE [4]	Red	Low	2003
†OCTAVE-S [4]	Red	Low	2003
†OCTAVE-Allegro [10]	Red	Low	2007
†OSSF [24]	Green	N/A	2017
*Patel & Ziveri Model [25]	Red	N/A	2010
†SFR [37]	Red	N/A	2005
†*TARA (Intel) [26]	Yellow	Low	2009
†*TARA (MITRE) [35]	Yellow	Low	2011

†Indicates Qualitative *Indicates Quantitative

A. Common Framework Pitfalls

No surveyed model rated "green" for IoT advancement has been implemented in a live network. Similarly, all models rated "high" for implementation scored "yellow" in IoT advancement. This overwhelmingly indicates that the state of the art has not yet accounted for IoT properly, and no single framework can be recommended as an immediate solution to the IoT problem. The current model of a qualitative risk assessment may no longer be viable as IoT devices continue to become more critically integrated into networks. Each qualitative model surveyed attempts to use only existing resources to secure the IoT threat vector. In order to continue using existing risk models, it is necessary to either invest in new architecture to account for the largely unknown vulnerabilities presented by current off the shelf IoT systems, or incorporate only IoT systems which have been subjected to a much higher degree of security analysis. The current model of minimal support and small device marketshare footprint is unlikely to result in a solution to the IoT problem.

B. IoT Advancements

It is imperative that security development be proactive due to the increasingly vital role that IoT devices have in enterprise networks. Among the most promising proposed models is the zero trust approach in the IoT/M2M framework. Rather than attempt to impose enterprise security methods on IoT devices, it attempts to section them off as much as possible into other network segments. This is not a full solution, but it may prove more effective than current implementations. The frameworks that have the ability to accurately model risks to ICS and IoT systems primarily have implemented a quantitative risk assessment approach, but no solution has been able to provide cost-effective coverage to a larger network. The primary weakness to this solution is some devices will eventually have to have a trusted relationship, and this will lead to inevitable vulnerabilities. This method is at best a technique to shrink the attack surface of a network, and does not fully mitigate the risk of IoT devices.

C. Proposed Solutions

Two courses of action for securing IoT devices based on the analysis of the 28 frameworks surveyed are:

1) Short Term: Use network segmentation and a zero trust model: IoT devices cannot be considered trusted or secure by a risk analysis model until a more robust vulnerability assessment process can be developed. Designing network architecture to create the smallest foothold possible for compromised IoT devices may be an effective short term solution. Potential examples of this would be creating an IoT device Virtual Local Area Network (VLAN), De-Militarized Zone (DMZ), or using bastions as IoT interface servers. Similarly, isolating IoT devices from domain credentials and trust settings is also vital to ensuring that a vulnerable IoT device does minimized damage if exploited.

2) Long Term: Increase viability of quantifiable risk assessment frameworks with Machine Learning: Quantitative frameworks have demonstrated the highest level of potential risk analysis, but are not capable of modeling large networks in their present state. The next iteration of quantitative framework must solve this problem in order for them to become viable. This could be accomplished by using machine learning to implement their risk algorithm, and to develop the individual device profiles. This direction would require substantial resources to establish, but potentially yield lower operating costs. The threat profile and logical/physical location of a device would be inputted, and the risk profile of the network could be automatically adjusted to compensate for the addition. This system would also allow for very accurate projections of security level in proposed architecture developments, as well as software migrations and patching.

V. Conclusion and Future Work

The breakdown of findings shows significant shortcomings in all state of the art risk assessment frameworks. No de-

velopmental model was identified that could be considered deployment ready with capabilities clearly exceeding those of the current generation of qualitative system. Several proposed frameworks with the ability to incorporate both cyber-physical systems and enterprise architecture in a large scale network were reviewed, but none have been tested in a live environment. At this time, there is still a significant need for research on methods to incorporate IoT devices into enterprise networks without losing either accessibility or security. The scale and diversity of IoT has been insurmountable for qualitative models, but future research developing Proposed Solution 1). may yield significant advancements. A significant change in funding or ease of implementation will be necessary in order to drastically alter the current risk assessment terrain away from qualitative models. Minimal published research on the application of machine learning to cyber risk assessment was identified, but this avenue of research outlined in Proposed Solution 2). is one of the primary methods of making the quantitative model viable again.

ACKNOWLEDGMENT

Disclaimer: The views expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

REFERENCES

[1] S. Almuhammadi and M. Alsaleh, "Information Security Maturity Model for NIST Cyber Security Framework." Computer Science & Information Technology 51 2017.

[2] M. Ahlmeyer and A. M. Chircu, "Securing the Internet of Things: A review." Issues in Information Systems, vol. 17, no. 4, 2016.

[3] W. Al-Ahmad and B. Mohammad, "Can a Single Security Framework Address Information Security Risks Adequately." International Journal of Digital Information and Wireless Communications, vol. 2, no. 3, pp. 222-230, 2012.

[4] C. Alberts, A. Dorofee, and J. Stevens, "Introduction to the OCTAVE Approach." Carnegie-Mellon Univ. Software Engineering Inst, 2003.

[5] S. Amin, G. A. Schwartz, and A. Hussain, "In Quest of Benchmarking Security Risks to Cyber-Physical Systems." IEEE Network, vol. 27, no. 1, pp. 19-24, 2013.

[6] I. Atoum, A. Otoom, and A. A. Ali, "A Holistic Cyber Security Implementation framework." Information Management & Computer Security, vol. 22, no. 3, pp. 251-264, 2014.

[7] F. Baiardi, C. Telmon, and D. Sgandurra, Hierarchical, Model-Based Risk Management of Critical Infrastructures, Reliability Engineering & System Safety, vol. 94, no. 9, pp. 1403-1415, 2009.

[8] A. Buecker, M. Borrett, C. Lorenz, and C. Powers, "Introducing the IBM security Framework and IBM Security Blueprint to Realize Business-Driven Security." IBM Redpaper 4528, no. 1, pp. 1-96, 2010.

[9] A. Buecker, S. Arunkumar, B. Blackshaw, M. Borrett, P. Brittenham, J. Flegr, and J. Jacobs, "Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security." IBM Redbooks, 2014.

[10] R. Caralli, J. Stevens, L. Young, and W. R. Wilson, "Introducing Octave Allegro: Improving the Information Security Risk Assessment Process. No. CMU/SEI-2007-TR-012. Carnegie-Mellon Univ. Pittsburgh PA Software Engineering Inst, 2007.

[11] J. Cebula and L. R. Young, "A Taxonomy of Operational Cyber Security Risks." Carnegie-Mellon Univ. Pittsburgh PA Software Engineering Inst, No. CMU/SEI-2010-TN-028, 2010.

[12] D. D. Deavours, G. Clark, T. Courtney, and D. Daly, "The Mobius framework and its Implementation." IEEE Transactions on Software Engineering, vol. 28, no. 10, pp. 956-969, 2002.

[13] D. DiMase, Z. A. Collier, K. Heffner, and I. Linkov, "Systems Engineering Framework for Cyber Physical Security and Resilience." Environment Systems and Decisions, vol. 35, no. 2, pp. 291-300, 2015.

[14] J. Frahim, "Cisco: Securing the Internet of Things: A Proposed Framework." 2016.

[15] C. Fruhwirth and T. Mannisto. "Improving CVSS-Based Vulnerability Prioritization and Response with Context Information." Proceedings of the 2009 3rd international Symposium on Empirical Software Engineering and Measurement, IEEE Computer Society, 2009.

[16] G. Giannopoulos, R. Filippini, and M. Schimmer, "Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A state of the art." JRC Technical Notes, 2012

[17] Government of Canada, "Harmonized Threat and Risk Assessment Methodology" Ottawa, 2007. Accessed Sep. 11, 2019

[18] M. H. Henry and Y. Y. Haimes. "A Comprehensive Network Security Risk Model for Process Control Networks." Risk Analysis: An International Journal, vol. 29, no. 2, pp. 223-248, 2009.

[19] T. Humphreys, "State-of-the-Art Information Security Management Systems with ISO/IEC 27001: 2005." ISO Management Systems, vol. 6, no. 1, 2006.

[20] B. Karabacak and I. Sogukpinar, "ISRAM: Information Security Risk Analysis Method." Computers & Security, vol. 24, no. 2, pp. 147-159, 2005.

[21] G. Karokola, S. Kowalski, and L. Yngstrm, "Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View." In HAISA, pp. 58-73, 2011.

[22] J. Lainhart, "Introducing COBIT 2019: The Motivation for the Update?" ISACA Webinar Blog Post, 2018. Accessed Sep. 9, 2019.

[23] M. S. Lund, B. Solhaug, and K. Stlen. "A Guided Tour of the CORAS Method. In Model-Driven Risk Analysis" Springer, Berlin, pp. 23-43, 2011.

[24] J. Meszaros and A. Buchalcevova. "Introducing OSSF: A Framework for Online Service Cybersecurity Risk Management." Computers & Security, vol. 65, pp. 300-313, 2017.

[25] S. Patel and J. Zaveri. "A Risk-Assessment Model for Cyber Attacks on Information Systems." Journal of Computers, vol. 5, no. 3, pp. 352-359, 2010.

[26] M. Rosenquist, Prioritizing Information Security Risks with Threat Agent Risk Assessment Intel, 2009.

[27] R. Ross, "Guide for Applying the Risk Management Framework to Federal Information Systems" NIST, SP 800-37, Revision 1, 2010.

[28] K. Ruan, "Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk." Computers & Security, vol. 65, pp. 77-89, 2017.

[29] S. Shetty, M. McShane, L. Zhang, and J.P. Kesan, "Reducing Informational Disadvantages to Improve Cyber Risk Management." The Geneva Papers on Risk and Insurance-Issues and Practice, vol. 43, no. 2, pp. 224-238, 2018.

[30] K. Stolen, F. den Braber, T. Dimitrakos, and R. Fredriksen, "Model-Based Risk Assessment: The CORAS Approach." iTrust Workshop, 2002.

[31] T. Kevin. "Introducing the Cyber Assessment Framework v2.0" NSCS Blog Post, 2018. Accessed Sep. 9, 2019.

[32] U.S. Government Accountability Office INTERNET OF THINGS: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD Publication No. GAO-17-668, 2017.

[33] U.K. National Cyber Security Centre "Cyber Assessment Framework" Accessed sep. 9, 2019.

[34] K. V. Wal, J. Lainhart, and P. Tessin, "A COBIT 5 overview." ISACA Webinar Program, 2012.

[35] J. Wynn, J. Whitmore, G. Upton, L. Spriggs, and D. McKinnon, "Threat assessment & Remediation Analysis (TARA): Methodology" MITRE CORP BEDFORD MA, ver. 1.0, No. MTR110176, 2011.

[36] Z. Yazar, "A Qualitative Risk Analysis & Management Tool: CRAMM." SANS InfoSec Reading Room, White Paper 11, 2002.

[37] N. Ye, C. Newman, and T. Farley. "A System-Fault-Risk Framework for Cyber Attack Classification." Information Knowledge Systems Management, vol. 5, no. 2, pp. 135-151, 2005.

 ISBN: 978-1-61208-746-7