Surveying the Incorporation of IoT, SCADA, and Mobile Devices into Cybersecurity Risk Management Frameworks

Aaron Pendleton
Graduate Cyberspace Operations
Air Force Institute of Technology
Wright-Patterson AFB, Ohio 45433
Email: Aaron.Pendleton@afit.edu

Richard Dill
Dept. of Electrical and
Computer Engineering
Air Force Institute of Technology
Wright-Patterson AFB, Ohio 45433
Email: Richard.Dill@afit.edu

James Okolica
Dept. of Electrical and
Computer Engineering
Air Force Institute of Technology
Wright-Patterson AFB, Ohio 45433
Email: James.Okolica@afit.edu

Dillon Pettit
Graduate Cyberspace Operations
Air Force Institute of Technology
Wright-Patterson AFB, Ohio 45433
Email: Dillon.Pettit@afit.edu

Marvin Newlin
Graduate Cyberspace Operations
Air Force Institute of Technology
Wright-Patterson AFB, Ohio 45433
Email: Marvin.Newlin@afit.edu

***Abstract*—This paper reviews the state of the art in cyber risk management with a focus on the adaptations in methodology to account for 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. The purpose of this paper is to expand that work and assess additional risk models. Surveyed in this paper are 30 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 that 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; Mobile; Cybersecurity; Risk; ICS.

I. Introduction

This paper is a continuation of the work "Surveying the Incorporation of IoT Devices into Cybersecurity Risk Management Frameworks" presented in the 2019 SECURWARE proceedings [1]. The paper assesses the extent that risk management frameworks have adapted to Industrial Control Systems (ICS) and Internet of Things (IoT) devices which have infiltrated most networks that would traditionally be classified as enterprise networks. The transient or multi-connected nature of IoT devices poses a challenge to security methods based on creating a secure baseline. The unprecedented rise in popularity of mobile and interconnected IoT devices has made it challenging for companies to assess and mitigate the additional risk presented by incorporating them into networks implementing risk management frameworks. Frameworks from specific industries such as online services, critical infrastructure, research and design, and enterprise risk management have been evaluated an effort to fully assess the state of the art across the security and risk industry.

IoT devices present unique risks to a network due to their highly connective and often cyber-physical nature. Enterprise networks that are not equipped with methods of assessing vulnerabilities across less traditional interfaces or protocols such as Bluetooth or remote location devices with unsecured external connections are exposed to unaccounted risks. This physical influence can be leveraged to gain unauthorized access to systems which would not otherwise be accessible [2]. Similarly, they have been shown to exhibit several widespread security challenges that require special consideration. Many IoT devices are difficult to patch, do not have consistent software updates, or lack strong encryption. This creates vulnerabilities in networks that require authentication, access control, or data privacy [3]. It is also difficult to identify IoT devices that already exist on a network due to many autonomous and passive applications [3].

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 [2]. 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 [2].

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 [2].

Present DOD Instructional Guidance does not address IoT devices sufficiently [2]. Furthermore, no single DOD entity is responsible for the security of IoT systems, and the primary guidance on IoT security is a 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 [2]. 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. The extent of advancements in risk management is assessed in order to highlight current knowledge and research gaps. 30 original risk assessment and management models are compared based on their method of risk scoring, level of implementation, and future development plans. These metrics are 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 easily patched and secured. The ability of a risk analysis model to incorporate these common, but otherwise difficult to attribute systems is compared in order to establish the state of the art in currently employed systems. These methodologies are compared to recently proposed frameworks to assess the current gap in risk management. 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 accurate 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 this work in Section V with recommendations for future work.

II. Related Work

This section reviews elements of 30 risk frameworks and provides background information used in the analysis and assessment. Specific methodology is discussed in order to establish the basic elements of each model and to ascertain the level of effectiveness observed.

A. National Institute of Standards and Technology (NIST)

The United States uses a centralized risk framework system based on application. NIST is tasked with creating and maintaining effective cyber risk modeling and management frameworks implemented on millions of government and civilian devices [4].

1) Risk Management Framework (RMF): The primary risk assessment and management framework used by the U.S. government, military and DOD to conduct mission assurance is the cybersecurity Risk Management Framework (RMF) developed by NIST. The NIST RMF process shown in Figure 1 is a six step qualitative analysis method for assessing risk. RMF uses a strict adherence to process management to establish a secure baseline through identifying controls that are to be updated as changes are detected [5]. The strength of the RMF process is that it allows for a network to grow and evolve without a complete re-evaluation of its security posture. Best practices are evaluated and selected as security controls and solutions when new devices are added to the existing baseline. The weakness in this method is it sacrifices micro-level visibility of device interactions in favor of broad security measures. NIST RMF implementation policy requires end users to disable the impertinent network components of IoT devices, but not physical removal. This leaves the opportunity for subversion of the RMF process in personal and government devices by dis-associating some capabilities from the network and the secure baseline without fully mitigating the threat. IoT and mobile devices present heightened risk levels that are left unaccounted for in the overall assessment [2]. 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 [2].

2) Cybersecurity Framework (CSF): The CSF is designed to provide a higher level of protection specific to the unusual or irregular systems common in Critical Infrastructure (CI). CSF is considered one of the premiere risk management models for CI, and provides a five step, tiered, qualitative approach to modeling risk to networks both small and large. The CSF framework is a guide for security measures to be implemented and allows classification of the current security posture in order to highlight pressing weaknesses. Many academic institutions, government and DOD entities, and private companies have implemented CSF. CSF continues to struggle with the same weaknesses identified in RMF despite offering significant improvements over previous generations of risk framework [7].

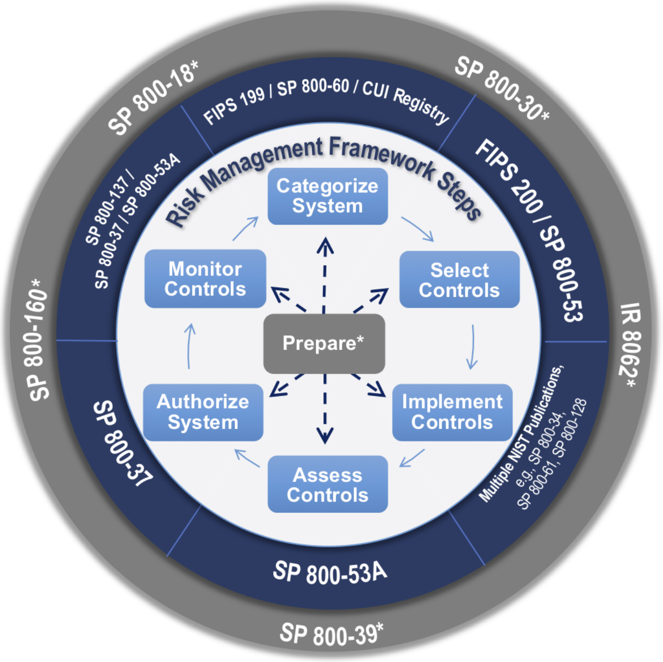

Fig. 1. Risk Management Framework Process and Governance [6]

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 [8][9]. COBIT 5 incorporated elements of the NIST CSF structure, but did not greatly mitigate the weaknesses of CSF when IoT devices are introduced to the network environment without adequate vulnerability scanning and assessment methods [7]. Initial information and methodology publications introducing COBIT 2019 have been released, but the framework implementation is not mature enough to analyze at this time [10]. Figure 2 introduces the process of implementing COBIT 2019. COBIT follows a process-based approach similar to other qualitative methods such as NIST RMF. A comparison of Figure 1 and Figure 2 shows the extent of the similarities between qualitative process-based risk management methodologies. The primary focus of the process is to identify the problem by outlining each device and defining its potential interactions with the previously established secure baseline. Security risks are then mitigated and monitored. This general approach is observed in each leading enterprise solution assessed in this survey.

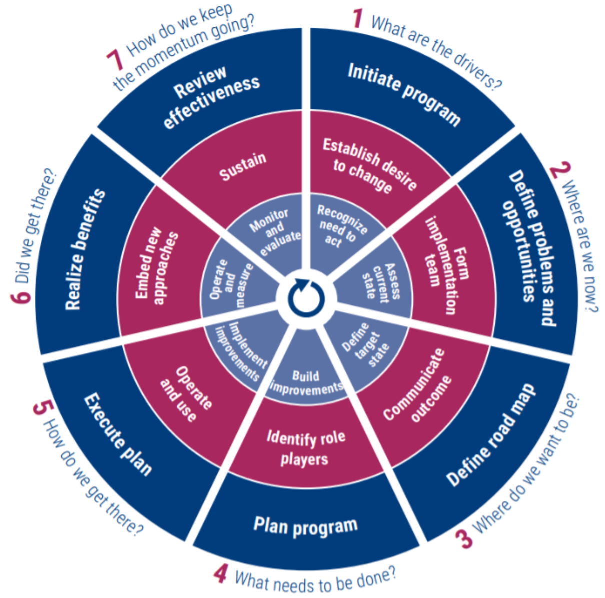

Fig. 2. COBIT 2019 Process Overview [11]

C. ISO Risk Management Frameworks

The International Organization for Standardization (ISO) is an independent and international organization dedicated to developing international standards. The standards created by ISO are not inherently designed for cybersecurity applications, but they are tools for assessing risk across multiple domains.

1) ISO31K Series: The ISO 31000 standard is a general risk standard mandated in some information technology applications built off of the Australian/New Zealand risk management standard AS/NZS 4360. It identifies specific language to be used when classifying risk, but is not a strong methodology for addressing it. It is not based on quantifiable probabilities or decision points, but a qualitative assessment conducted at key points in the risk management cycle. It is important to note that the standard is specifically not intended for purposes of certification. ISO 31000 alone cannot be considered sufficient for a risk assessment framework within an enterprise network, but frameworks have been designed to provide compliance with this standard [12] [13].

2) ISO27K Series: The ISO/IEC 27000 series is a large framework of best practices published by the ISO and the International Electrotechnical Commission (IEC). 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. Implementation is conducted through a six step qualitative process that assesses the current state of the network. Governance of the network is through the assignment of controls using a methodology similar to the NIST RMF. ISO 27K is a contemporary of the NIST RMF, COBIT 5, and other qualitative networks which are the operational state of the art. It is currently in extensive use across the European Union [14] [15] [5].

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 [16].

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 currentimplementations in one system. The framework is still at a theoretical stage of implementation, but has the potential to create a more complete qualitative solution [5].

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

1) OCTAVE (original): OCTAVE is a self directed risk management solution for large enterprises. It makes assumptions regarding 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 relies 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 [17].

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 [17].

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 qualitative nature of Allegro, it can have issues with implementation consistency. This can be especially challenging when accounting for IoT devices [18].

G. Holistic Cyber Security Implementation Framework (HCS-IF) (2014)

Atoum [19] 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 of the current state of the art. Frameworks that have used metrics of qualitative adherence to create a security score give some users the perceived confidence of a quantitative system without the overhead of a fully mapped risk framework. HCS-IF identifies core issues with bringing quantitative risk modeling back to cyber risk frameworks, but rather than create a fully quantitative methodology it attempts to advance the state of the art in qualitative models. The potential value added by their research must assessed in future studies before making any significant assertions of overall effectiveness [19].

1) HCS-IF Implementation Case Study (2017): The National Information Assurance and Cyber Security Strategy (NI-ACSS) of Jordan analyzed the HCS-IF in 2017 to determine if it could be applied at a national level. An implementation of HCS-IF is anticipated within the next three years following an evaluation by the Jordanian National Information Technology Center (NITC). Primary areas of improvement identified prior to adoption included change management and human resource issues [20].

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 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. IoT/M2M employs 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 been published. The proprietary nature of this framework significantly hinders any further testing in a research environment [21]. IoT/M2M builds a compelling argument for the success of the theoretical model and it may serve as the basis for future IoT security research.

I. Mobius

Mobius is a legacy framework included as an example of quantitative systems. It creates a quantifiable model which allows for risk calculations to be made using custom designed profiles for each device. The weakness of this methodology the poor scaling and implementation relative to more modern tools. As enterprise networks have grown in both size and diversity it is not financially advantageous to manual create a threat model for each device. This requires extensive expertise to properly employ, and additional development to account for IoT devices [22].

J. Online Services Security Framework (OSSF)

The OSSF framework is designed to manage risk in an enterprise network offering online services and remote access. It provides a structure or guide to create a secure baseline for both the provider and the consumer, but inherently must be configured by the end user. It accounts for highly mobile IoT devices, but it is currently limited in its application until it can be expanded to more diverse networks [23].

K. The CORAS Method

The CORAS approach is an 8 step model-based solution which allows a great deal of flexibility in implementation. It is built on the ISO 31000 standard for risk management as a self contained risk management solution for information technology systems. A risk evaluation matrix is populated using the CORAS tool that provides both high and low level analysis, but at the cost of significant labor as the baseline is constantly redefined when new assets are introduced. It uses a threat diagram to estimate risk based on past experience [24] [12].

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. TARA offers high levels of security, but the tradeoff is high operating costs. TARA attempts to bridge the gap between quantitative and qualitative systems, but the framework is not simplified enough to gain prominence [25].

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 threat actors during the system design and acquisition phase. 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. This method attempts to create stovepipes that can be tracked and modeled quantitatively. TARA is designed to be used primarily as an assessment tool to establish a risk baseline before a more sustainable qualitative tool is employed for the operational phase of the network life-cycle [26].

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 [27].

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 [28]. The intent is to provide support from NCSC to adoption of the European Union (EU) Network and Information System (NIS) directive. The framework is new, without published academic assessment, but it has been adopted at an international level with a particular focus on SCADA and business IT systems. CAF is implemented through the 14 principles of cybersecurity and resiliency identified by the NCSC. CAF provides an approachable methodology, but does not yet have the validated technical controls of more mature qualitative frameworks [29].

1) CAF 3.0 Release: The release of CAF 3.0 makes no changes to the structure or technical content of the CAF, but replaces specific NIS Directive terminology with simpler language better suited to users outside the direct purview of NIS [30].

P. Cyber Risk Scoring and Mitigation (CRISM)

CRISM was developed in 2018 as an effort to reintroduce quantifiable metrics into cyber risk assessment in order to mitigate the information advantage of the network owner in cyber insurance applications. The model uses Bayesian graphs to build an end-to-end automated capability which can provide security scores and prioritized mitigation plans. The primary goal is to identify the exploitable attack surface of the network, and then to assess the risks of lateral propagation. With this information, a risk mitigation plan can be created and implemented. CRISM relies on network scanning tools to analyze the attack surface, which can struggle to detect IoT devices. The likelihood of device exploitation is based on CVSS to access the Common Vulnerability Exposures (CVE) library. The weakness in this method is that a CVE entry must exist for the vulnerability [31]. CRISM leverages a high level of automation to make implementation much simpler for small teams, but live network testing has not been published. Additional testing and development is necessary before CRISM is deployed to an enterprise network [32].

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 [33].

R. Cyber-Physical Systems Security (CPSS)

DiMase [34] 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. The model does not yet employ a holistic approach, but it is anticipated in future research and development. Additional standardization is also necessary in order to allow the framework to function across multiple domains. The concept has not yet been tested on a live netowrk. Despite the need for extensive future development, the framework attempts to solve many current issues with cyber-physical system security [34].

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. HTRA follows the NIST model closely in an attempt to preserve scalability and consistency, but does not implement the rigorous controls used by RMF [35].

T. System-Fault Risk (SFR)

The qualitative framework created by Ye employs systems engineering, fault modeling, and risk assessment to classify cyber attacks. It accounts for several layers of interconnection by creating multiple attack origin classification models. The framework is modular and capable of extension into nearly any device that operates on a network, but at extreme cost. SFR takes the form of a checklist taxonomy which requires manual assessment and identification of devices in order to populate the risk matrices. It is not intended to be used as a full enterprise solution in its current form, but provides attack classification and characterization tools. Future research intends to provide further development toward a functional system [36].

U. Hierarchical Model Based Risk Assessment

Baiardi introduces a quantifiable framework based on security dependency hypergraphs which have the capability to identify attack paths which an analyst may miss in a qualitative assessment, but the model does not account for the inner state or operations of components. Risk is modeled and predicted within the graph. This allows for risk assessment and mitigation for each individual node or device. Tools for basic implementation were developed but not widely tested in a live network [37].

V. Patel & Ziveri Model

The model is a quantitative system which depends on predetermined types of attacks and devices to populate a risk matrix. This is accomplished by identifying the level of vulnerability each device has to each type of attack across several levels of effect. The model accounts for equipment loss, control loss, time loss, potential damage, and cost of prevention. A case study is performed in a small laboratory with several ICS 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 [38].

W. IBM Security Framework

The IBM security blueprint stovepipes security into domains which are broken down further into distinct objectives and services. The IBM model is specific to proprietary implementations of IBM hardware and products, but includes applications with devices from other vendors. Network sub-domains are defined by the framework in order to give the network managers sufficient segmentation for their environment. IBM relies heavily on operating according to industry best practices [39]. An update in 2014 showed successful results in several live networks [40].

1) Additional Publications (2016): IBM has published a series of books [41] to address practical application of the IBM security framework. They recognize the theoretical nature of the original publication [40] and introduce controls to assist in implementation of the framework. Each security domain is broken down into individual elements and appropriate security solutions are advocated. IoT devices are only accounted for through host and endpoint security measures and Access Control Lists (ACLs). The security model is simplistic, but operates at a level equivalent to current generation frameorks [41].

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. It operates by using one of the fundamental risk calculations, a function of probability and consequence. ISRAM relies heavily on surveys to populate risk tables. The case study was limited to a 20 device Local Area Network (LAN). The primary weakness of ISRAM is that it is blind to risk that is not identified through the surveys [42].

Y. Cyber-Physical Security (CPS) Model

Amin [43] employs elements of game theory to estimate security risks using technology based security defenses grounded in information security tools and fault tolerant controls in an attempt to create a more quantitative framework to address the risks presented by cyber-phsyical systems on a network. The methodology struggles to account for all components simultaneously in a large composite model, and lacks extensibility. Amin argues that the inter-dependencies of cyber-physical systems is not well documented, and the risks they pose to an established network are not assessed accurately due to the lack of research in cyber-physical system vulnerabilities [43].

Z. Cybernomics

Cybernomics is an attempt to incorporate cyber risk management and economic modeling to build a more quantifiable framework which can be scaled to a larger enterprise network using a formally proposed unit of cyber risk. It provides a more network centric portfolio, and in turn may be capable of providing sound IoT accountability. This framework is reliant on large scale adoption as a means to populate common threat indexes and create informed risk models. Live network testing is anticipated in a future publication [44].

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 specifically. Nearly all models surveyed neglected to take special measures towards securing IoT devices versus other enterprise components. Models which account for IoT/mobile/ICS often highlight that they are a security challenge, but do not have specific countermeasures in place to mitigate the threats they introduce. 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 can provide unparalleled threat modeling at the expense of scalability. Popular methods of quantitative modeling require manual analysis of each device to identify network interfaces and operating systems. For the purpose of this assessment a framework must demonstrate device specific risk or attack probability considerations to be classified as quantitative. Frameworks employing specific architecture requirements, implementation controls, and vulnerability assessments were categorized as primarily qualitative. Any system that used a method of device abstraction for a quantitative analysis is classified as qualitative.

B. Level of Implementation

Models are assigned an enterprise network implementation score of high, low, or N/A in order to account for the broad range of real-world testing frameworks have received. It is considered irresponsible to recommend an untested framework for use in production networks prior to significant live testing. A framework with hundreds of implementations and years of feedback will similarly have more data points to evaluate than a network which is conceptual or in its first live network test. Many surveyed frameworks have not yet been employed in a significant capacity on a live network, but they are included in this survey. Untested frameworks are examined in order assess approaches that have been tried in previous research, or are on the cutting edge of risk management development.

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, but they are important to consider when examining the current state of IoT adaptation. Several analyzed methodologies have been iterated over the course of years and decades. The version of a methodology selected for this paper is reflected by the date and any version release information discussed in Section II. When applicable, the individual publications are cited and referenced with the specific iteration selected for analysis.

D. Overall Rating

The current industry standard for a risk assessment framework is the a qualitative model. This method of assessment relies on robust security policy and patching processes alongside vulnerability scanning and security controls. Examples of these frameworks include the NIST RMF, NCSC CAF 3.0, and ISACA COBIT. These methods are suitable for securing a traditional enterprise network, but have weaknesses to IoT devices that are introduced without being fully incorporated to the baseline. Any framework that meets, but does not have the potential to exceed the current state of the art implementation is rated “Yellow”. Yellow rated models are a relatively good assessments of cyber risk, but they 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 is rated “Red”. Models which have made a meaningful step towards properly accounting for IoT devices within enterprise networks will be rated “Green”. Several methodologies rated green have not been fully deployed in a live test, but have demonstrated that they manage IoT devices with a higher level of effectiveness.

IV. Analysis of Risk Assessment Frameworks

A live test and assessment of each risk model is beyond the scope of this survey. Each selected methodology is broken down according to the criteria outlined in Section III. The assessment of each framework allows for comparison across methodology, age, implementation level, and effectiveness rating. This breakdown is introduced in Table I.

TABLE I. RISK FRAMEWORK COMPARISON

	Framework Analysis		
Reviewed Framework	***Rating***	***Implementation***	***Year***
†CAF [28]	Yellow	High	2018
†COBIT 5 [14][9]	Yellow	High	2012
†CORAS [45]	Red	Low	2003
*CPS Model [43]	Red	N/A	2013
†CPSS [34]	Red	N/A	2015
*CRAMM [27]	Red	Low	2003
*CRISM [32]	Green	N/A	2018
*Cybernomics [44]	Green	N/A	2017
†HCS-IF [19]	Green	N/A	2014
†*Hierarchical Model[37]	Red	N/A	2009
†HTRA [35]	Yellow	High	2007
†IBM Framework [39]	Yellow	Low	2010
†IoT/M2M [21]	Green	N/A	2016
†ISO27K [14][15]	Yellow	High	2005
†ISO31K [13]	Yellow	High	2009
*ISRAM [42]	Red	N/A	2005
†ISSM [5]	Green	N/A	2017
†ISSM [16]	Yellow	Low	2011
*Mobius [22]	Red	N/A	2002
†NIST CSF [7]	Yellow	High	2014
†NIST RMF [46]	Yellow	High	2015
*NSRM [33]	Red	N/A	2009
†OCTAVE [17]	Red	Low	2003
†OCTAVE-S [17]	Red	Low	2003
†OCTAVE-Allegro [18]	Red	Low	2007
†OSSF [23]	Green	N/A	2017
*Patel & Ziveri Model [38]	Red	N/A	2010
†SFR [36]	Red	N/A	2005
†*TARA (Intel) [25]	Yellow	Low	2009
†*TARA (MITRE) [26]	Yellow	Low	2011

†Indicates Qualitative *Indicates Quantitative

A. *Common Framework Pitfalls*

Initial assessment standards required a significant implementation instance in order to merit a "green rating", but no surveyed models with production implementation were designed to account for IoT devices. This requirement was removed as a result each model that rated "green" for IoT advancement has not 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 risk assessment 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 market share footprint is unsustainable if security is to be prioritized.

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 have primarily implemented a quantitative risk assessment approach, but no solution has been able to provide cost-effective coverage to a larger network. Most quantitative models draw from the CVE database, which is reliant on vulnerability publications. Due to the obscurity of IoT systems, many face less rigorous assessment and have fewer published CVE findings. The primary weakness to this solution is some devices will eventually have to have a trusted relationship, and this will lead to inevitable unmitigated 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 30 frameworks surveyed are proposed based on short term and long term research goals. The trend of predominately quantitative risk assessment frameworks in early models was primarily rendered obsolete due to implementation costs rather than level of effectiveness. A short term approach focused on bolstering the IoT specific security controls of qualitative methods is recommended based on current developments in IoT and ICS security best practices. The long term approach recommended by this paper is based on reintroducing elements of quantitative risk assessment and mitigation models through the use of Artificial Intelligence (AI) solutions designed to perform risk modeling and attack probability extrapolation.

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. IoT and ICS devices both utilize interfaces which are not assessed by most current enterprise network vulnerability assessment tools. Physical access on remote devices must also be considered by a risk methodology. Designing network architecture to create the smallest foothold possible for compromised IoT devices may be an effective short term solution, but would need to be accompanied by policy and control updates. Potential examples of this would include creating requirements to implement 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 vital to ensuring that a vulnerable IoT device does minimized damage if exploited. Due to the inherent hidden vulnerabilities in many IoT devices, the threat of lateral attack propagation is extremely high. These strategies focus on limiting an attackers influence in the event that they do gain access to a device. This strategy has been well documented and proposed in several IoT risk management models, but have not been implemented at the scale of a large enterprise in any research studies. Models such as the Cisco IoT/M2M [21] provide an overview of this concept. The focus of the network security controls is placed on regulating and limiting the level of interaction a device can have with other elements of the network.

2) Long Term: Increase viability of quantifiable risk assessment frameworks with Machine Learning: Quantitative frameworks have demonstrated the highest level of accuracy when employed to assesses cyber risk, but are not capable of modeling large networks in their present state. The next iteration of quantitative framework research, currently underway, relies on existing CVE score data to calculate risk, and requires significant oversight to operate. This model still suffers from the scalability issues observed in past threat-quantification based methodologies. This problem must be solved in order for quantifiable frameworks to become viable.

Potential methods for achieving this could include the use of machine learning (ML) in order to implement risk classification and develop individual device profiles. This direction requires significant future research with live testing and development, but could yield lower operating costs when applied at an enterprise level. Building the threat profile and identifying logical/physical location of a device are currently the areas that reliant on the effectiveness of a human input to the system. Creating a method capable of employing passive device detection automatically adjusted to compensate for the additional network systems offers significantly higher reliability at the cost of adding nodes to each subnet. This increases reliance on initial configuration, rather than reliance on network data inputted through survey. Additional scanning tools would be necessary to provide oversight of external network interfaces created by IoT devices similar to proposed solution 1).

ML Tasks typically fall into two categories: regression and classification. Regression involves predicting a real-valued output while classification involves predicting a categorical value [47]. A regression task that could be applied for cyber risk frameworks is to predict values of risk using inputs like those that go into the CVE score along with other risk features. Using these features as input, an ML algorithm could be applied to predict risk values much in the same way as the CVE score. This system would also allow for very accurate projections of security level in proposed architecture developments, as well as software migrations and patching. A classification approach could be applied in coupling with items such as an Intrusion/Anomaly Detection System. The IDS can monitor traffic and create traffic profiles and then they can be fed in as inputs. Using these features, a classification of risk level could be made using a classification algorithm such as Support Vector Machines, Logistic Regression or Random Forest.

Using ML for risk classification and device profiles would require a multi-level approach. For developing device profiles, a classification task could be applied to classify the traffic for each device. With these classifications, then, using a separate ML algorithm, risk level could be classified using the device profiles and passive network traffic such as Snort logs [48]. Coupling this with an input such as CVE scores for known vulnerabilities visible in the traffic could allow for classification of successive levels of risk. Regardless of the ML algorithm used, an approach such as this would require a significant amount of time and data to be useful. The data would also have to be labelled so as to be useful for training and testing an ML algorithm. Thus, this would not be a quick solution, but could be quite powerful if implemented.

V. Conclusion

The assessment of 30 cyber risk assessment frameworks shows significant shortcomings in all state of the art risk methodologies. No developmental model was identified that could be considered deployment ready with capabilities clearly exceeding those of the current generation of qualitative system. Developmental models 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 while maintaining necessary levels of accessibility balanced with security. The scale and diversity of IoT has been insurmountable for qualitative models, but future research developing Proposed Solution 1). may yield significant advancements that do not require substantial changes in architecture. At this time there is not a methodology shown to be able to quantify the additional risk presented by IoT devices. A significant change in funding or advancement in implementation methods 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). offers a potential way forward to make the quantitative model viable again. The development of quantifiable risk methodologies is well regarded, but most current research avenues are still reliant on known vulnerabilities. Additional research in IoT vulnerability assessment is needed in order to accurately populate the risk matrices employed by most proposed quantified frameworks.

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] A. J. Pendleton, D. Pettit, and R. Dill, "Surveying the incorporation of IoT devices into cybersecurity risk management frameworks," *SECURWARE 2019, The Thirteenth International Conference on Emerging Security Information, Systems and Technologies*, pp. 128—-133, 2019.

[2] Government Accountability Office, "Internet of things: Enhanced assessments and guidance are needed to address security risks in dod," *Publication No. GAO-17-668*, 2017.

[3] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," 2018.

[4] K. L. Dempsey, G. A. Witte, and D. Rike, "Summary of nist sp 800-53, revision 4: Security and privacy controls for federal information systems and organizations," Tech. Rep., 2014.

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

[6] National Institute of Standards and Technology. (2016) Risk management framework steps. Last Accessed 2019-12-2. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/images-media/NIST-RMF.png

[7] N. Keller, "NIST Cybersecurity Framework (CSF) Reference Tool," 2014.

[8] M. Ahlmeyer and A. M. Chircu, "Securing the internet of things: A review." *Issues in information Systems*, vol. 17, no. 4, 2016.

[9] K. Wal, J. Lainhart, and P. Tessin, "A cobit 5 overview," 2012.

[10] J. Lainhart, "Introducing COBIT 2019: The Motivation for the Update?" 2018.

[11] ISACA, "Cobit 2019 framework: Introduction and methodology," 2018.

[12] M. S. Lund, B. Solhaug, and K. Stølen, *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media, 2010.

[13] M. Leitch, "ISO 31000: 2009—The new international standard on risk management," *Risk Analysis: An International Journal*, vol. 30, no. 6, pp. 887–892, 2010.

[14] 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.

[15] T. Humphreys, "State-of-the-art information security management systems with iso/iec 27001: 2005," *ISO Management Systems*, vol. 6, no. 1, 2006.

[16] G. Karokola, S. Kowalski, and L. Yngström, "Towards an information security maturity model for secure e-government services: A stakeholders view." in *HAISA*, 2011, pp. 58–73.

[17] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," Carnegie-Melon Univ Pittsburgh PA Software Engineering Inst, Tech. Rep., 2003.

[18] R. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE allegro: Improving the information security risk assessment process," 2007.

[19] I. Atoum, A. Otoom, and A. A. Ali, "Holistic cyber security implementation frameworks: A case study of jordan," *International Journal of Information, Business and Management*, vol. 9, no. 1, p. 108, 2017.

[20] ——, "Holistic cyber security implementation frameworks: A case study of jordan," *International Journal of Information, Business and Management*, vol. 9, no. 1, p. 108, 2017.

[21] "Cisco: Securing the internet of things: A proposed framework." 2016.

[22] D. D. Deavours, G. Clark, T. Courtney, D. Daly, S. Derisavi, J. M. Doyle, W. H. Sanders, and P. G. Webster, "The mobius framework and its implementation," *IEEE Transactions on Software Engineering*, vol. 28, no. 10, pp. 956–969, 2002.

[23] J. Meszaros and A. Buchalcevova, "Introducing ossf: A framework for online service cybersecurity risk management," *computers & security*, vol. 65, pp. 300–313, 2017.

[24] M. S. Lund, B. Solhaug, and K. Stølen, "A guided tour of the CORAS method," in *Model-Driven Risk Analysis*. Springer, 2011, pp. 23–43.

[25] M. Rosenquist, "Prioritizing information security risks with threat agent risk assessment," *Intel Corporation White Paper*, 2009.

[26] J. Wynn, J. Whitmore, G. Upton, L. Spriggs, D. McKinnon, R. McInnes, R. Graubart, and L. Clausen, "Threat assessment & remediation analysis (tara): Methodology description version 1.0," MITRE CORP BEDFORD MA, Tech. Rep., 2011.

[27] Z. Yazar, "A qualitative risk analysis and management tool–cramm," *SANS InfoSec Reading Room White Paper*, vol. 11, pp. 12–32, 2002.

[28] United Kingdom National Cyber Security Centre, "Cyber assessment framework," 2020.

[29] T. Kevin, "Introducing the cyber assessment framework v2.0," 2018.

[30] ——, "Introducing the cyber assessment framework v3.0," 2019.

[31] Government Accountability Office, "Internet of things: Status and implications of an increasingly connected world," *Publication No. GAO-17-75*, 2017.

[32] S. Shetty, M. McShane, L. Zhang, J. P. Kesan, C. A. Kamhoua, K. Kwiat, and L. L. Njilla, "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.

[33] 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.

[34] 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.

[35] Government of Canada, "Harmonized Threat and Risk Assessment (HTRA) Methodology," 2007.

[36] 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.

[37] 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.

[38] 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.

[39] 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*, vol. 4528, no. 1, pp. 1–96, 2010.

[40] A. Buecker, S. Arunkumar, B. Blackshaw, M. Borrett, P. Brittenham, J. Flegr, J. Jacobs, V. Jeremic, M. Johnston, C. Mark *et al.*, *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*. IBM Redbooks, 2014.

[41] A. Buecker, B. Chakrabarty, L. Dymoke-Bradshaw, C. Goldkorn, B. Hugenbruch, M. R. Nali, V. Ramalingam, B. Thalouth, J. Thielmann *et al.*, *Reduce Risk and Improve Security on IBM Mainframes: Volume 1 Architecture and Platform Security*. IBM Redbooks, 2016.

[42] B. Karabacak and I. Sogukpinar, "Isram: information security risk analysis method," *Computers & Security*, vol. 24, no. 2, pp. 147–159, 2005.

[43] 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.

[44] K. Ruan, "Introducing cybernomics: A unifying economic framework for measuring cyber risk," *Computers & Security*, vol. 65, pp. 77–89, 2017.

[45] K. Stolen, F. den Braber, T. Dimitrakos, R. Fredriksen, B. A. Gran, S.-H. Houmb, M. S. Lund, Y. Stamatiou, and J. Aagedal, "Model-based risk assessment-the coras approach," in *iTrust Workshop*, 2002.

[46] R. S. Ross and L. A. Johnson, "Guide for applying the risk management framework to federal information systems: A security life cycle approach," Tech. Rep., 2010.

[47] G. James, D. Witten, T. Hastie, and R. Tibshirani, "Classification," in *An Introduction to Statistical Learning*. New York: Springer Science & Business Media, 2013, ch. 4, pp. 127–173.

[48] M. Roesch, "Snort-Lightweight Intrusion Detection for Networks," in *Proceedings of LISA '99*, 1999, pp. 229–238.