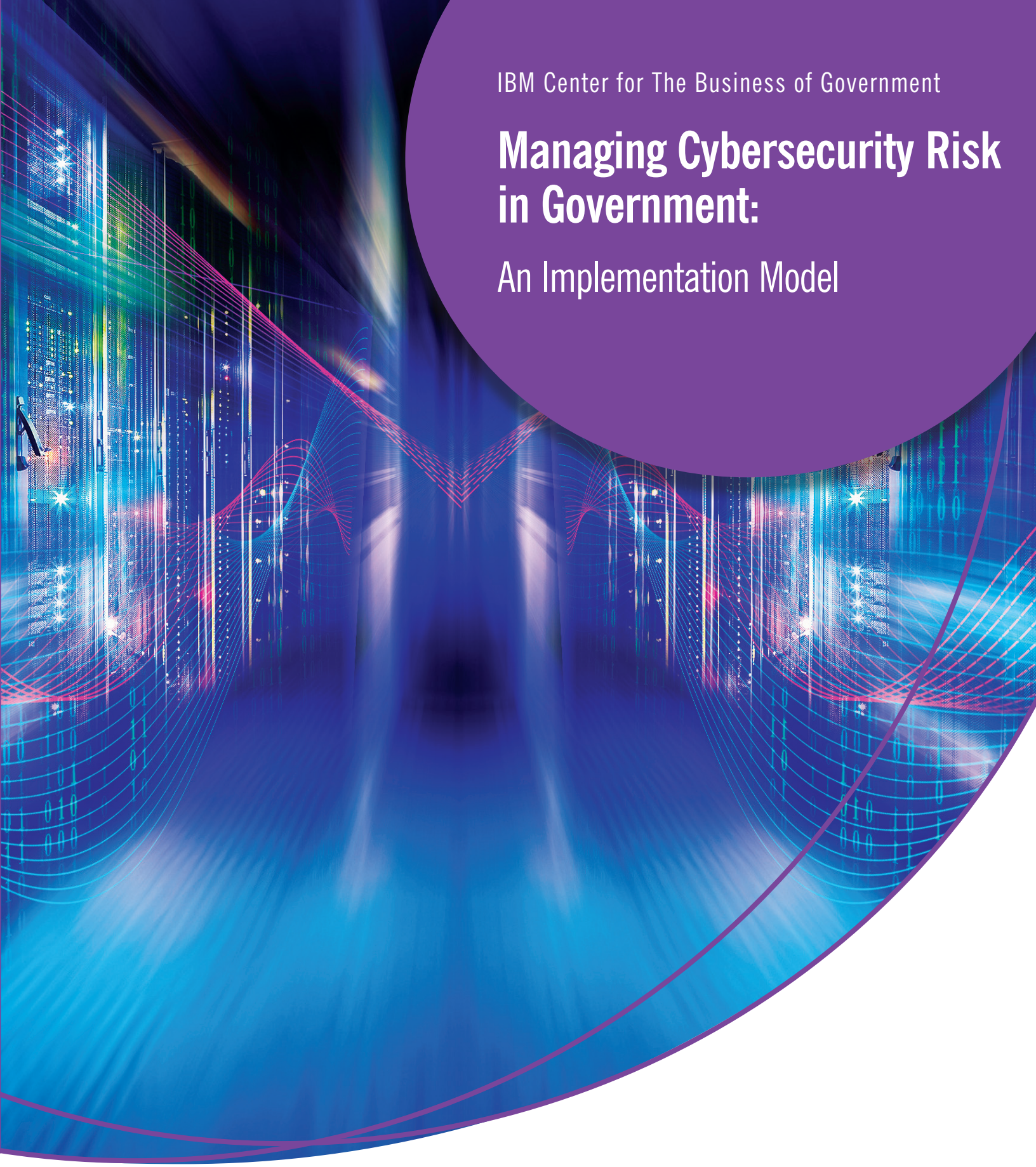


IBM Center for The Business of Government

Managing Cybersecurity Risk in Government:

An Implementation Model

Rajni Goel
Howard University

James Haddow
Howard University

Anupam Kumar
Howard University

IBM Center for
The Business of Government
20 years of research for government:
informing today, envisioning tomorrow

1998-2018

Managing Cybersecurity Risk in Government: An Implementation Model

2018

Rajni Goel
Howard University

James Haddow
Howard University

Anupam Kumar
Howard University

IBM Center for
The Business of Government
20 years of research for government:
informing today, envisioning tomorrow
1998-2018

TABLE OF CONTENTS

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, Managing Cyber Risk in Government: An Implementation Model, by Rajni Goel, James Haddow, and Anupam Kumar of Howard University.

The increased use of technologies such as social media, the Internet of Things, mobility, and cloud computing by government agencies has extended the sources of potential cyber risk faced by those agencies. As a result, cyber is increasingly being viewed as a key component in enterprise risk management (ERM) frameworks. At the same time, agency managers encounter the challenge of implementing cyber risk management by selecting from a complex array of security controls that reflect a variety of technical, operational, and managerial perspectives.

DANIEL J. CHENOK

In this report, the authors address current and potential future organizational cybersecurity and risk management needs by creating a decision model that allows agencies to tailor approaches for particular cyber challenges. The authors review existing risk management frameworks in use across government, and analyze steps that agencies can take to understand and respond to those risks in a manner consistent with existing law and policy. They put this work together to develop an implementation model based on taking five steps to improve cybersecurity outcomes: Prioritize, Resource, Implement, Standardize, and Monitor–the PRISM model.

SHUE-JANE THOMPSON

This report builds on recent Center publications that address risk management, including *Managing Risk in Government: An Introduction to Enterprise Risk Management* by Karen Hardy; *Managing Risk, Improving Results: Lessons for Improving Government Management from GAO's High Risk List* by Don Kettl; and *Improving Government Decision Making through Enterprise Risk Management,* by Thomas Stanton and Douglas Webster.

We hope that this report provides a useful model for government agencies to adapt in managing cyber risks.

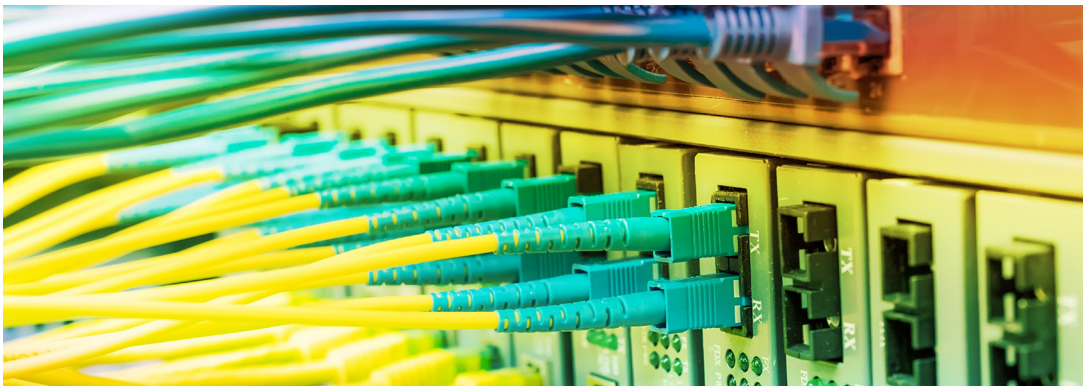
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com

Shue-Jane Thompson
Vice President, Cyber and Biometrics Service Line
IBM Global Business Services
shuejane@us.ibm.com

INTRODUCTION

"Always connected" is the new normal due to advancements in information and communication technologies.

As government organizations expand operations to include the use of technologies such as social media, the Internet of Things, mobile, and cloud, they inherently extend their cyber exposure. Data stratification in cyberspace extends throughout government organizations, and regardless of the level of traditional security precautions, cyber risk persists anywhere data exists. This creates a need for cybersecurity risk strategies to protect and manage private and sensitive information. The need for customized management strategies at the organizational/agency level is enhanced given that the number of cyberattacks against governments and commercial enterprises globally continues to grow in frequency and severity.



Risk management focuses on assessing significant challenges to an organization and its operations and implementing a set of predetermined risk responses. An IBM Center for The Business of Government report[1] identifies the benefits and limitations of the traditional risk management approach, and details the evolution of Enterprise Risk Management (ERM) in the federal government to overcome the shortcomings of managing risk in silos. ERM has become an integral element in organizational strategy today. Securing data and managing cyber risk must now be viewed as a key component within an organization's ERM framework.

The National Institute of Standards and Technology (NIST) advises that similar to financial and reputational risk, poorly managed cybersecurity risk may negatively affect performance and place an organization at risk by reducing its ability to innovate. This can occur even while leaders focus in the near term on the precise status of their organization's cybersecurity posture and the risk of becoming a victim of cybercrime or cyberattack. Currently, U.S. Government agencies certify the operational security of their information systems against the requirements of the NIST Risk Management Framework (RMF).[2] The RMF focuses on the federal government and is complemented by the *Framework for Improving Critical Infrastructure Cybersecurity* (known as the Cybersecurity Framework, CSF), developed as guidance to help organizations of all sizes (private or public) to manage cybersecurity risk critical infrastructure.[3]

1. D. W. Webster and T. H. Stanton, "Improving Government Decision Making through Enterprise Risk Management," Risk Series Report, IBM Center for The Business of Government, 2015.
2. National Institute of Standards and Technology, "NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems," 2010, http://dx.doi.org/10.6028/NIST.SP.800-37r1
3. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cyber Security, February 2014.

Yet, how much do governmental decision makers and executives know about their cybersecurity risk status and issues? And how can agencies begin to quantify and manage cybersecurity risks within established ERM frameworks?

Inadequate cyber risk assessments in the government are evident as critical government information systems continue to be subject to successful attacks *in spite of* the RMF and other NIST frameworks. This is partially a factor of complexity. Though an agency is required by the RMF to implement security controls specified in NIST SP 800-53 for various sensitivity levels across the agency's systems, the volumes of top-level controls—each with a series of multiple variations—make implementation a complicated task. Also, while NIST guidance details each control and its variations, agencies must develop tools that enable them to make precise interpretations in their own cyber environments. Additional risks arise when a particular control is not implemented by the agency's system and executives decide to accept the associated risk. Agency executives are not adequately trained to fully comprehend either specific control requirements or the downstream impact of technical and operational risks. In this respect, several studies have cited the need to further define a risk-based approach to cybersecurity.[4]

To improve the ability of organizations to implement effective cyber risk management, a decision matrix can help identify an appropriately tailored approach to address federal system cyber risk. In this report, we propose a structured process for such implementation based on a model that calls on agencies to draw on analysis of their cyber environment in taking five steps: Prioritize, Resource, Implement, Standardize, and Monitor (PRISM). The PRISM model can serve as an operational cyber risk management tool. We suggest a macro-level approach that can be broadly applied irrespective of the organization type. PRISM can help agency security leaders to communicate the impact of investments in security resources on reducing targeted cyber risks.

PRISM is a methodological approach in assessing, prioritizing, investing, implementing and subsequently mitigating cybersecurity risks. The framework originates from the fundamental theory that the lack of strategic focus on *prioritization* of cyber activities is a key gap in the tailoring of a successful risk management process for individual agencies. Prioritizing includes identifying the main risk drivers and interdependencies among them. The PRISM model expands the focus of achieving cybersecurity objectives, such as identifying and reducing vulnerabilities, meeting mission requirements, standardizing operations, and simplifying processes. This decision framework will enable cyber decision makers to identify and operationalize a tailored approach to address risk management and cybersecurity problems. Such an approach will also assist agency leaders in adapting an overall organizational cybersecurity risk assessment to organizational prioritizes.

The following sections summarize the body of knowledge in the domain of cybersecurity risk and existing frameworks, and highlight the nature of diversified threats faced by organizations. Subsequently, the report details how the PRISM framework and its applications can help agencies implement cyber risk management and concludes with a summary of recommendations for practical implementation steps that agencies can take.

4. C. Andrews, "From the inside out: Creating a holistic cybersecurity strategy for government," GovLoop, December 13, 2016, https://www.govloop.com/resources/inside-creating-holistic-cybersecurity-strategy-government; D. Chenok and J. Lainhart, "Achieving Cost-Effective, Mission-Based Cybersecurity: Using Risk Management and Analytics to Manage Vulnerabilities and Threats," IBM Center for The Business of Government, March 27, 2014, http://www.businessofgovernment.org/blog/achieving-cost-effective-mission-based-cybersecurity-using-risk-management-and-analytics-manage.

Enterprise and Cybersecurity Risk Management

Cybersecurity refers to securing data in *electronic* form. The Committee on National Security Systems (CNSS) defines information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Cybersecurity includes the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the organization's cyber environment including hard and soft assets.

To address cybersecurity concerns in the federal government, the Federal Information Security Management Act (FISMA) codifies the Department of Homeland Security (DHS) as the operational lead for federal cybersecurity. FISMA provides DHS authority to coordinate government-wide cybersecurity efforts, including continuous diagnostics and mitigation efforts across agency systems. While a coordinated and concerted effort under the stewardship of DHS has helped mitigate the issue of constrained resources and capabilities with individual agencies, existing approaches to cybersecurity continue to be largely reactive and lacking in a risk-based strategy.

Cyber risk can be thought of as the likelihood of an event occurring, factoring in the consequences of that event. Risk is fundamentally the quantitative measure of the potential damage caused by specific threat. The likelihood of a breach or a security incident is a function of the (1) likelihood of a threat appearing and (2) likelihood that the threat is successful (which is relative to successfully exploiting a vulnerability in the system). Hence, the cyber risk assessment process includes identifying, characterizing, and understanding potential risk scenarios, which translates to studying, analyzing, and describing the set of outcomes and likelihoods for a given cyber activity.

Unfortunately, cybersecurity is often thought of as primarily an information technology (IT) problem—in fact, it is also a people, process, and management/leadership problem. Understanding cybersecurity requirements means assessing unique organizational risks associated with multiple factors, including business processes, organizational structure, goals, risk tolerance, culture, and system design. Calculating cyber risk is complex as it requires a combination of vectors, ranging from threats (known and unknowns), to vulnerabilities (including information sharing), to human behavior, and to organizational assets (tangible and intangible).

To assist with these issues, existing ERM plans are expanding to include cyber risk assessment frameworks. In fact, the World Economic Forum's Partnering for Cyber Resilience initiative report indicates that cyber risk is increasingly viewed as a key component in ERM frameworks.[5] The report quantified cyber risk in a three-fold approach to make sound investment and risk mitigation decisions:

- Understand key cyber risk drivers required for modeling cyber risks
- Understand the dependences among these risk drivers that can be embedded in a quantification model
- Identify ways to incorporate cyber risk quantification into ERM

A cybersecurity risk management (CSRM) framework enables an organization to build an end-to-end risk strategy for gathering and analyzing information and developing approaches aligned with the mission. Currently, agency leaders may reference commonly known CSRM strategies for cybersecurity controls without adaptation to address their unique cyber environ-

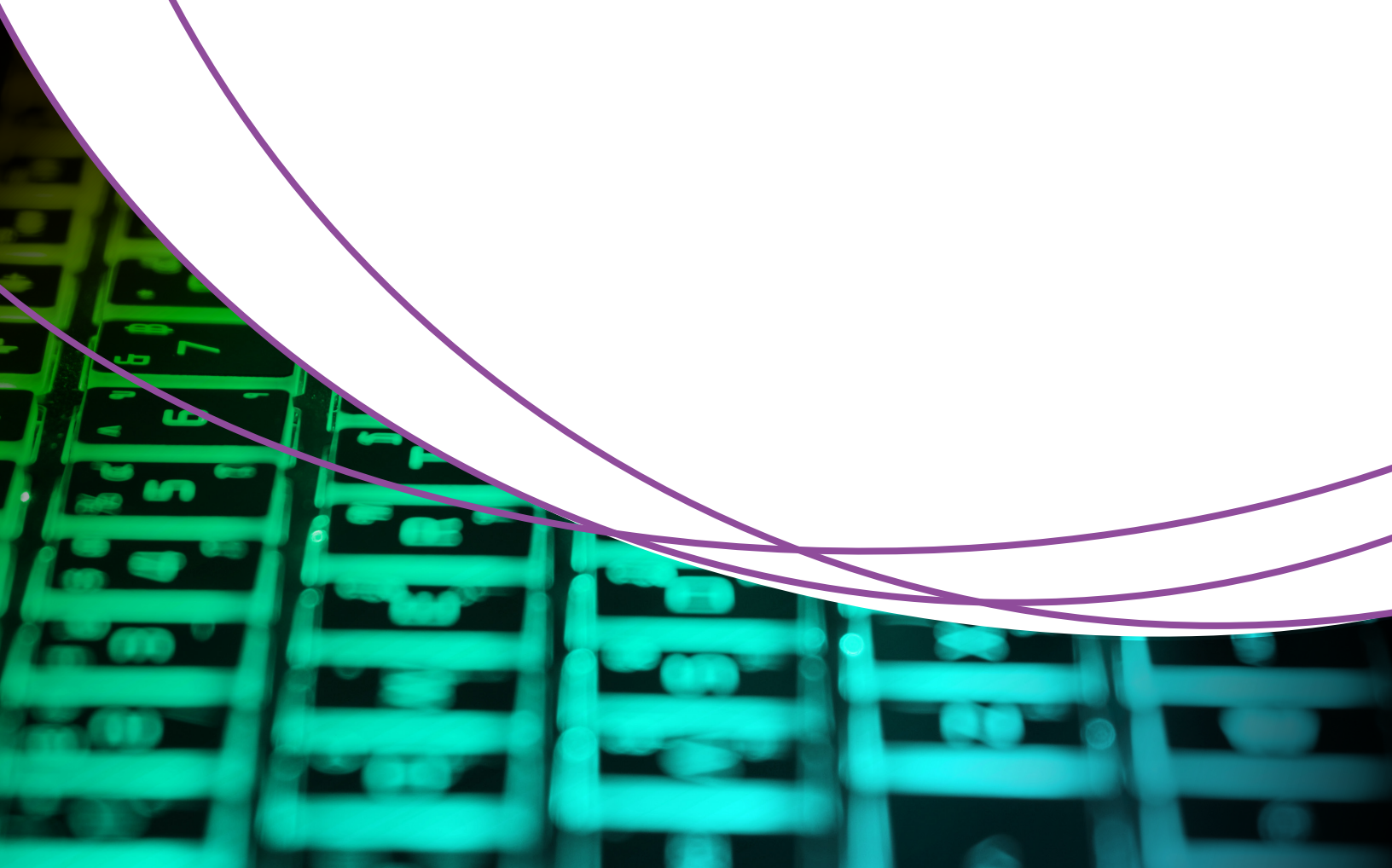
5. World Economic Forum, "Partnering for Cyber Resilience towards the Quantification of Cyber Threats," January 2015.

ment. But they encounter the challenge of selecting from a daunting number of security controls and commercially available solutions tied to infrastructure and assets. Competing risk management frameworks and approaches focus on different priorities, and therefore prescribe solutions that are often difficult to compare from one functional area to another, and from one organization to the next. Hence, agency leaders ideally require a cyber risk situational awareness dashboard that displays how their enterprise is positioned and organized to implement CSRM. This dashboard should highlight individual agency levels of sensitivity, risk drivers, and a current status on resources, assets, and people deployed.

For ERM generally, organizations that provide definitions and characteristics include the Casualty Actuarial Society (CAS), the Association for Enterprise Risk Management (AFERM), and the Risk and Insurance Management Society (RIMS). RIMS suggests seven distinguishing ERM features, including how ERM encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc.) and how ERM should prioritize and manage those exposures as an interrelated risk portfolio, not individual silos.[6] Following on these and other ERM foundations, several frameworks have been established that act as guides for organizations to navigate the complexities of cybersecurity risk management (described in detail in subsequent sections).

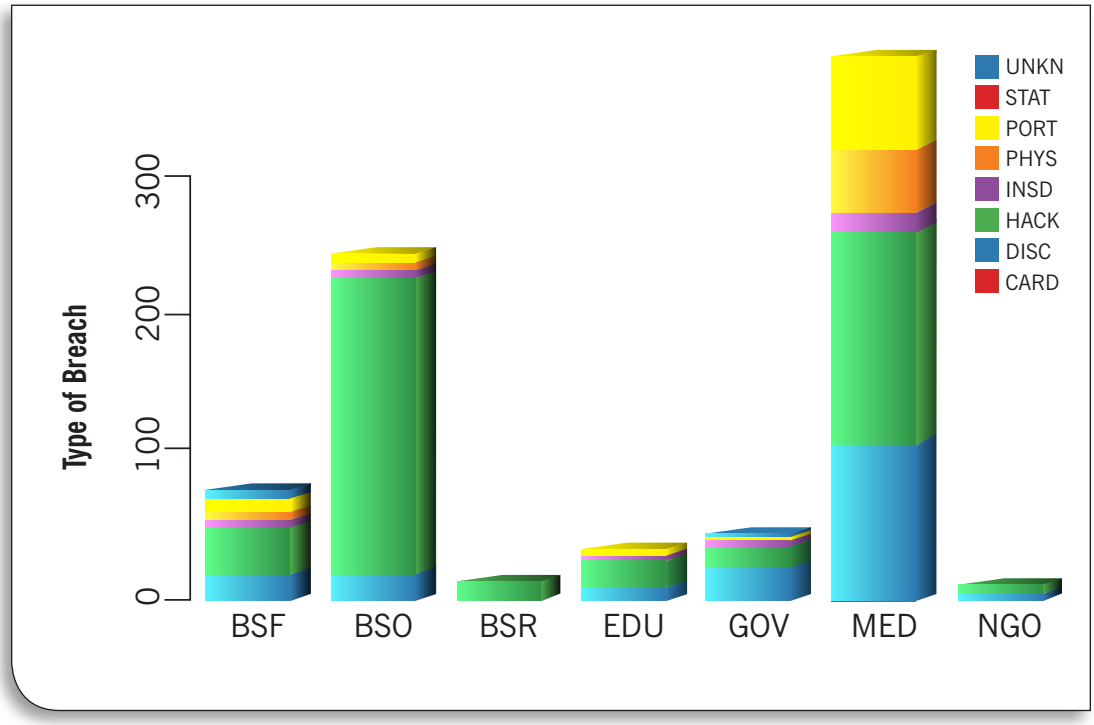
6. The Institute of Risk Management, *IRM Cyber Risk: Executive Summary,* 2014.

Nature of Cybersecurity Threats



CSRM is necessary for organizations that seek to deliver on their missions while facing a multitude of cyber threats—including phishing attacks, sophisticated viruses exploiting zero-day vulnerabilities, and above all, internal threats to confidential data from state and non-state actors. Multiple types of evolving threats vary in size and complexity, and emerge in organizational contexts that make it difficult to create a one-size-fits-all solution. For example, an attack on the electricity grid is different from an attack to steal intellectual property from a vault on a firm's server. In general, experts distinguish between supervisory control and data acquisition (SCADA) systems like those that power electricity grids from traditional information systems. The specific prioritization of actions for availability, integrity, and confidentiality in SCADA may differ from similar priorities in a traditional information system. This exemplifies the need for a tailored cybersecurity risk management framework that aligns with organizational priorities.

Figure 1. Type of breach by organization type.



In addition, there is little consensus on how best to protect against cybersecurity threats, especially the unknowns, like a "zero-day" vulnerability. A zero-day vulnerability is an unknown hole in the software that cannot be identified prior to an attack and can be exploited by fast evolving cyber intrusions. Industry experts have advocated varying response levels depending on what is at stake. Responses range from disconnecting from the Internet to building strong firewalls to strengthening system monitoring as protection from unwanted attacks.

It is impossible to completely eliminate cybersecurity risks given numerous access points to information systems. Furthermore, organizations must weigh the cost of implementing solutions that might be against delivering on mission requirements. For example, setting up a disconnected intranet is expensive and could stymie innovation and efficiency that occur by leveraging solutions developed on the open Internet.

Recent incidents highlight the challenges in maintaining a cybersecurity posture that can defend against every possible attack scenario. The avenues of attacks are proliferating faster than organizational response times in deploying safeguards. As a result, it is of utmost importance for organizations to improve their security posture and dedicate sufficient resources for cybersecurity. Organizations must to be able to isolate attacks, limit losses, and be able to recover rapidly from cyberattacks.

Given the broad range of attacks, it therefore becomes important for organizations to understand their vulnerabilities and focus resources on areas where there is a greater likelihood of attack. Based on data reported by privacyrights.org covering a period starting January 2015, the stacked bar chart in Figure 1 illustrates the frequency of attack specific to organization type. The website records and provides data on several types of breaches by organization type. The type of breaches included are payment card fraud (CARD), hacking or malware (HACK), insider (INSD), physical loss (PHYS), portable device (PORT), stationary device (STAT), unintended disclosure (DISC), and unknown (UNKN). The types of organizations included in this dataset include financial and insurance services (BSF), retail businesses including online (BSR), educational institutions (EDU), military and government (GOV), healthcare and medical (MED), non-profits (NGO), and others (BSO). An examination of the figure suggests that the preponderance of breaches in the retail organization type (BSR) are from hacks, as opposed to the government and military (GOV) type, which deal with several different forms of breaches. In addition, the government suffers from a sizable amount of unintended disclosures in its set of breaches.

Moreover, with the General Data Privacy Regulation (GDPR)[7] that took effect on 25 May 2018, the aftermath of cyberattacks can carry significant monetary and reputational impacts. GDPR obligations span across controls necessary to protect privacy in both public and private organizations; as a result, a complete guide to manage cybersecurity risk is essential.

7. European Union, *General Data Protection Regulation,* (EU) 2016/679, April 14, 2016. https://gdpr-info.eu.

Frameworks to Manage Cybersecurity Risk

In order to analyze and manage cyber risks, the quantification of cyber threats and vetted approaches is necessary to make sound investments into risk mitigation decisions. Multiple frameworks, standards, and policies assist organizations to understand their risk. Several qualitative and quantitative models have been proposed for enterprise risk management in general, and cybersecurity risk management within the ERM context specifically. Several relevant risk-based standards, models, and decision frameworks follow:

1. Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework led by NIST) https://www.nist.gov/cyberframework

2. Control Objectives for Information and Related Technologies (COBIT)[8] https://cobitonline.isaca.org/publications

3. CORAS (Construct a platform for Risk Analysis of Security Critical Systems) methodology http://coras.sourceforge.net/documents/080828TheCORASMethod.pdf

4. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) https://www.cert.org/resilience/products-services/octave/

5. DREAD MS (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability) https://wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD

6. CRAMM (CCTA Risk Analysis and Management Method) https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83

7. ISO 27000 https://www.itgovernance.co.uk/iso27000-family

The applicability of the above models require detailed knowledge, especially in the risk assessment and risk mitigation phase, about IT security and the organization's technical environment.[9] Given the circumstances, agencies may typically rely on domain experts in data, networking, and operating system security. A natural result of such practices is a fragmented approach that moves away from an enterprise-wide strategy for managing cybersecurity risk. In addition, these detailed frameworks could be enhanced with executive guidance that can help senior leaders manage cybersecurity risk. We highlight two of the primary frameworks, NIST and COBIT, in the following section.

NIST

The Cybersecurity Framework from NIST reflects one of the most comprehensive frameworks with regard to the breadth of cybersecurity, and points to "Informative References" as examples of pre-existing and detailed treatments reflecting greater depth on specific topics in cybersecurity (e.g., controls catalogs, technical guidance) that pair well with the Framework. The Cybersecurity Framework lists five core functional areas for cybersecurity: identify, protect, detect, respond, and recover. Under these five areas are 23 categories and 108 subcategories mapped to various secondary references (such as CSC, COBIT 5, and ISO 27000). For the purposes of evaluation, each of the categories or subcategories can be mapped to one of the four tiers to assess the organization's maturity on that category/sub-category.

8. As a catalogue of controls, COBIT is similar to NIST Special Publication 800-53rev4. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

9. A. Ekelhart, S. Fenz and T. Neubauer, "Aurum: A framework for information security risk management," *Proceedings of the 42nd Hawaii International Conference on System Sciences,* January 2009.

NIST standards include significant detail and references to secondary standards. For example, NIST points to several other standards, such as COBIT 5 or ISO, but having been written for non-cybersecurity experts and cybersecurity experts alike, NIST guidance does not provide a simplified way to implement the framework without deciphering a complex span of technical controls available through references to other standards. In addition, some stakeholders have expressed an interest in adding a quantitative dimension to the Cybersecurity Framework for accuracy of assessment and to reduce subjectivity in its application.

COBIT

COBIT is a good-practice process oriented framework for IT management and IT governance. It was created by a professional organization called Information Systems Audit and Control Association (ISACA). COBIT 5 includes an add-on related to information security and assurance. COBIT 5 is based on the following five key principles for governance and management of enterprise IT:

- Meeting stakeholder needs to align business and IT goals
- End-to-end coverage of the enterprise that covers all functions and processes, both internal and external
- A single, integrated framework that integrates various other frameworks and can serve as an overarching framework
- A holistic approach that accounts for organizational processes, culture, structures, etc.
- Separate governance and management to de-conflict roles and responsibilities

It has been acknowledged that COBIT can deliver much-needed operational rigor, however, implementation has proven problematic. COBIT requires outsourcing help as implementation is typically executed by a third-party IT service provider. In such a scenario, the emphasis is on standardization and repeatability for the purposes of compliance and certification.[10] The downside is a disconnect with the business processes of the organization that disincentivizes participation by members of the organization. It is therefore imperative that cybersecurity be an enterprise-wide approach with complete commitment from the top members of the agency. For the stated purpose of top-down involvement, it is important to have a cybersecurity framework that is easily accessible for executive decision making.

10. S. Overby, "Adopting ITIL, COBIT Is Not Always the Best Practice," CIO, February 2012, https://www.cio.com/article/2399188/it-organization/adopting-itil--cobit-is-not-always-the-best-practice.html.

Cyber Risk in the Federal Sector

How do federal agencies currently assess and manage their cyber risk? How aware are federal agency executives about the precise status of their organization's cybersecurity posture or risk of being a victim of cybercrime or cyberattack? In 2013, the continuation of cyberattack losses led U.S. President Obama to issue Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, and NIST released the Cybersecurity Framework (CSF). The principle behind cybersecurity risk management is to manage the investment in protecting cyber assets so that it does not exceed the expected harm from the risk that is addressed. This principle forms the basis for the NIST Framework.

The NIST Framework—with partnership and guidance from several agencies including the Department of Defense—is in use by federal agencies, which are required to comply and certify their information systems with the Risk Management framework (RFM). The RFM requires the implementation of controls as outlined in the NIST Special Publication (SP) 800-53 for sensitivity of the agency's systems.

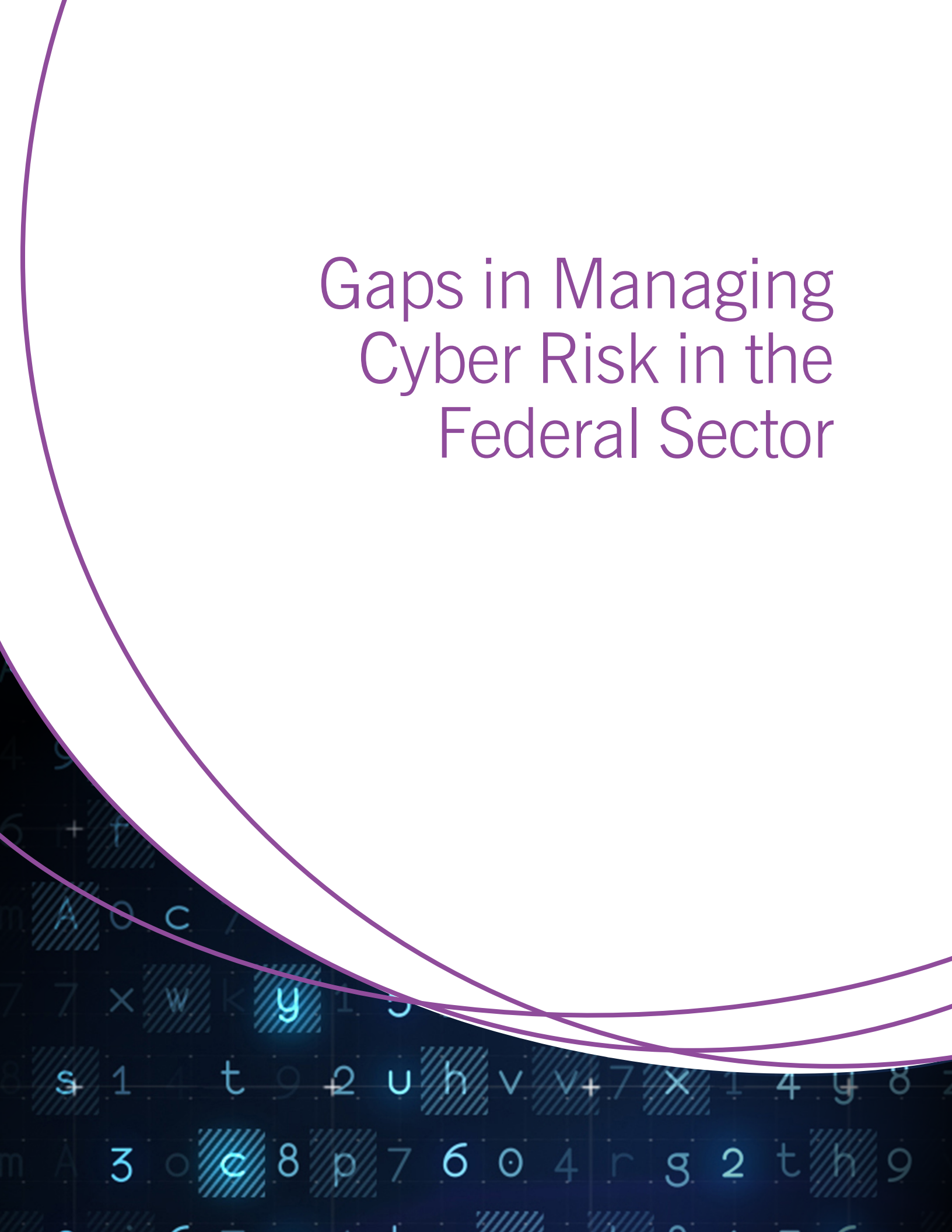
The NIST Cybersecurity Framework provide agencies with a common structure for top-level controls and many variations, both within and across federal agencies and with private sector partners. Though the CSF was originally designed to support providers of critical infrastructure systems, it is available to any organization that wishes to better manage cybersecurity risk. The NIST Framework does not provide an exhaustive list of security activities to be implemented that would cover the requirements of all agencies. Instead, CSF provides a catalog of common security outcomes mapped back to a set of cybersecurity standards. Stated otherwise, the Cybersecurity Framework provides "the what" (i.e., outcomes), and "the how" is left to the implementing party; typically, "the how" is enumerated in more detailed controls catalogs and technical guidance, providing users with flexibility to prioritize, implement, and manage exceptions. Hence, the CSF does not dictate to an organization exactly what to do or where to begin.

According to the Federal Information Security Modernization Act (FISMA) of 2014, the Office of Management and Budget (OMB) is responsible for overseeing federal agency information security practices, priorities, and implementation guidelines. The annual FISMA report to Congress provides an overall view of ongoing federal efforts to mitigate and prevent cyber incidents and implement cybersecurity policies and programs that protect and secure their networks, data, and overall systems.[11]

The report for 2016 presented agency specific Cybersecurity Performance Summaries in which chief information officers (CIO) used metrics that applied criteria from OMB guidance and the NIST standards to report on cybersecurity performance. In addition, cybersecurity was one of the Cross-Agency Priority (CAP) goals. The goal metrics further enable tracking agencies' compliance with and application of NIST standards and guidance. Currently each agency's Cybersecurity Performance Summaries Scorecard reports four items: CIO Assessment, CAP Goal Metrics, Independent Assessment, and US-CERT Incidents by attack vector. Under FISMA and the RMF process, agency executives can accept risk at a level relative to their mission needs, as there are no mandatory security requirements.

11. Office of Management and Budget, *FISMA FY 2016 Annual Report to Congress,* 2016.

Gaps in Managing Cyber Risk in the Federal Sector



Government cyber systems continue to have vulnerabilities and to be a target for successful attacks. Examples include the Office of Personnel Management (OPM), the IRS, and Pentagon intrusions. Today, attackers have expanded their attack vectors to not only include anything connected to the Internet, but also to use the newly available connectivity capabilities as intermediaries through which to launch their attacks. This is seen in the news regarding data breaches being reported regularly by government and private sector enterprises.[12]

Currently, government agencies' estimation of risk in the cyber domain cannot be precisely calculated to indicate the amount of security an investment buys, or the changed level of consequence expected. Potential causes may be an incomplete understanding and measurement of the threat, uncertainty around the effectiveness of countermeasures, and inability to quantify consequences of successful attacks, all of which are necessary to measure risk.

How and where does government begin to quantify and decipher risk that is inherent in an agency's digital assets? Currently, a consistent process to help organizations identify the best approach to addressing supply chain performance, risk management, and cybersecurity does not exist. As a result, managers encounter the challenge of selecting from a daunting number of security controls from all different perspectives.

Having spoken to various leaders in charge of the information security of large and small organizations, we have confirmed that there is a lack of consistent decision-making polices and cyber risk management platforms. Leaders are in a reactive mode. The task of assessing the likelihood of a breach is often inadequately resourced. More investment needs to be made in resources that enable threats to be monitored and defenses to be continuously upgraded. NIST standards are known. Cyber performance could be strengthened by a formal process for cyber risk management to assist in decision making.

The lack of a holistic strategy in dealing with cybersecurity threats has resulted in a number of challenges:[13]

- Government agencies have employed a myriad of tools with a reactive approach that patches vulnerabilities by procuring the latest fix, adding to an already complex technical landscape.
- IT portfolio rationalization has been slow, with legacy systems remaining in place as newer technology is added to address the most recent vulnerability.
- As a result of this technical complexity, senior leaders have poor visibility into their enterprise's assets, as well as an inadequate understanding of the systems to be secured.
- A large chunk of current resources are consumed in dealing with only 20-25 percent of known vulnerabilities, leaving organizations exposed.

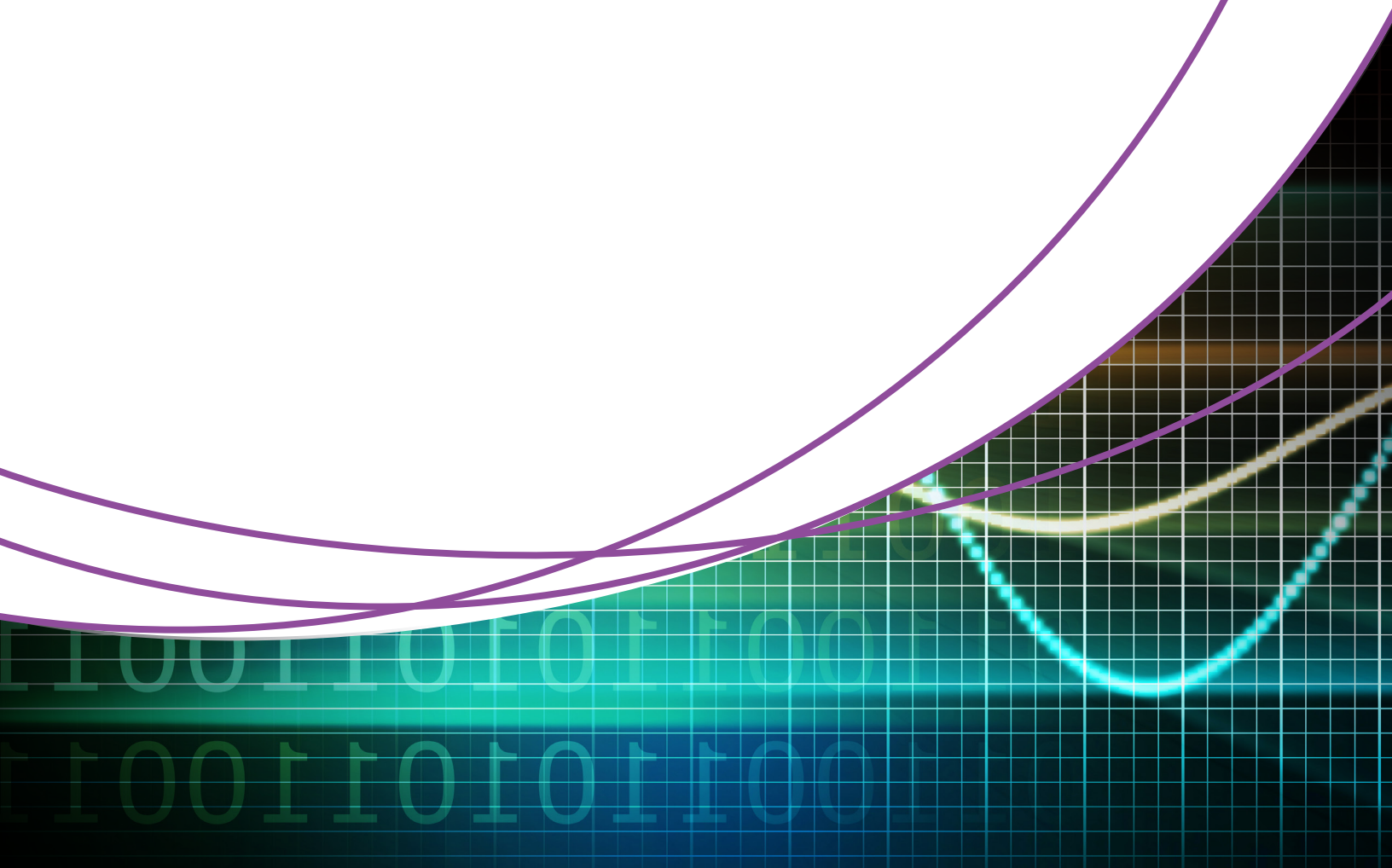
The shortcomings are further highlighted in an analysis of OMB's cybersecurity report.[14] For example, phishing attacks and anti-phishing training are among the continuing concerns in some agencies, yet few gains have been made following current efforts by the federal government.

12. S. Lipner and B. Lampson, "Risk Management and the Cybersecurity of the U.S. Government," Input to the Commission on Enhancing National Cybersecurity, 2016.
13. C. Andrews, "From the inside out: Creating a holistic cybersecurity strategy for government," *GovLoop,* December 13, 2016, https://www.govloop.com/resources/inside-creating-holistic-cybersecurity-strategy-government
14. Zach Noble, "FISMA report shows pain, few gains," Federal Computer Week, March 21, 2016, https://fcw.com/articles/2016/03/21/fisma-omb-noble.aspx.

In summary, agencies face multiple challenges in addressing cybersecurity risk. First, competing and detailed frameworks make prioritization and strategic decision making a challenge. Second, current approaches are often reactive and ad hoc, which can lead to a fragmented approach that drives organizations away from formulation and implementation of a clear strategy for managing cybersecurity risk. Third, inadequate resources to manage cybersecurity risk persist, and the lack of strategy leads to sub-optimal deployment of available resources. And fourth, the fact that attacks affect certain agencies and certain parts of a specific agency suggests that cybersecurity implementation lacks standard practice, which in turn could be resulting in fragmented adoption. Across and within agencies, a lack of standardization and information sharing results in weaknesses and risks that could otherwise be mitigated. Finally, the extensive and prolonged nature of attacks in certain instances highlight issues surrounding monitoring capabilities.

To improve the ability of organizations to address cyber risks, we propose a decision matrix framework to identify appropriate approaches to resolve these problems. A significant body of knowledge regarding cyber risk currently exists in the form of industry white papers and academic research. To synthesize this body of knowledge, we take a multipronged approach for understanding the extent of cybersecurity risk management frameworks. First, we conducted our own meta-analysis of existing white papers to gain an industry viewpoint for developing a framework. We then summarize feedback from leading industry experts to complete the development and validation of a decision matrix for assessing and addressing cybersecurity risk.

Elements Necessary in a Cyber Risk Framework: A Meta-Analysis



Existing cybersecurity frameworks vary in terms of details and resources, including time and budget, needed to complete an assessment. In addition, most existing frameworks do not assist with the formulation of a cybersecurity strategy. While the existing frameworks are detail oriented, they can be overwhelming from an executive viewpoint as an aid to developing a coherent cybersecurity strategy.

In this respect, we find that there is a need for a strategic framework to aid in developing and maintaining a cybersecurity strategy at the enterprise level. We focus on a qualitative model to structure the decision framework as a first step in the cyber risk management process. While quantitative models lead to a detailed assessment, a decision framework using a qualitative model helps to start the planning process in a way that provides value to executives. As a first step towards building a qualitative decision framework, we synthesize the knowledge from existing work using content analysis techniques.

To lay the foundation for a decision framework, we performed a meta-analysis of the existing body of knowledge to harvest key elements of cybersecurity risk management. This approach is based on content analysis of existing industry white papers, academic research, as well as existing framework and risk management documents published by the government. We reviewed a corpus of 32 documents that include cybersecurity related publications including NIST 800-39 and risk management process guidelines developed by the Department of Energy (see Appendix C for a list of the documents reviewed).

To develop common areas of analysis for CSRM, we analyzed key terms that appear throughout these 32 documents—this keyword analysis highlights the areas of emphasis across the corpus. Subsequently, we group the keywords into common thematic areas using an exploratory factor analysis, to guide the building of a decision framework. Table 1 lists the results of the factor analysis.

To further leverage the content analysis, we use keywords within a factor to harvest a central theme, using the standards based on extant literature for thematic association (factor loadings of 0.4 or more). The underlying keywords associated with each of the factors meeting the stated criteria are highlighted in yellow. Themes emerge by leveraging synonyms and extensions of how keywords are commonly used in the cybersecurity industry. For example, a sample of the keywords loading on the first factor include: *chart, map, defender, breach, block,* and others typically associated with monitoring activity that defines the functions of an intrusion detection system.

In addition to associating keywords to a certain cybersecurity function (such as *breach* or *block* vis-à-vis the function of detection), we also look at synonyms for highlighted keywords in the determination of an underlying theme. For example, *critical* or *choice* are associated with the function of selecting or ordering. Finally, we use a level of subjective assessment for interpretation of certain keywords. For example, *government* is extended to regulations with an intent to *standardize*. We conclude by assigning an overall *theme* to each factor, and synthesize them down to *five underlying themes* that we believe are of consequence in establishing a cybersecurity framework for decision making at the highest level of the organization.

The Meta Analysis leads to the five emergent themes of **P**rioritize, **R**esource, **I**mplement, **S**tandardize, and **M**onitor from the content analysis supporting our proposed operational model allows for a tailored approach to cybersecurity risk management: **PRISM.**[15] The following section elaborates on the model developed from the initial content analysis.

15. Note that this model is unrelated to NIST's Program Review for Information Security Assurance (PRISMA)–for information about that program see https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance.

Table 1: Content Analysis of Key Cyber Elements

Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7	Factor 8	Factor 9	Factor 10	Factor 11	Factor 12
data	video	choice	system	asset	industry	process	organization	employee	assessment	risk	firm
pyramid	cyber	c-level	deception	public	development	us	csf	consumer	term	information	fraud
eye	anomaly	north	attack		executive		framework	media		management	
defender	acc	technology	scada				individual	plan		standard	
incident	IT	critical	attacker					online		government	
breach	strategy	cloud	infected					percent		retail	
dark	respond	google	firewall							available	
box	use	satisfied	energy								
enumeration	scale	owned	solution								
block	model	result	server								
cover	comprehensive										
loss	capability										
section	activity										
report	operational										
hacking	operator										
error	change										
action	understanding										
double											
year											
number											
chart											
map											
attribute											
meaning											
right											
payment											

Monitor	Standardize	Prioritize	Implement	Resource	Monitor	Standardize	Resource	Monitor	Prioritize	Standardize	Identify

Decision Framework for Cybersecurity Risk Assessment: The PRISM Approach

As indicated previously, federal agencies rely upon the NIST Cybersecurity Framework that uses five functional areas (Identify, Protect, Detect, Respond, and Recover) and provides agencies with a common structure for top-level controls and assessments. Under FISMA, each agency is required to conduct an annual independent assessment using an Inspector General or Independent Auditor.

This assessment relies primarily on an agency's *"maturity of controls"* to potentially address cybersecurity risks. Specifically, these *controls* reflect each agency's level of maturity based on *"policies, procedures and strategy."* The agency does not necessarily address whether these controls are formalized, documented, implemented, measured, and regularly updated. This approach creates a significant gap since it does not provide insights regarding prioritizing cybersecurity risks within and across agencies based on attack vectors (e.g., phishing, removable media, violation by authorized user, and loss of equipment).

The current Information Security Continuous Monitoring Mitigation (ISCM)[16] approach identified in the 2016 FISMA report to Congress has a key focus on monitoring, rather than agency cybersecurity risk management. Moreover, FISMA reporting on its own does not prioritize risk incidents, nor does it identify if adequate resources are allocated in each agency to mitigate major risks on a sustainable basis. The FISMA report does not detail specific steps agencies should implement to reduce the losses from an incident (e.g., the loss and theft of equipment), nor a process to share and standardize those steps across agencies. Thus, FISMA reporting does not address where federal systems have gaps regarding the themes of allocation of adequate resources, implementation and standardization actions to address an agency's cybersecurity risk awareness, and proactive defense of attacks. Our PRISM model thus complements the FISMA process by addressing missing components (as validated by themes derived in our content analysis above) critical for cyber risk assessment and management. This framework incorporates key drivers of risk identified in the FISMA report.

Through the proposed PRISM decision model, an agency leader continuously Prioritizes, evaluates and allocates adequate Resources, Implements, Standardizes, and Monitors an agencies' cybersecurity posture, preparedness, and responsiveness. Figure 2 below reflects how PRISM aligns with the NIST Cybersecurity Framework.

Prioritize—The distributed environment in which agencies operate includes telecommuting, standard offices, cloud and mobile computing, and web access through personal devices. This environment opens multiple avenues of cyber exposure. Agencies then need to assess the risk or potential impact from compromises in their cybersecurity posture through these different attack vectors, using computational techniques to quantify the probability of compromise through any given avenue.

Cyber analytics can potentially assist each agency component to identify threats and impacts, based on historical data on similar threat vectors and expected effects on sensitive datasets. Both the likelihood of an attack and extent of the impact must be calculated for risk prioritization. For example, if an agency executive determines that a particular office has a major risk from phishing that has resulted in exposure to sensitive information and/or damage to specific systems/applications, the agency should categorize this risk with a high priority weighting.

Resource—Most agencies report that cybersecurity is underfunded, even as the opportunity cost of poor security can far outweigh protective investments. Funding can support financial,

16. National Institute of Standards and Technology, "NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," 2011. http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

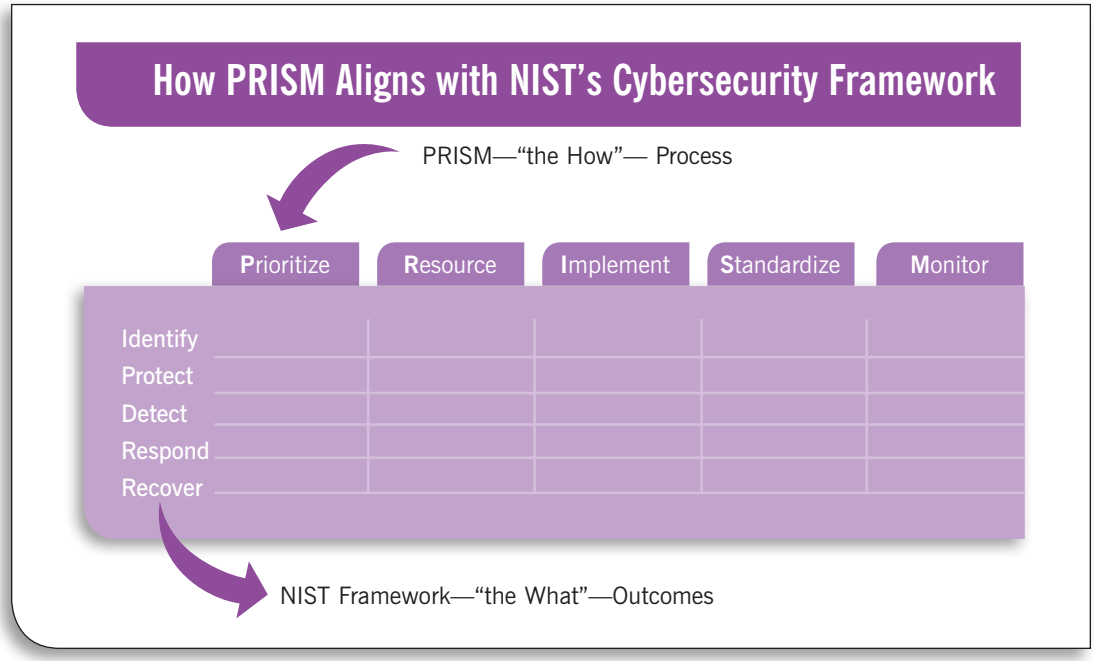
personnel, technology, and/or other resources necessary to address and resolve a cybersecurity risk area, factor, or vector. Applied to the phishing example above, this would support providing adequate resources to address and resolve the issue, and point to establishing ongoing standardization and monitoring processes to mitigate similar risks in the future.

Implement—Agencies should rapidly detect and destroy viruses and other forms of malware introduced in their ecosystem. The initial approach can be localized and tactical in nature. However, agencies must also "stage" implementation tactics to address specific risk management elements.

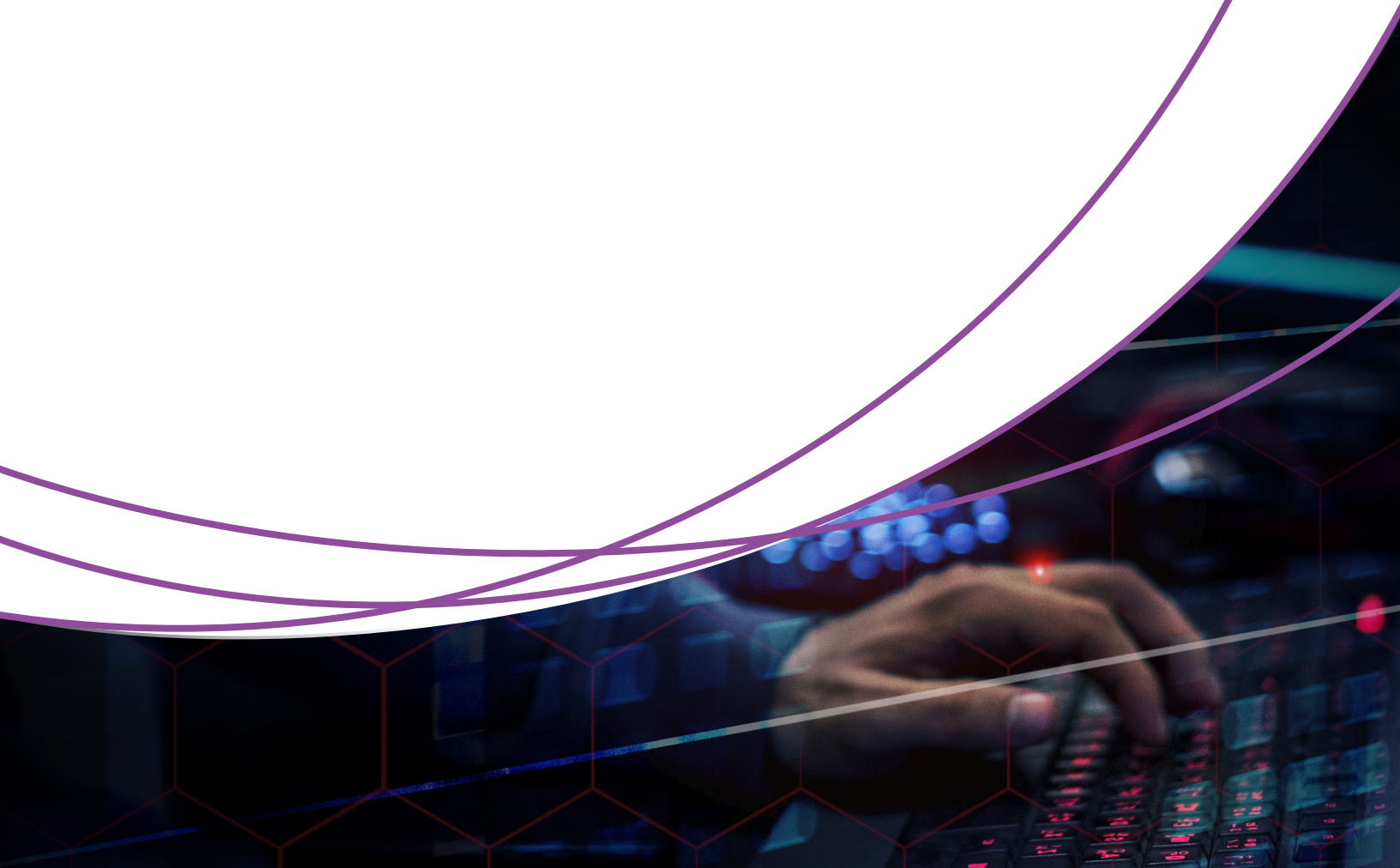
Standardize—By sharing information across agencies, the federal government can institutionalize knowledge and solutions about cyberattacks to avoid repeat incidents and incrementally build awareness, preparedness and response knowledge and tactics. Agencies should incorporate new knowledge and tactics into their standard operating procedures (SOPs) to support remote locations and partners. This should be done in a manner tied to the key metrics that demonstrate cyber performance in and across agencies.

Monitor—Agencies must constantly monitor their systems for unusual behavior. From monitoring, agencies can track digital footprints and assess system loads to detect anomalies, protecting their cyber interests. Continuous monitoring, implemented in the federal space as the Continuous Diagnostics and Mitigation (CDM) program, is a critical on-going activity that agencies must adopt to protect systems, networks, information, and data from attacks.

Figure 2: Alignment from the NIST Cyber Framework to PRISM



Implementing the PRISM Decision Model



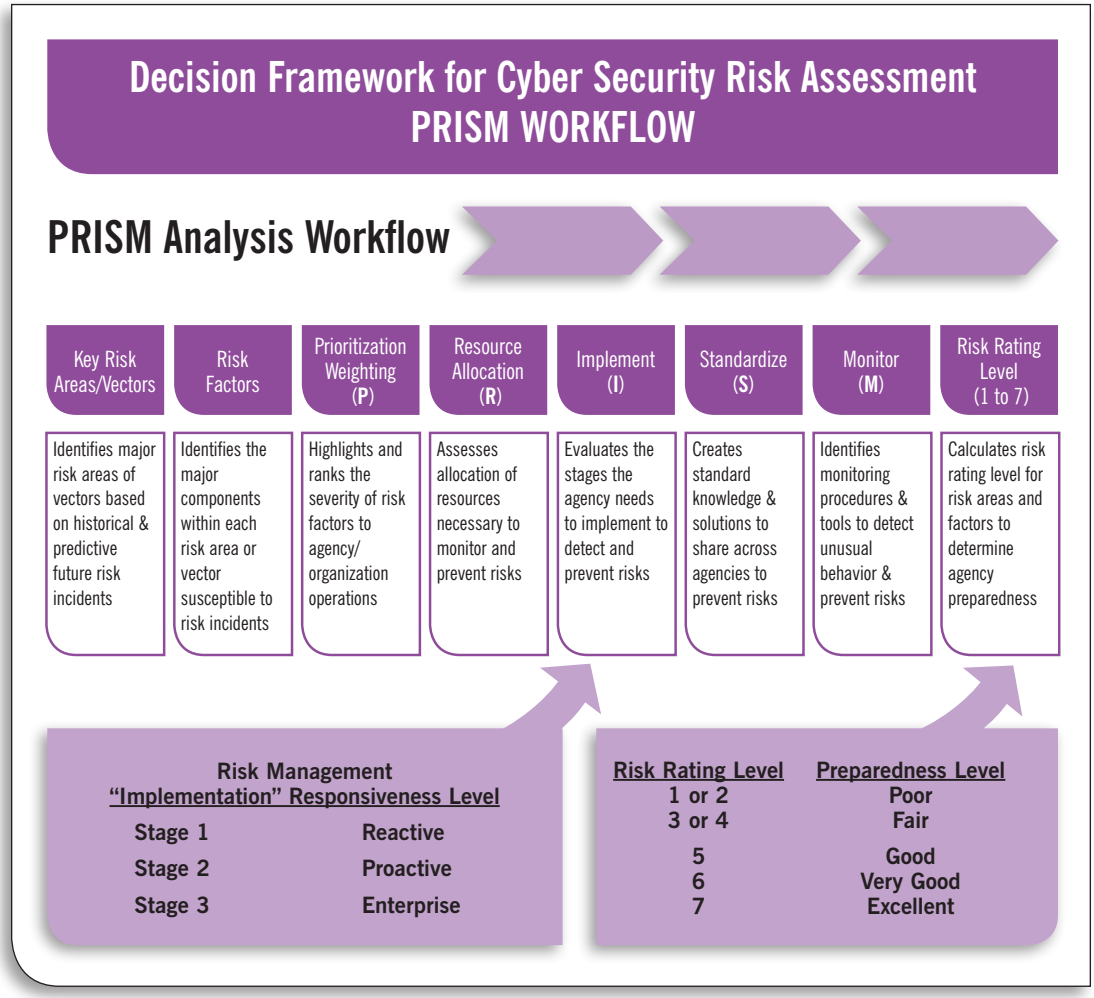
To operationalize the PRISM model, we identify a detailed set of risk factors for scoring using the PRISM criteria. The framework assesses an agency's "current status" on a range of information or operational security risk factors. Designated experts in an agency can use the framework to independently and collectively review each of the risk factors to determine the agency's current "stage" of risk management response capacity. The findings of this review would identify security areas, factors, or vectors that need minor to major enhancements to mitigate future security risks (prioritize). Table 6 of the FY2016 FISMA report entitled "Agency-Reported Incidents by Attack Vector" identified eight attack vectors, shown in column 1 in the table below. The nine Key Risk Areas in the last column below encompass the eight attack vectors contained in Table 6 of the FY2016 FISMA report.[17] The broader risk areas defined in the PRISM model encapsulate narrower attack types that are specific to units in an organization. This enables the use of PRISM across many different types of agencies and the functions they provide.

Attack Vector	Description	CFO	Non-CFO	Government-wide	Key Risk Area(s)
Attrition	Employs brute force methods to compromise, degrade, or destroy systems, networks, or services	108	1	109	Components, Applications/ Tools
E-mail/ Phishing	An attack executed via an email message or attachment	3,160	132	3,292	Data and Information
External/ Removable Media	An attack executed from removable media or a peripheral device	132	6	138	Storage Devices
Impersonation/ Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	60	4	64	Applications/ Tools, Networks
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories	3,920	210	4,130	Governance
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization	5,313	377	5,690	Operational–Products & Services
Web	An attack executed from a website or web-based application	4,766	102	4,868	Networks, Applications/ Tools
Other	An attack method does not fit into any other vector or the cause of attack is unidentified	11,365	437	11,802	Components
Multiple Attack Vectors	An attack that uses two or more of the above vectors in combination	789	17	806	All Risks
Total		29,613	1,286	30,899	

17. Office of Management and Budget, FISMA FY 2016 Annual Report to Congress, 2016.

Figure 3A below provides an overview of the PRISM Model Analysis Workflow for risk mitigation. Figure 3B below provides the Detailed Risk Analysis Areas and the critical questions that agencies should ask regarding their current risk management preparedness and responsiveness. These figures summarize detailed charts shown in Appendices A and B.

Figure 3A: Cybersecurity Decision Framework PRISM Workflow



An agency organizational assessment using PRISM would be accomplished through the multi-step process shown in Figure 3A.

1. **Identify Key Risk Areas/Vectors, Component Risk Factors and Prioritization Weighting**—A team of designated organizational experts within the agency will have in-depth knowledge of information and operational security processes. This team will be responsible for identifying agency major risk areas or vectors plus components within each risk area or vector. This team would also assign the priority weighting for each risk area/vector plus focus on reporting findings and making recommendations to senior management for implementation.

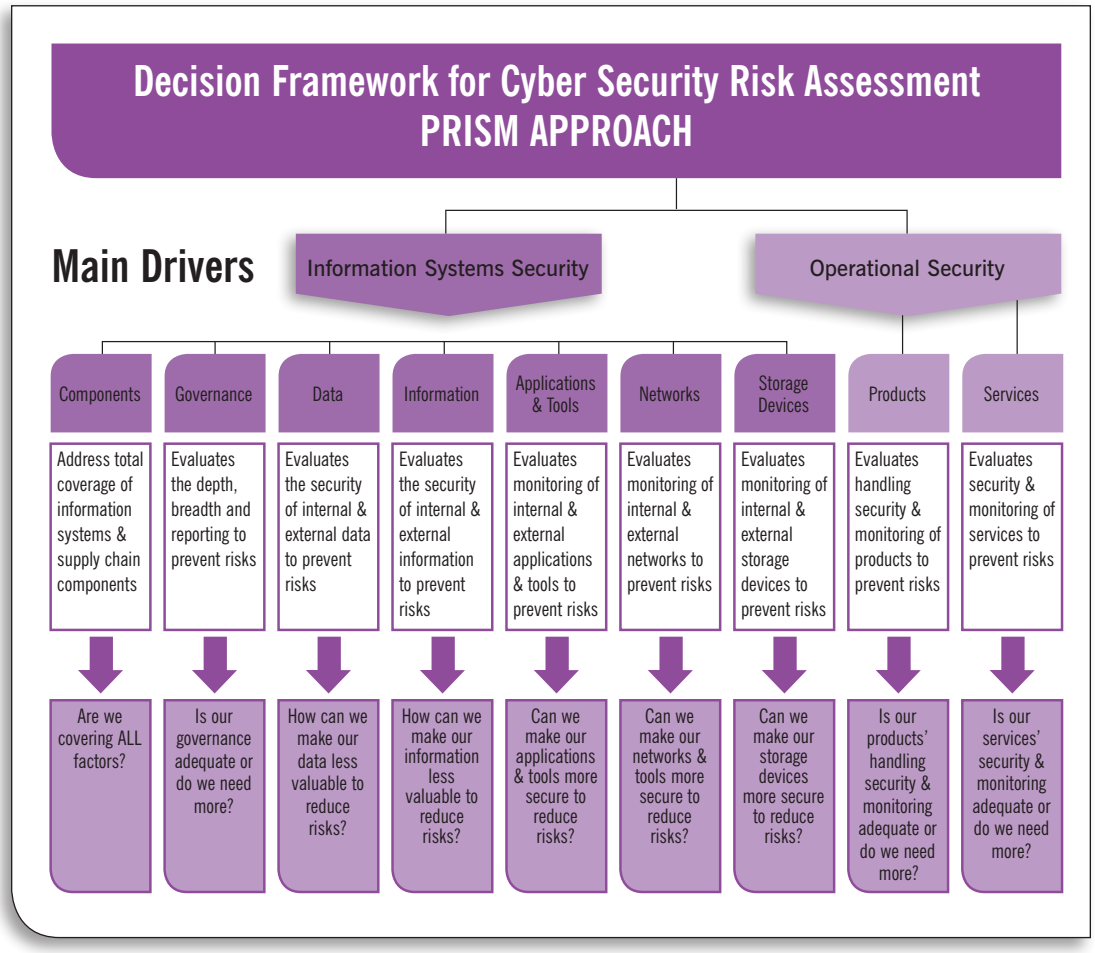
2. **Implementation**—The designated team of experts will, at least annually, review individual cyber factors to determine the agencies' current "stage" of preparedness and responsiveness to risk management.

3. **Resource Allocation**—The organizational experts will examine the agencies' level of commitment/resource allocation on each of the PRISM dimensions with a simple "yes/no" rating. A helpful taxonomy for future resource analysis may come from the Technology Business Management (TBM) Taxonomy used by the Federal CIO Council to allocate technology management costs with activities and outcomes (see https://www.cio.gov/fed-it-topics/sustainability-transparency/tbm).

4. **Risk Rating Level**—A composite "Risk Rating Level" score for each PRISM dimension will be calculated based on binary coding of responses with appropriate weights assigned to each factor. These risk level rating scores can range from 1 to 7. Based on the "Risk Rating Level," the agencies' "Preparedness Level" would be assigned based on a standard taxonomy (e.g., Poor, Fair, Good, Very Good, Excellent).

5. **Standardize and Monitor**—Using both the Risk Rating Level and Preparedness Level, the expert reviewers will make improvement recommendations for each dimension. These recommendations would identify specific changes to implement to move from Stage 1 (Restore) to Stage 2 (Proactive) to Stage 3 (Enterprise) as applicable to each dimension.

Figure 3B. Cybersecurity Decision Framework Detailed Risk Assessment Areas/Vectors & Questions



During the agency organizational assessment, the team of experts would address the key risk assessment questions shown in Figure 3B.

1. **Components and Governance**—The team will be responsible for ensuring that all information systems and supply chain components are included in the assessment. This team would also evaluate the adequacy of agency governance.

2. **Data and Information**—The designated team of experts will review the actual and perceived value of different types of data and information within the agency. This assessment would identify how the agency could make its data and information less valuable to reduce risks.

3. **Applications and Tools**—The team of experts will examine each of the agencies' internal and external applications and tools to identify potential risks. This assessment would identify what the agency could do to make the applications and tools more secure to reduce risks.

4. **Networks**—The team of experts will examine each of the agencies' internal networks and external network interfaces to identify potential risks. This assessment would identify what an agency could do to make their networks more secure to reduce risks.

5. **Storage Devices**—The team of experts will examine each of the agencies' internal and external storage devices to identify potential risks. This assessment would identify what the agency could do to make the storage devices more secure to reduce risks.

6. **Operational Products and Services**—The team of experts will examine all the agencies' internal and external operational products to identify potential risks (e.g., laptops, desktops, phones, etc.) In addition, the team will examine all the agencies' internal and external operational services to identify potential risks (e.g., help desk, database access, etc.) This assessment would identify what an agency could do to make the operational products and services more secure to reduce risks.

PRISM Model Validation

Based on interviews with various industry CIOs conducted for this report and a PricewaterhouseCoopers study of 1,581 corporate executives released in April 2017,[18] the following key findings were identified by the respondents. The PRISM Key Risk Areas were consistent with the top security threat areas identified in Figure 3B.

18. "PWC Risk in Review–Managing Risk from the Front Line–6th Annual Survey of Corporate Executives" *Wall Street Journal,* April 18, 2017.

Top Security Threat/Risk Areas (Figure 3B)

- Information Systems Security–Internal and External
  - Components
  - Governance
  - Data
  - Information
  - Applications/Tools
  - Networks
  - Storage Devices
- Operational Security–Internal and External
  - Products
  - Services

Top Critical Risk Factors

- Financial–Pricing and Customer Data
- Legal/Regulatory–Compliance and Implementation
- Organization & Resources–Designated Department/Group, Responsibilities, and Segregation of Duties
- Strategic/Governance–Standardization of Policies, Procedures, and Processes
- Compliance–Monitoring, Controls, and Reporting
- Reputation/Brand–Prioritization of Disaster Preparation, Remediation, and Implementation Responsiveness
- Third Parties–Interfaces with Customers, Suppliers, and Stakeholders
- Information Systems–Architecture, Networks, Connectivity, and Communications
- Technology–Applications, Tools, Networks, and Storage Devices

Risk Management Strategies and Implementation Response Priorities

- Security and risk culture is at the forefront of successful organizations, accepted by senior management, board of directors, business units, and all employees
- Understanding risk areas that need improvement and building agility and resilience to mitigate risk events, enabling long-term success
- Ability to be proactive and predictive, consistent with successful Enterprise Risk Management
- Valuing critical assets and data helps prioritize focus on specific risk drivers

PRISM Application Exemplified

In applying the PRISM decision model, a government agency cybersecurity risk that the framework would proactively address is the significant number of *"loss or theft of equipment"* incidents reported in the FY2016 FISMA report to Congress (e.g., 5,690 incidents, which was the highest level excluding the "Other" risk vector). While the FISMA FY2016 report indicates agencies are working on this risk area, only 61 percent of all agencies have made progress toward safeguarding their high value information technology assets.

Figure 4 displays a simulated example for Laptops and Backup Drives. This encompasses the "Loss or Theft of Equipment and External/Removable Media Risk Areas/Vectors" identified in the FISMA FY2016 report. Using PRISM to walk through the stages in this decision framework, reviewers would enter responses and calculate their Risk Rating Level along with the Preparedness Level for each dimension.

Figure 4. Example Cybersecurity Decision Framework for Laptops & Backup Devices "Storage Devices Risk Areas/Vectors"

Cyber Security Evaluation Enhanced PRISM Framework - Stages of Preparedness Example Information Systems and Operational Security											
					<--- Implementation Responsiveness --->						
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)	Preparedness Level (See Legend)
Detailed Risk Areas/Vectors Analysis:											
Storage Devices											
	Laptops	Failure to secure & monitor Agency and Employee Laptops to prevent risks	No	Yes	Assigned asset Stored/ Carried in personal computer case with personal password updated periodically Yes	Assigned asset Stored/ Carried in locked personal computer case with laptop password updated every 90-days No	Assigned asset Stored/ Carried in locked agency computer case, encrypted hard drive with password updated every 30-days No	No	No	2	Poor
	Backup Drives	Failure to secure & monitor Agency and Employee Backup Drives to prevent risks	Yes	Yes	Personal device used with assigned asset Stored/ Carried in personal computer case used with other assets No	Agency assigned asset Stored/ Carried in locked personal computer case only used on assigned asset Yes	Agency Assigned asset Stored/ Carried in locked agency computer case, encrypted backup drive only used on assigned asset - No	Yes	Yes	6	Very Good

LEGEND: Risk Rating Level and Preparedness Level. 1=Poor, 2=Poor, 3=Fair, 4=Fair, 5= Good, 6=Very Good, 7=Excellent

The following examples highlight potential benefits of applying PRISM in a retrospective analysis of cybersecurity incidences at state and federal agencies.

1. **A State Case**—In 2011, the Texas Comptroller's office revealed a breach of 3.5 million Texan's personal information that had inadvertently been kept on a publicly accessible state server. In applying PRISM, the activity of prioritization to include securing sensitive data would have led the CIO to request a risk-based report on how data is secured across various servers and platforms. Data resident on a public server would have raised the risk priority and called for further action. Furthermore, it would have precipitated a statewide review to ensure any such exposed data was secured appropriately, and standardization and monitoring processes would have been put in place to preclude future occurrences.

2. **A Federal Case**—One of the largest data breaches of federal personal information was at the Office of Personnel Management (OPM). In mid-2015, the OPM announced it had discovered two separate (but linked) intrusions compromising unencrypted data that affected an estimated 21.5 million people. Proper identification of risk levels (levels of preparedness across main risk drivers) and appropriate allocations of available resources to prioritized risks would have enabled OPM to provide better responsiveness. Implementation of FISMA guidance including the RMF, and application of the PRISM model, would have prioritized the risk with an appropriate level of urgency assigned to mitigation strategies. More importantly, PRISM would also advocate strategies around standardization that might prevent repetition of similar intrusions and attacks/intrusions affecting multiple parts of the agency.

3. **Two Examples of Simple Oversight**—While resources are tied up in complex design and deployment of sophisticated infrastructure to protect sensitive information, often a simple oversight results in significant cybersecurity consequences. In 2009, for example, the National Archives shipped a malfunctioning hard drive containing sensitive data on veterans to a contractor for repair, compromising the personal information of 76 million veterans. In another case, in 2015, an incorrectly configured database exposed on the open Internet compromised data on 191 million voters. Given the overwhelming anecdotal evidence pointing toward issues around oversight and management, PRISM would serve as a key framework for establishing a cyber strategy supported by underlying processes for managing cyber risk.

SUMMARY

In response to the exponential growth of cyber threats, agencies/organizations have applied a variety of frameworks and/or approaches to address different supply chain performance, enterprise risk management, and cybersecurity problems.

However, a single process to help agencies/organizations identify the best approach to addressing supply chain performance, risk management, and cybersecurity problems does not exist currently across all agencies/organizations. To improve the ability of IGs, CIOs, and others to address problems, the opportunity exists to create a methodology for cross-agency cybersecurity risk management. Cyber resilience requires a strategic approach that includes a methodology to bring awareness of the risk levels in securing prioritized assets, and a system to counter risks with appropriate mitigation and monitoring resourcing.

Evaluating problems through a single decision matrix creates an opportunity to harmonize different approaches across agencies. Our proposed cybersecurity evaluation PRISM model will help agencies/organizations identify and implement the most tailored risk management and cybersecurity approach applicable to their problem(s). Our proposed model can also be used by agencies/organizations to set priorities, to explore gaps in current processes, and to steer an organization in the right direction to resolve risk management and cyber risks specific to an organizational strategy and its functions. Risk management and cybersecurity areas/vectors would be evaluated by the agency/organization using quantitative values to identify the best approach to resolve current or evolving problems. These characteristics drive critical conversations, evaluation, and ultimately decision making about appropriate, tailored approaches to resolve risk management and cybersecurity problems in agencies/organizations.

APPENDICES:

Appendix A summarizes the detailed analysis in Appendix B, which covers the nine Key Risk Areas/Vectors. Appendix C lists the documents used for content analysis that underlies the PRISM Model.

Appendix B also identifies the primary risk factors within each Risk Area/Vector that agencies/organizations need to focus on to enhance their risk management preparedness and responsiveness. Columns C through K of Appendix B provide information that designated agency experts can leverage when assessing an agencies' current risk management status. This would also enable identifying agency actions necessary to mature in their cyber risk management posture, moving from Stage 1 (reactive) to Stage 2 (proactive) to Stage 3 (enterprise) during the implementation phase of the PRISM framework.

The Detailed Risk Areas/Vectors Analysis (Appendix B) roll-up to the Summary Risk Areas/Vectors Analysis (Appendix A) for identification of the Key Risk Areas/Vectors that need improvement. The agencies would use this scorecard to prioritize and identify the precise risk vectors, to leverage existing standards (as described earlier) to resource, and to operationalize a strategy to mitigate the risks.

Appendix A–"Summary" risk driver analysis

Cyber Security Evaluation Enhanced PRISM Framework - Stages of Preparedness											
Information Systems and Operational Security					<--- Implementation Responsiveness --->						
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/ Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/ Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)	Preparedness Level (See Legend)
Summary Risk Driver Analysis:											
Information Systems & Supply Chain Components	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
Governance	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
Data	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
Information	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
Applications/ Tools	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
Networks	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
Storage Devices	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
Products	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
Services	Internal	Adequacy of Actions/Activities									
	External	Adequacy of Actions/Activities									
		"Yes" Subtotal:									

LEGEND: Risk Rating Level and Preparedness Level. 1=Poor, 2=Poor, 3=Fair, 4=Fair, 5= Good, 6=Very Good, 7=Excellent

Appendix B–Detailed Risk Driver Analysis: Information Systems & Supply Chain Components

Detailed Risk Driver Analysis:											
Information Systems and Operational Security					<--- Implementation Responsiveness --->						
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/ Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/ Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No = 0 (1 to 7)	Preparedness Level (See Legend)
Information Systems & Supply Chain Components											
	Organization: Responsibilities - Labor	Individual/Team actions or activities that contribute to cyber security risks									
	Segregation of Duties	Disparate Duties that create monitoring voids or coordination failures									
	Legal/Regulatory	Failure to implement Legal & Regulatory requirements to prevent risks									
	Controls (e.g., Enterprise, Individual, etc.)	Failure to implement adequate Controls that contributes to risks									
	Interfaces - Customers, Suppliers, Regulatory	Various Interfaces that are not secure that contributes to risks									
	Testing (e.g., Penetration)	Failure to perform adequate Testing to prevent risks									
	Assets (e.g., Buildings, IT, People, etc.)	Adequacy of Asset management practices to prevent risks									

Appendix B–Detailed Risk Driver Analysis: Governance

Detailed Risk Areas/Vectors Analysis:					<--- Implementation Responsiveness --->					
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/ Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/ Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)
Governance										
	Strategy/ Strategies	Failure to implement a Strategy or Strategies to prevent risks								
	Policies / Standards	Failure to establish Policies & Standards to prevent risks								
	Functions and Programs	Failure to create Functions & Programs to prevent risks								
	Controls	Failure to establish Controls to prevent risks								
	Reporting	Failure to establish Reporting to prevent risks								
	Compliance	Failure to monitor Compliance to prevent risks								
	Technology Innovations	Failure to monitor Technology Innovations to prevent risks								
	Remediation Procedures	Failure to establish Remediation Procedures to mitgate or prevent risks								
	Stakeholders	Failure to establish appropriate procedures for Stakeholders								
	Reputation	Failure to establish procedures to manage Reputation								
	Finances	Failure to establish procedures to manage Finances								
	Hazards (e.g., Liability, Theft, Fire)	Failure to establish general Hazard Procedures to mitgate or prevent risks								
	Other Risks	Failure to establish basic procedures to mitgate or prevent risks related to Other Risks not currently defined in general								

Appendix B–Detailed Risk Driver Analysis: Data

Detailed Risk Areas/Vectors Analysis:					<--- Implementation Responsiveness --->					
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)
Data										
	Pricing	Failure to secure Pricing Data to prevent risks								
	Financial	Failure to secure Financial Data to prevent risks								
	Customers	Failure to secure Customer Data to prevent risks								
	Suppliers	Failure to secure Supplier Data to prevent risks								
	Operational	Failure to secure Operational Data to prevent risks								
	Value	Failure to identify the Value of Data to prevent risks								

Appendix B–Detailed Risk Driver Analysis: Information

Detailed Risk Areas/Vectors Analysis:					<--- Implementation Responsiveness --->					
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)
Information										
	General - Public	Failure to secure Public Information to prevent risks								
	Confidential - Internal HR	Failure to secure HR Information to prevent risks								
	Confidential - External Credit Card	Failure to secure External Information to prevent risks								
	Confidential - Trade Secrets (IP)	Failure to secure Trade Secrets to prevent risks								
	Confidential - Contract Terms	Failure to secure Contracts Information to prevent risks								
	Value	Failure to identify the Value of Information to prevent risks								

Appendix B–Detailed Risk Driver Analysis: Applications/Tools

Detailed Risk Areas/Vectors Analysis:					<--- Implementation Responsiveness --->					
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)
Applications/ Tools										
	Email	Failure to secure & monitor Email systems to prevent risks								
	Websites	Failure to secure & monitor Websites to prevent risks								
	URLS	Failure to secure & monitor URLS to prevent risks								
	Social Media	Failure to secure & monitor Social Media systems to prevent risks								
	SPAM	Failure to monitor SPAM Threats to prevent risks								
	Viruses	Failure to monitor Virus Threats to prevent risks								
	Malware	Failure to monitor Malware Threats to prevent risks								
	Restriction of Service	Failure to monitor Restriction of Service Threats to prevent risks								
	Internet - General	Failure to monitor Internet Interfaces plus Industry Advisories to prevent risks								

Appendix B–Detailed Risk Driver Analysis: Networks

Detailed Risk Areas/Vectors Analysis:					<--- Implementation Responsiveness --->					
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)
Networks										
	Internal - Infrastructure	Failure to secure & monitor Internal Networks to prevent risks								
	External - Infrastructure	Failure to secure & monitor External Networks to prevent risks								
	Connectivity	Failure to secure & monitor Internal & External Network Connectivity to prevent risks								
	Communications	Failure to secure & monitor Internal & External Network Communications to prevent risks								
	Architecture	Failure to establish & implement Network Architecture to prevent risks								

Appendix B–Detailed Risk Driver Analysis: Storage Devices

Detailed Risk Areas/Vectors Analysis:					<--- Implementation Responsiveness --->					
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)
Storage Devices										
	Local Servers	Failure to secure & monitor Local Servers to prevent risks								
	Cloud - Public	Failure to establish secure & monitor Public Cloud Devices to prevent risks								
	Cloud - Private	Failure to establish secure & monitor Private Cloud Devices to prevent risks								
	Laptops	Failure to secure & monitor Agency and Employee Laptops to prevent risks								
	Desk Tops	Failure to secure & monitor Agency and Employee Desk Tops to prevent risks								
	Tablets	Failure to secure & monitor Agency and Employee Tablets to prevent risks								
	Mobile Phones/ Devices	Failure to secure & monitor Agency and Employee Mobile Phones to prevent risks								
	Backup Drives	Failure to secure & monitor Agency and Employee Backup Drives to prevent risks								

Appendix B–Detailed Risk Driver Analysis: Products

Detailed Risk Areas/Vectors Analysis:					<--- Implementation Responsiveness --->					
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)
Products										
	Materials (e.g., raw, semi- finished, finished, intransit)	Failure to secure & monitor Agency Materials to prevent risks								
	Components	Failure to secure & monitor Agency Components to prevent risks								
	Classification	Failure to establish & monitor Agency Product Classifications to prevent risks								
	Quality	Failure to establish & monitor Agency Product Quality levels to prevent risks								
	Reliability	Failure to establish & monitor Agency Product Reliability levels to prevent risks								
	Counterfeits	Failure to monitor Product Counterfeits to prevent risks								
	Value	Failure to maintain Product Values to prevent risks								

Appendix B–Detailed Risk Driver Analysis: Services

Detailed Risk Areas/Vectors Analysis:					<--- Implementation Responsiveness --->					
Key Risk Areas/ Vectors	Risk Factors (Internal/ External)	Risk Factor Relevance to Cyber Security	Prioritization Risk Areas/Vectors Weighted? (Yes/No)	Resources Allocated to Risk Areas/Vectors? (Yes or No)	Stage 1 "Reactive" Risk Management	Stage 2 "Proactive" Risk Management	Stage 3 "Enterprise" Risk Management	Standardization Knowledge and Solutions Institutionalized? (Yes or No)	Monitoring Constantly Assess Unusual Behavior? (Yes or No)	Risk Rating Level Yes = 1, 2 or 3 & No =0 (1 to 7)
Services										
	Activities and/ or Actions	Failure to secure & monitor Agency Services to prevent risks								
	Processes	Processes to prevent risks								
	Assessments - General or Specific	Failure to establish & monitor Service Assessments to prevent risks								
	Quality	Failure to establish & monitor Service Quality levels to prevent risks								
	Reliability	Failure to establish & monitor Service Reliability levels to prevent risks								
	Systems	Failure to monitor Service Systems to prevent risks								
	Deliverables	Failure to monitor Service Deliverables/Delivery to prevent risks								
	Value	Failure to maintain Service Values to prevent risks								

Appendix C – List of documents used for content analysis

Title (Organization/Firm)	Source
Using Risk Modeling & Attack Simulation for Proactive Cybersecurity Predictive Solutions for Effective Security Risk Management (Skybox Security)	www.skyboxsecurity.com
Managing Information Security Risk (NIST: 800-39)	https://csrc.nist.gov/publications/detail/sp/800-39/final
Electricity Subsector Cybersecurity Risk Management Process (U.S. Department of Energy: DOE/OE-0003)	https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf
Healthcare's Model Approach to Critical Infrastructure Cybersecurity (HITRUST)	https://hitrustalliance.net/content/uploads/2015/09/ImplementingNISTCybersecurityWhitepaper.pdf
A Threat-Driven Approach to Cybersecurity (Lockheed Martin)	https://pdfs.semanticscholar.org/be09/f7a16eb4a379e698d8f42100fd8a91943a0c.pdf
Cyber program management—Identifying ways to get ahead of cybercrime (Ernst & Young)	http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf
Threat smart: Building a cyber resilient financial institution (PwC)	https://www.pwc.com/us/en/industries/financial-services/library/viewpoints/cyber-resilient-financial-institution.html
Defining a Cybersecurity Model for Operational Excellence (Accenture)	https://www.accenture.com/t00010101T000000Z__w__/au-en/_acnmedia/PDF-10/Accenture-Defining-Cyber-Security-Model-Operational-Excellence.pdf
The Five Critical Attributes of Effective Cybersecurity Risk Management (Crowe Horwath)	https://www.crowehorwath.com/Website/SiteTemplates/template-main.aspx?id=12069
Cybersecurity and universities: managing the risk (Universities U.K.)	http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf
Competency Models for Enterprise Security and Cybersecurity (Apollo Education Group)	http://www.apollo.edu/content/dam/apolloedu/microsite/security_industry/AEG-UOPX%20Security%20Competency%20Models%20report.pdf
Partnering for Cyber Resilience Towards the Quantification of Cyber Threats (World Economic Forum)	http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf
Approaching Cyber Risk Management Model (Quality Solutions)	https://www.dis.uniroma1.it/~querzoni/corsi_assets/1516/SystemsAndEnterpriseSecurity/Cyber_Risk_Management16122015.pdf
Cybersecurity Risk Management and Best Practices (The Communications Security, Reliability and Interoperability Council IV Working Group 4 Final Report)	https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf
Cybersecurity Management Programs (CISCO)	
CyberM^3 Cyber Threat Landscape Requires New Approach to Measuring, Managing, and Maturing Cybersecurity (Booz Allen Hamilton)	https://www.boozallen.com/e/insight/publication/cyberm3-measure-manage-and-mature.html
Cybersecurity Maturity (FFIEC Cybersecurity Assessment Tool)	https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Cybersecurity_Maturity.pdf
A framework for cybersecurity information sharing and risk reduction (Microsoft)	http://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf
A Taxonomy of Operational Cybersecurity Risks (Software Engineering Institute)	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9395
Cybersecurity Compliance Basics: Taking a Proactive Approach to Protecting Your Company's Information (Workplace Answers)	www.workplaceanswers.com

Title (Organization/Firm)	Source
Dynamic Deception for Industrial Automation and Control Systems (Attivo Networks)	https://attivonetworks.com/documentation/Attivo_Networks-Dynamic_Deception_IACS.pdf
Boardroom Cyber Watch Survey 2014 Report (IT Governance Ltd.)	www.itgovernance.co.uk
Guide to Information Security Controls Frameworks (CEB)	www.cebglobal.com
Examining the costs and causes of cyber incidents (Journal of Cybersecurity)	Journal of Cybersecurity, 2016, 1–15 doi: 10.1093/cybsec/tyw001
DHS Risk Lexicon 2010 Edition (Department of Homeland Security)	https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf
Cyber Risk Report 2016 (Hewlett Packard Enterprise)	https://www.thehaguesecuritydelta.com/media/com_hsd/report/57/document/4aa6-3786enw.pdf
Human Behaviour as an aspect of Cybersecurity Assurance (Cornell University Library)	https://arxiv.org/ftp/arxiv/papers/1601/1601.03921.pdf
Insurability of Cyber Risk: An Empirical Analysis	https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf
The swinging pendulum: Board governance in the age of shareholder empowerment	http://www.lexissecuritiesmosaic.com/gateway/sec/speech/assets_pwc-2016-annual-corporate--directors--survey.pdf
The Human Point. An Intersection of Behaviors, Intent & Critical Business Data (Forcepoint by Raytheon)	https://www.forcepoint.com/sites/default/files/resources/files/report-fp-human-point-survey.pdf
How Much Is Enough? A Risk-Management Approach to Computer Security (CRISP)	http://www.cl.cam.ac.uk/~rja14/econws/06.doc
2016 Data Breach Investigations Report (Verizon)	https://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

ABOUT THE AUTHOR

RAJNI GOEL

Dr. Rajni Goel is a Professor and former Chairperson of the Information Systems and Supply Chain Management Department in the School of Business at Howard University. Dr. Goel served as a Fulbright-Nehru Scholar in India, conducting research and assisting in curriculum development in the area of Cyber security. She currently serves as the Director of Research of the Howard University Cyber-Security Education and Research Center (CERC), assisting with it's establishment and funding from industry and government entities. Dr. Goel participates as a panelist in various forums where she enjoys discussing Business of Cyber Security, diversity of thought and careers for developing a robust Cyber-Security ecosystem. She has served as Cyber-Security Speaker in Malaysia as part of the U.S. Department of State's International Information Programs.

She holds a Ph.D. in IT (Dissertation in Information Security), an M.S. (Mathematics), and a B.A. (Mathematics) and began her career as a High School Mathematics teacher. Upon joining Howard University, she significantly impacted the establishment of the Cyber Security Education and Research Center, including assisting Howard University to become designated as a NSA Center of Excellence in Information Assurance. She has developed new teaching pedagogy in experiential learning and is distance learning certified.

Dr. Goel actively participates in government grants and projects ranging from topics of Railway security to Cyber Risk Management. Her research interests range from information security, railway security, RFID privacy, enterprise security, to supply chains and curriculum development. She has published on these topics in journals such as Journal of Computer Security and, International Journal of Strategic Management, Innovations in Systems and Software Engineering and Journal of Transportation Technologies.

JAMES HADDOW

James Haddow (Jim) is Director of the Center for Excellence in Supply Chain Management in the School of Business at Howard University in Washington DC. Currently, Jim teaches a range of supply chain management courses for both undergraduate and graduate level students. His interests also include national and global operational and information system risk management. Jim has made supply chain presentations at ISM, IMC, APICS, PMAC and other Global industry conferences over the last several years.

A career of more than 30 years of consulting and industry experience encompassing global procurement, supply chain management, supply chain operations, business planning and commercial business development provides hands-on teaching examples for his students. Jim retired as Director of Global Procurement (Chief Procurement Officer) for global consulting firm.

A University of Maryland graduate, Jim earned a B.S. in Business and Management as well as an MBA with a concentration in Logistics. His industry affiliations include ISM, APICS and AAWC in addition to his service on the Boards of several local community and national organizations in various roles including Treasurer, Executive Vice President and President.

ANUPAM KUMAR

Dr. Anupam Kumar teaches at Howard University. He has over a decade of consulting experience working for firms such as IBM, PricewaterhouseCoopers LLC, and Parsons Engineering and Science, Inc. He led the Public Sector Supply Chain Planning group at IBM. His expertise spans data management, business intelligence, and business analytics.

Dr. Kumar's research has been published in International Journal of Production Economics, Journal of Strategy and Management, Corporate Reputation Review, Journal of Supply Chain Management and other academic outlets. His primary research focuses on drivers of corporate social responsibility. Dr. Kumar's research portfolio also includes cybersecurity risks, inventory management, and the intersection of supply chain performance with policy in government contracting.

Dr. Kumar received a BS in Civil Engineering from Indian Institute of Technology, Kanpur in 1989, an MS in Environmental Engineering from Oklahoma State University in 2000, an MS in Applied Statistics from George Mason University in 2006, and a Doctorate in Business and Management from the University of Maryland in 2014.

KEY CONTACT INFORMATION

To contact the author:

Rajni Goel Ph.D.

Professor & Fulbright Scholar
Information Systems & Supply Chain Management

Howard University School of Business

2600 6th St NW

Washington, DC 20059

Phone: (202) 806-1649

rgoel@howard.edu

Jim Haddow

Director, Center for Excellence in
Supply Chain Management

Howard University School of Business

2600 6th Street, NW – Room 452

Washington DC 20059

Phone: (202) 806 1604

james.haddow@Howard.edu

Anupam Kumar, Ph.D.

Assistant Professor, Dept. of Information Systems
and Supply Chain Management

Howard University School of Business

2600 6th Street NW

Washington DC, 20059

Phone: (202) 806-1603

anupam.kumar@howard.edu

REPORTS FROM THE IBM CENTER FOR THE BUSINESS OF GOVERNMENT

For a full listing of our publications, visit www.businessofgovernment.org

Recent reports available on the website include:

Acquisition

Ten Actions to Improve Inventory Management in Government: Lessons From VA Hospitals by Gilbert N. Nyaga, Gary J. Young, and George (Russ) Moran
Beyond Business as Usual: Improving Defense Acquisition through Better Buying Power by Zachary S. Huitink and David M. Van Slyke

Collaborating Across Boundaries

Cross-Agency Collaboration: A Case Study of Cross-Agency Priority Goals by John M. Kamensky
Interagency Performance Targets: A Case Study of New Zealand's Results Programme by Rodney Scott and Ross Boyd

Improving Performance

Seven Drivers Transforming Government by Dan Chenok, Haynes A. Cooney, John M. Kamensky, Michael J. Keegan, and Darcie Piechowski
Five Actions to Improve Military Hospital Performance by John Whitley

Innovation

Tiered Evidence Grants - An Assessment of the Education Innovation and Research Program by Patrick Lester
A Playbook for CIO-Enabled Innovation in the Federal Government by Gregory S. Dawson and James S. Denford
Making Open Innovation Ecosystems Work: Case Studies in Healthcare by Donald E. Wynn, Jr., Renée M. E. Pratt, and Randy V. Bradley
Laboratories of Innovation: Building and Using Evidence in Charter Schools by Patrick Lester

Leadership

Best Practices for Succession Planning in Federal Government STEMM Positions by Gina Scott Ligon, JoDee Friedly, and Victoria Kennel

Risk

Risk Management and Reducing Improper Payments: A Case Study of the U.S. Department of Labor by Robert Greer and Justin B. Bullock
Ten Recommendations for Managing Organizational Integrity Risks by Anthony D. Molina

Using Technology

Delivering Artificial Intelligence in Government: Challenges and Opportunities by Kevin C. Desouza
Using Artificial Intelligence to Transform Government by The IBM Center for The Business of Government and the Partnership for Public Service
Digital Service Teams: Challenges and Recommendations for Government by Ines Mergel
Ten Actions to Implement Big Data Initiatives: A Study of 65 Cities by Alfred T. Ho and Bo McCall
A Roadmap for IT Modernization in Government by Dr. Gregory S. Dawson

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.

IBM Center for
The Business of Government

20 years of research for government:
informing today, envisioning tomorrow

1998-2018