This article is adapted from Dr. Rajni Goel, James Haddow, and Dr. Anupam Kumar, Managing Cybersecurity Risk in Government: An Implementation Model *(Washington, D.C., IBM Center for The Business of Government, 2018)*

Managing Cybersecurity Risk in Government: An Implementation Model

By Dr. Rajni Goel, James Haddow, and Dr. Anupam Kumar

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. Diverse agency data stores extend the source of risk throughout government organizations, bringing the need for new approaches that move beyond traditional security precautions. Cyberattacks against government are becoming more common and have more severe impact.

In a new report from the IBM Center for The Business of Government, *Managing Cybersecurity Risk in Government: An Implementation Model,* we address cybersecurity risk management needs by developing a decision model that allows agencies to tailor approaches for particular cyber challenges. We 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. We 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.

The PRISM model can lead agencies to make intelligent choices about how best to address cyber risk. The model helps agencies begin by prioritizing risk drivers and interdependencies, and by linking cybersecurity goals to mission and operational objectives. The model can also assist agencies in communicating return on security investments to mitigate cyber risks. Such communications can foster discussion, assessment, and decisions and actions to tailor approaches for addressing cyber risk management in government.

Understanding Cybersecurity Risk Management

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.

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). 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.

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. This exemplifies the need for a tailored cybersecurity risk management framework that aligns with organizational priorities.

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.* ***James Haddow*** *(Jim) is Director of the Center for Excellence in Supply Chain Management in the School of Business at Howard University.* ***Dr. Anupam Kumar*** *Assistant Professor, Dept. of Information Systems and Supply Chain Management at Howard University.*

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 non-connected intranet is expensive and could stymie innovation and efficiencies that occur by leveraging solutions developed on the open Internet. And recent incidents highlight the challenges in maintaining a cybersecurity posture that can defend against every possible attack scenario, when the avenues of attacks are proliferating faster than organizational response times in deploying safeguards.

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.

In 2013, the continuation of cyberattack losses led to issuance of Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, and the National Institute of Standards and Technology (NIST) released the Cybersecurity Framework. 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. Along with requirements under the Federal Information Security Management Act (FISMA), the NIST Framework provides agencies with a common structure for top-level controls and many variations, both within and across federal agencies and with private sector partners.

Agencies face multiple challenges in addressing cybersecurity risk.

- Competing and detailed frameworks make prioritization and strategic decision making a challenge.
- 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.
- Inadequate resources to manage cybersecurity risk also persist, and the lack of strategy leads to sub-optimal deployment of available resources.
- Across and within agencies, a lack of standardization and information sharing results in weaknesses and risks that could otherwise be mitigated.
- 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, this report proposes a decision matrix framework to identify appropriate approaches to resolve these problems, building on a significant body of knowledge regarding cyber risk that currently exists in the form of industry white papers and academic research.

Decision Model for Cybersecurity Risk Assessment: The PRISM Approach

This report finds that there is a need for a strategic framework to aid in developing and maintaining a cybersecurity strategy at the enterprise level. The authors performed a meta-analysis of the existing body of knowledge to harvest key elements of cybersecurity risk management. This leads to the five emergent themes of Prioritize, Resource, Implement, Standardize, and Monitor, or PRISM, from which content analysis supporting the proposed operational model allows for a tailored approach to cybersecurity risk management.

The PRISM model complements the FISMA process by addressing additional implementation components critical for cyber risk assessment and management.

Key elements of the PRISM decision model are intended to help improve an agency's cybersecurity posture, preparedness, and responsiveness.

- **Prioritize.** Agencies 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.

- **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, personnel, technology, and/or other resources necessary to address and resolve a cybersecurity risk area, factor, or vector.

- **Implement.** Agencies should rapidly detect and destroy viruses and other forms of malware introduced in their ecosystem.

- **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. 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.

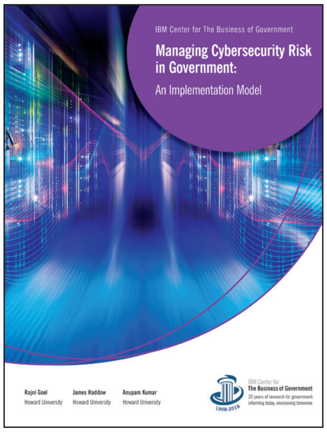
Summary—Contributions to Better Cyber Risk Decision Making

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 framework 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 in agencies and cybersecurity problems in organizations.

TO LEARN MORE

Managing Cybersecurity Risk in Government: An Implementation Model
By Dr. Rajni Goel, James Haddow, and Dr. Anupam Kumar


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
1998-2018

The report can be obtained:

- In .pdf (Acrobat) format at the Center website, **businessofgovernment.org**
- By e-mailing the Center at **businessofgovernment@us.ibm.com**
- By calling the Center at **(202) 551-9342**