Carnegie Mellon University
Software Engineering Institute

Summer Fowler
Technical Director, Risk & Resilience, CERT Division
Carnegie Mellon University's Software Engineering Institute

Hearing on "Assessing the State of Federal Cybersecurity Risk Determination"
Before the Subcommittee on Cybersecurity and Infrastructure
United States House of Representatives Committee on Homeland Security
July 25, 2018

Chairman Ratcliffe and Ranking Member Richmond, thank you for the opportunity to participate in this hearing on assessing cybersecurity risk. I am the Technical Director of Cybersecurity Risk and Resilience for the CERT Division, part of Carnegie Mellon University's Software Engineering Institute (SEI)[1], a Department of Defense (DoD) Federally Funded Research and Development Center (FFRDC). The SEI conducts research and development in software engineering and cybersecurity, working to transition new and emerging innovations into government and industry. The SEI holds a unique role as a FFRDC sponsored by the DoD that is also authorized to work with organizations outside of the DoD, including engagement across the federal government, the private sector, and academia. As such, we have been working with Department of Homeland Security's critical infrastructure protections since they were established in 2013. Our research, prototyping, mission application, training, and education activities are heavily interrelated and are relevant to a broad range of problem sets, such as protection of the nation's critical infrastructure and improved software engineering for large-scale systems of systems.

Disruptions of critical functions that are reliant on computer systems are inevitable. No organization, government, or agency can anticipate every disruption or prevent every cyber attack. Agencies must be able to anticipate and respond to changes in their risk environment at a moment's notice. Furthermore, despite these disruptions, organizations should be capable of continuing operations and meeting mission goals.

We at the SEI applaud the work of the Office of Management and Budget, detailed in the May 2018 report "Federal Cybersecurity Risk Determination Report and Action Plan." As a high-level assessment of government cybersecurity risks, the report identifies four core actions that I believe will indeed, done correctly, mitigate a significant number of cyber risks across the federal agencies.

[1] https://www.sei.cmu.edu/

Notwithstanding, there are some finer points, not included in the report that are worth discussing and implementing. First, the report concentrates on only one half of cyber risk management. In order to successfully execute cyber risk management, agencies must ensure they analyze and manage cyber risk or threats as well as the potential impact of the cyber risks and threats on their organization. While the report concentrates on the threat of cyber security and proposes better understanding of the cyber risk, outlining the potential effect of any realized threat requires just as much effort[2]. If agencies are to achieve the ability to complete their mission no matter the cyber threat, it is imperative that we manage both the cyber threat and the consequences of the attacks.

Accomplishing this continuity of operations requires a **resilience** approach to cybersecurity—an integrated, holistic way to manage security risks, business continuity, disaster recovery, and IT operations, executed in the context of each organization's mission and strategy.

Second, by the report's own admission, it does not cover older, legacy information technology (IT) or workforce challenges. Both legacy IT and the workforce shortage are significant and must be addressed if the federal enterprise is to understand the current cyber risk environment and credibly prepare for the future.

The SEI's Enterprise Risk and Resilience research includes advancing cyber risk management and enhancing it via the planning, integration, execution, and governance of operational resilience. We leverage our research to develop best practices, resilience management models, tools and techniques for measuring and improving enterprise risk management and operational resilience in the form of actionable guidance for the DoD and federal civilian agencies.

Operational Resilience

Operational Resilience is the ability to continue to operate, and to meet the organization's mission, in the face of evolving cyber conditions. In the ever-changing cyber and technological landscape, organizations need techniques that allow people, processes, and systems to adapt to changing patterns. These patterns include the incessant introduction of both unique threat actors and the means by which systems are exploited. Operational resilience is obtained by ensuring your cyber risk management takes into account both the threat and the consequences of cyber risk.

[2] As reinforced in NIST 800.39, Managing Information Security Risk Organization, Mission, and Information System View and NIST 800.37, Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach

Cyber risk management, as proposed by the report, is a process to identify, analyze, dispose of, monitor, and adjust approaches to handling threats. Yet we know cyber risk management alone is not enough to ensure that we are prepared to address current and emerging threats. The concept of risk management must adhere to formula between likelihood of threat and consequence of impact.

At the SEI we have found cyber risk is best managed by determining potential impact first. This requires articulation of mission, enumeration of critical services or activities to achieve mission, and asset management[3]. Once critical assets are identified, then we can walk back toward a list of specific threat types and threat actors. Cyber professionals whose efforts are concentrated in the assessment of threats are often doing very good cybersecurity work; however, without consideration of impact and asset management, they may not be protecting the assets most critical to that particular organization. Focusing on mission objectives and critical assets creates operational resiliency in an organization regardless of the source or type of threat. This focus on mission context also improves the ability to communicate risk, ultimately helping to address finding number four in the OMB report.

Examining consequences helps organizations to identify and mitigate operational risks that could lead to service disruptions before they occur. Organizations can then prepare for and respond to disruptive events in a way that demonstrates balance of command and control of threat mitigation, incident response, and service continuity. Finally, by establishing a robust understanding of assets, agencies can prioritize investments needed to protect, respond, recover, and restore mission-critical services and operations after an incident and within acceptable time frames.

Considering impact is key for comprehensive cyber risk management leading to resilience. If an agency looks only to malicious threats to operations, it risks missing 17% (one in five) of overall data breaches, which are the result of human error. In the healthcare and information industries, these errors are much higher at 35% and 26% respectively.[4] Organizations cannot overlook the role of humans in the management of cyber risks. A malicious act of deliberate sabotage or the unintentional actions of a confused system operator can both lead to a profound disruption. A resilience approach is agnostic of the type of disruption and enables the organization to plan for, avoid,

[3] Asset management is a collection of practices to identify and prioritize the people, processes, data, technology, and facilities required to execute the activities.
[4] Verizon 2018 Data Breach Investigations Report, https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

detect, respond to, and recover from incidents including natural disasters, human error, or malicious cyber attacks.

Furthermore, in today's ever-increasing global economy, many organizations depend on external entities for information and technology, increasing the potential risk to their missions and key services. These third-party entities are an extension of the organization and are often given a trusted place in the management of systems and processes. When trust in an external entity is misplaced or misused, the consequences can be significant. Examples include breaches due to a third party's failure to protect data, poor integrity of hardware and software deployed within an organization, or malicious use of trusted extrinsic relationships to gain access to or harm the organization. Agencies must approach the management of supply chain, also called third-party or external dependencies, with a risk-based approach. This approach includes adopting new ways of continuously measuring and managing the risk from external dependencies.

Additionally, agencies can and should determine the maturity of their external dependencies-management practices. Guided by specific service-level agreements, which establish meaningful measures of cybersecurity performance, agencies can better understand and manage the capabilities of their external dependencies, thus increasing organizational resiliency. For example, external dependencies management is especially critical as the government continues to modernize its IT capabilities using cloud service providers.

Lastly, for true operational resilience, agencies must move beyond simplistic checklist compliance or penetration testing and take demonstrable steps to improve cybersecurity posture. Our team at Carnegie Mellon University has codified operational resilience in the CERT® Resilience Management Model (CERT®-RMM).[5] Developed by deriving practical tools and methods from the best concepts that academia has to offer and best practices from the public and private sectors, CERT-RMM has been applied to measure and evaluate organizations of all sizes and compositions. Developed initially in collaboration with members of the financial services community, CERT-RMM has been used more than 600 times by the Department of Homeland Security to measure the cyber resilience across all 16 critical infrastructure sectors. CERT-RMM can also be used as a way to measure capabilities against the NIST Cybersecurity Framework. Enabling agencies both to ensure compliance and to show measurable improvement in cybersecurity posture, CERT-RMM provides a resource guide mapped to several industry and government standards.

[5] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

Most importantly, CERT-RMM is a framework that does not require agencies to start over, but allows every organization, whatever its current competence, a way to assess baseline capabilities and develop a roadmap for improvement as an enhancement to cyber risk management. This also enables a way to address the next topic of legacy information technology (IT).

Legacy IT

Organizations do not have unlimited resources with the option of replacing older systems and software en masse to help mitigate new cybersecurity threats. Most, in both government and the private sector, have a mix of old and new systems all connected to each other and most likely accessible to threat actors via the Internet. While layers of safeguards are placed between these systems and the outside world, legacy IT remains a serious concern and has led to many notable cyber breaches despite these defenses. Knowing where the most fragile legacy IT systems are located is essential. Consequently, at a minimum an organization must engage in effective asset management to gain a detailed inventory of IT. Without a valid inventory, accompanied by a network map, it is unlikely any organization could adequately defend itself or have appropriate continuity plans in place. Moving these deprecated legacy systems to a more secure platform, like the cloud, is a valid and appealing option. Asset management practices enable us to prioritize what needs to be moved in order to ensure that our highest priority assets are addressed first. Asset management practices are key ingredients that allow an analysis of the risk and reward of migrating legacy IT to new operating models such as third-party cloud service providers.

Workforce Development

It is not a secret; there is a shortage of experienced and capable cybersecurity personnel. Some studies indicate that the global workforce shortage will reach almost 2 million by 2022.[6]Furthermore, federal agencies face stiff competition from private industry for the limited supply of cyber professionals that do exist. Consequently, organizations need a long-term plan for amplifying their cybersecurity capabilities. Agencies would benefit from an accurate and objective evaluation of their cyber workforce, and with the right methods and technologies, organizations can identify gaps in essential competencies that are unique to their workforce. This allows agencies to make better, targeted, hires as well as continuing education decisions for current employees, resulting in more efficient use of taxpayer dollars. It will take a combination of strategic hiring and developing staff in parallel to meet the need for qualified

[6] https://iamcybersafe.org/gisws/

resources. Programs like Scholarship for Service,[7] which provides tuition and stipends to students studying cybersecurity and related fields, represent a vital pipeline of cybersecurity professionals for the federal government. Agencies should leverage these options, along with partnerships and training such as the Carnegie Mellon University CISO Executive Certificate Program or incident handling courses, to maximum advantage in their workforce development strategies.

Additionally, we need to make cybersecurity an integrated part of our educational curricula starting with our youngest students. Following the 2007 cyberattacks that crippled dozens of its government and corporate sites, Estonia evolved its approach to cybersecurity to include robust educational programs at all age levels and is now recognized as having the best cybersecurity in Europe. In 1961 our nation committed to a dramatic expansion of our space program with a goal of being the first nation to land a human on the moon. Similarly, addressing our cyber risks with the goal of a federal government that is resilient against current and future cyber disruptions requires a national initiative to prepare our workforce. It is essential that we commit to research in emerging areas like artificial intelligence, autonomy, and data analytics methods, and the corresponding training, that will advance our cyber risk management practices in the future.

Conclusion

Cyber risks are not unlike other risks that organizations face. Constrained by limited resources limited resources, we must mitigate cyber risks by addressing both threats and consequences in a balanced way. The goal is to ensure that we are operationally resilient, preserving the ability to achieve our mission, despite any disruptions, such as cyber attacks. To be resilient requires us to understand and prioritize our assets, including technology, data, facilities, as well as people and processes, so that we can invest in the protection and continuity of the assets most critical to our mission. This is a fundamental concept in operational resilience practices that will enhance federal cyber risk management capabilities.

Addressing these challenges and the actions listed in the report is even more necessary as we address the integration and risks of cyber physical systems (CPS) in the federal landscape. Cyber physical systems already exist in manufacturing, healthcare, automotive systems, and financial services to name a few. These CPS systems were often built with functionality as a goal and cybersecurity as a secondary or tertiary consideration at best. The U.S. military and federal government are also integrating

[7] https://www.sfs.opm.gov/ - CMU-SEI is a participating institution

CPS in areas like medical devices in VA hospitals, Internet of Things capabilities in the U.S. Mint, or census collection activities. These capabilities present new attack surfaces for our adversaries and require that we advance our cybersecurity risk management practices with a focus on operational resilience.

Thank you again for the opportunity to participate in this hearing and to discuss how we can better address cyber risks through operational resilience practices.