To: Kevin Stine
National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899

From: The Boston Consulting Group

Re: Input to the Commission on Enhancing National Cybersecurity

Date: September 9, 2016

Dear Mr. Stine,

The Boston Consulting Group is pleased to submit this response to National Institute of Standards and Technology (NIST) Request for Information (RFI) on Current and Future States of Cybersecurity in the Digital Economy. Our response to this RFI focuses on critical infrastructure cybersecurity.

Based on our experience, BCG believes that the single most important recommendation the Presidential Commission can make is to encourage all critical infrastructure organizations to integrate cybersecurity strategy as a fundamental component of their overall organizational strategic plan and planning processes.

We support the work of the Commission and look forward to its recommendations.

Any questions about the content of this response can be directed to Nadya Bartol at Bartol.nadya@bcgplatinion.com or +1 301-503-5278.

Sincerely,

Michael Coden	Nadya Bartol
Head of Cybersecurity Practice	Associate Head of Cybersecurity Practice
BCG Platinion	BCG Platinion

Current technology environment

Today's critical infrastructure (CI) organizations are experiencing a dramatic transition to becoming sophisticated digital organizations of the future. CI organizations such as utilities, healthcare providers, oil and natural gas providers, chemical producers, manufacturers, government agencies, defense, first responders, financial services, or transportation systems, generally own and operate two types of systems and networks – information technology (IT) and operational technology (OT). Simply speaking, IT is what we know of as office systems, while OT comprises the systems that run the CI operation to perform the organization's mission. In the past, OT consisted of stand-alone systems that used obscure proprietary protocols. This resulted in those systems being secure by obscurity. In the last 10 years that has changed. Modern OT systems run on the same software and hardware platforms as IT systems which are well known and understood. The OT systems are no longer stand-alone, they are now connected to the enterprise IT systems, in more or less secure manner.

These changes are driven by:

1. Growing demand to make the data generated by OT available for planning, forecasting, billing, customer service, and other business-related purposes.

2. Phasing out of OT use of proprietary technologies to be replaced by Internet Protocol (IP)-based technologies.

This business demand is driven by customer, regulator, and business stakeholder critical needs. These include the ability to get online information on utility outages and restoration, to remotely adjust a thermostat or medical device from a smart phone, and to remotely monitor transportation, oil and gas, manufacturing, and electricity or water usage to achieve conservation goals.

Although the technology now being used in CI organizations is "smarter," it is also more vulnerable. Expanded feature sets and combining capabilities that were previously provided by several devices into more complex multi-functional devices create greater opportunities for compromise. Where security was not required in the past, it has become increasingly more important. CI organizations have to address new and emerging security expectations while designing, implementing, and maintaining smart systems and networks. Maintaining and securing smart devices requires more time, precision, and knowledge.

Smart networks, digital CI enterprises, and smart cities rely on a variety of devices that are networked, intelligent, and more vulnerable than the older devices. But that is not the only challenge. The increased number of devices exponentially increases the network's attack surface – more devices, more vulnerabilities, more potential points of entry. Moreover, the modern industrial control systems (ICS) and specialized communications devices that now run on many OT networks are better known than in the past and no longer obscure. According to publicly available government and industry reports, many attempts have been made to explore and map OT networks in the U.S., Europe, and other parts of the world, and there is now specific malware that targets ICSs and other critical infrastructure systems.[1][2] The threat actors have become more sophisticated and knowledgeable—just as the systems and networks of CI organizations have become better understood and more accessible.

Challenges

Today's CI organizations have to satisfy current and future business requirements, while managing risks of being exploited by ever better equipped threat agents. This has to happen as their systems and networks are more interconnected and more exposed than ever. That creates a number of cybersecurity challenges, including:

1. Securing CI organizations of the future while business requirements and technology are evolving
2. Availability of qualified workforce that understands how to secure the converged CI enterprise
3. Managing cybersecurity risks associated with supplier relationships
4. Resource and scale disparities among larger and smaller organizations.

Challenge 1. Securing CI organizations of the future while business requirements and technology are evolving

Emerging business, regulatory, and consumer requirements necessitate deployment of increasingly smart and sophisticated technologies. These include renewable and distributed energy generation, smart cities, electric vehicles, and other capabilities that require sophisticated applications, systems, and networks. Although some of these technologies have not yet matured, CI organizations must plan for systems and networks that will provide these capabilities reliably, safely, and securely. For example, it is not easy to plan for security overhead for a future network when one does not know how much bandwidth will be required for that security overhead. This is like trying to build an airplane while in fight and not knowing what the size and capacity of airplane will be.

The OT systems of CI organizations are based on layers of technology that have accumulated over time.[3] There is a significant installed base of older technologies that were designed and implemented before cybersecurity was a concern. For many CI organizations, the technology refresh cycle is at least 7 years and may be decades long. Because replacing the installed base is expensive and resource-consuming, CI organizations must protect their existing infrastructures while building and securing for the future.

[1] Cylance, Operation Cleaver Report, 2014 (https://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf)

[2] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A; and https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

[3] http://docs.house.gov/meetings/SY/SY21/20150910/103914/HHRG-114-SY21-Wstate-BartolN-20150910.pdf

Challenge 2. Availability of qualified workforce that understands how to secure the converged CI enterprise

Any endeavor requires sufficient numbers of qualified individuals to lead, manage, and execute. The general cybersecurity workforce shortages are well known and documented by ICS2, ISACA, and other professional organizations. CI organizations experience an even more severe shortage of individuals who can address cybersecurity needs for both IT and OT. While OT system and network technology evolved to converge with the IT system and network technology, the cybersecurity techniques used on IT systems need to be carefully considered when applied to OT systems. OT systems manage and control physical events (e.g., power generation, transmission, distribution), run over vast geographically distributed areas, and behave differently than IT systems. The goals of IT systems (confidentiality, integrity and availability) are also different from those of OT systems (reliability, safety, and availability). The practices, culture, education, and mindsets of these two groups of people are different as well.

According to industry experts, putting IT practitioners in the OT environment and expecting them to be immediately effective is unrealistic.[4] What's more, the available training and education programs aimed at this population do not meet the demand. This shortage of security professionals able to "speak" both IT and OT is felt by both CI organizations and their vendors, and at all levels of the organization, from top management to entry-level workers.

Challenge 3. Managing cybersecurity risks associated with supplier relationships

Cyber supply chain risk management is a critical concern for CI organizations. Although suppliers have always been key members of the CI ecosystem, they play an even more important role today. This is caused by the exponential growth in the deployment of smart devices that need to be securely designed, implemented, and managed. Many suppliers who in the past manufactured simpler devices for the CI now make smart(er) devices that carry programmable logic (i.e., software). These suppliers are learning about security as they are producing these devices. CI organizations have had to educate their suppliers about a variety of security methods and techniques, including secure development lifecycle. Additionally, communicating security expectations to suppliers is still work in progress. Leading CI organizations have implemented sophisticated supply chain risk management programs but this is not yet the norm.

Challenge 4. Resource and scale disparities among larger and smaller organizations

Cybersecurity is a complex discipline that includes many different areas of knowledge. Larger CI organizations with more resources are better equipped to hire their own experts and run sophisticated cybersecurity programs. CI organizations that are not in this position have to manage the same set of risks with fewer human and financial resources and less scale. While smaller CI organizations are starting to outsource some of the needed services, this approach has its own challenges, such as getting the required financial resources and negotiating contracts that include

[4] Ibid.

appropriate security provisions. This is especially true for water utilities and emergency response organizations, many of which are very small.

Progress in Addressing the Challenges

Utilities have made substantial strides in securing their systems over the past 10 years. A number of the concepts and initiatives adopted by the utilities sector can be adapted to other CI organizations. Examples of these initiatives include:

- The Cybersecurity Capability Maturity Model (C2M2)—originally developed by the Energy industry in collaboration with the government—has been updated and now has three different versions: Electricity, Oil and Gas, and generic. Over 200 utilities conducted self-assessments and assessments against this model and many are using it to drive their cybersecurity programs.
- Cybersecurity Procurement Language for Energy Delivery Systems, developed by a group of industry experts, is used by many utilities to help integrate security requirements into technology procurements.
- Many utilities have designated Chief Information Security Officers (CISO) or similar leadership positions that are responsible for cybersecurity across the organization.
- Availability of training and education on industrial control systems (ICS) cybersecurity and utility IT/OT environments has increased in the last 3-5 years.
- A number of utilities have implemented comprehensive supply chain risk management programs that integrate cybersecurity risks into supply chain risk management.

Additionally, electric utilities have implemented North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards for Bulk Electric System (BES), which are now on Version 6. Version 7 is currently under development. While NERC CIP only applies to the Bulk Electric System (BES), utilities that do not fall under this regulation see it as benchmark for cybersecurity processes and controls.

What can or should be done now or within the next 1-2 years to better address the challenges

Increase availability of converged IT/OT Cybersecurity practitioner education and training.
It is challenging for CI organizations to continue improving cybersecurity when they are experiencing challenges recruiting, hiring, and retaining qualified cybersecurity workforce. Federally funded cybersecurity workforce development programs, such as National Initiative for Cybersecurity Education (NICE) are helpful, but they focus on cybersecurity training in general, not on IT/OT environments. As such, they don't address the needs of CI organizations in industries such as utilities, manufacturing, and transportation—or their vendor ecosystems. To correct the gap, we

need a broad range of approaches, including traditional education, mentorships, apprenticeships, training, and awareness.

Encourage CI organizations to mentor each other. Less experienced organizations can learn from those with more security expertise and maturity, and such knowledge transfer can be invaluable. Although CI organizations frequently collaborate based on some affinity, such as geographic proximity, creating explicit incentives for doing so will help reduce disparities among differently sized and resourced organizations. This model can be applied to CI organizations in all critical infrastructure sectors.

Encourage creation and availability of accessible and easy to use knowledge base. Cybersecurity is a vast and complex discipline with hundreds of standards, guidelines, best practices, and other resources. The amount of information needed to remain current can be overwhelming. The NIST Cybersecurity Framework provides a common language within the U.S. and is gaining use internationally. However, how it relates to NIST Special Publications, the ISO/IEC 27001 family of standards and other cybersecurity frameworks, standards and guidelines is not always clear for the cybersecurity practitioner. Digital technology can make these resources more accessible to more people—and provide a context for using them. A shared knowledge base would also help new practitioners get up to speed more quickly. Cybersecurity practitioners and their employers would benefit from having accessible open source resources that help quick learning and implementation of security controls, methods, and techniques. Ontological technologies could automate the mapping of frameworks used by multiple CI organizations.

Conclusion and Recommendations to the Commission for Action

Based on our experience, BCG believes that the single most important recommendation the Presidential Commission can make is to encourage all CI organizations to integrate cybersecurity strategy as a fundamental component of their overall organizational strategic plan and planning processes.

Unfortunately, too many CI organizations use cybersecurity technology solutions as a crutch. In BCG's experience, the most effective solutions are non-technical, but primarily strategic, organizational, managerial, process, and people-related. Effective cybersecurity requires a different way of thinking, along with changes in organization's culture and individual behavior. Most organizations already have most of the technology they need for effective cyber-defense, but have not trained their people to effectively use the existing technology, or to enforce effective cybersecurity policies. Much progress can be made by providing appropriate leadership support and oversight, using smarter processes, educating employees, and empowering them to implement a cybersecurity culture. The fact that most of the Categories in NIST Cybersecurity Framework are of non-technical nature is a strong indicator of this fact. Just as the development of Safety Culture has greatly improved the safety and reliability of our Critical infrastructure organizations, the development of a similar Cyber-safety culture will provide the most significant improvement in cyber resilience that can possibly be achieved in our critical infrastructure, and at the lowest cost.

In the experience of BCG, when Cybersecurity is a part of organizational culture, it serves as a business enabler and helps organizations grow and innovate faster and better. To make that happen, organizations need to rethink how they can integrate Cybersecurity into their organizational mission, broader risk management, and internal control activities – just as they currently do with quality management and safety. Absent that integration, decisions are made by siloed parts of the organization that do not have a full understanding of the impact that cybersecurity has on the overall organizational mission. As a result, cybersecurity requirements established in isolation from business requirements are usually misunderstood by the rest of organization and rather than being business enablers, have a negative impact on the organization's ability to perform its mission.