Energy & Manufacturing Competitiveness Partnership

Secure.

Ensuring Resilience & Prosperity in a Digital Economy

Compete.

Council on Competitiveness

Secure. Ensuring Resilience & Prosperity in a Digital Economy

THE COUNCIL ON COMPETITIVENESS is a nonprofit, 501(c) (3) organization as recognized by the U.S. Internal Revenue Service. The Council's activities are funded by contributions from its members, foundations, and project contributions. To learn more about the Council on Competitiveness, visit our home page at Compete.org.

Printed in the United States of America

Energy & Manufacturing Competitiveness Partnership

Secure.

Ensuring Resilience & Prosperity in a Digital Economy

Table of Contents

Letter from the Co-Chairs

Three years ago, the Council on Competitiveness (Council) launched the Energy and Manufacturing Competitiveness Partnership (EMCP) to better understand the policy implications of the tectonic shifts taking place in the energy and manufacturing sectors. The EMCP conducted six sector studies on the topics of: water and manufacturing; advanced materials; bioscience; agricultural and consumer water use; energy and aerospace.

These dialogues were designed to elicit common themes, findings and recommendations across the various sectors. Coming to the forefront very early on was the realization that the proliferation of data and increased connectedness of products and services was creating a new set of challenges and opportunities around securing information from the threat of cyber-attacks.

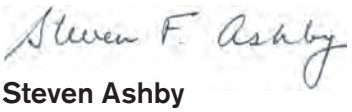
Cybersecurity is crucial to economic and national security and national competitiveness. And cyber threats to America's critical infrastructure are daunting. In its quadrennial *Global Trends* analysis, the National Intelligence Council warns that protecting critical infrastructure from cyber-attacks, including private sector networks and infrastructure such as crucial energy systems, will become an increasingly important national security challenge.

Securing energy infrastructure, in particular, from cyber threats is fundamental to U.S. economic and homeland security because of its crucial intersection with other critical infrastructures—from power and manufacturing to transportation and healthcare—that rely on energy to operate. In short, the United States needs new models for valuation of cybersecurity, including a commitment that resilience be baked into the DNA of organizations with robust processes, secure and responsive systems, and well-trained people.

Secure: Ensuring Resilience & Prosperity in a Digital Economy encapsulates the collective wisdom of more than 150 experts in the cyber field representing industry, academia, labor, national laboratories and government, and puts forth a national agenda for cybersecurity that, if enacted, would strengthen U.S. capabilities in this critical area. We look forward to working with all stakeholders to better prepare for, prevent and respond to cyber threats, and to ensure greater U.S. national and economic security.

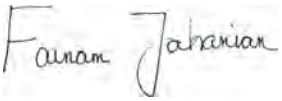
Sincerely,

Deborah L. Wince-Smith
President & CEO
Council on Competitiveness



Steven Ashby
Director
Pacific Northwest National Laboratory

George Fischer
Senior Vice President & Group President
Verizon Enterprise Solutions



Farnam Jahanian
President
Carnegie Mellon University

Executive Summary

The interconnectedness and openness made possible by the Internet and the broader digital ecosystem create unparalleled value for society. The architects of the Internet could not know, however, that it would reach the breadth and scope seen today.

In 2018, the U.S. Department of Homeland Security (DHS) declared that cyber weapons and sophisticated hacking pose a greater threat to the United States than the risk of physical attacks. With the U.S. economy losing between $57 billion and $109 billion per year to malicious cyber activity,1 it is clear that in order to remain secure and competitive, the United States needs a comprehensive national policy agenda in the cybersecurity space.

In recognition of the growing importance of cybersecurity to America's economic and national security, the Council on Competitiveness in 2018 launched a three-dialogue series on increasing the resilience of the nation's critical infrastructure, intellectual property and industrial operations against cyber-attack. The series, co-chaired by Dr. Steven Ashby, director of Pacific Northwest National Laboratory, Mr. George Fischer, senior vice president and group president of Verizon Enterprise Solutions, and Dr. Farnam Jahanian, president of Carnegie Mellon University, focused on the security and economic challenges posed by the increasing cyber threat and sought to identify mechanisms for building resilience in the new battlefield of digital warfare.

The cybersecurity initiative engaged more than 150 experts and consisted of three dialogues, each of which sought to identify the challenges and opportunities in distinct sectors of the economy. The first dialogue, hosted by Verizon in New Jersey in February 2018, examined the role of the private sector in U.S. critical infrastructure. The discussion made clear that despite the clear importance of cybersecurity in the current technological and political climate—and the threat cyber-attacks pose to critical infrastructure and intellectual property, and therefore to business operations and national security—resource constraints, both financial and human, are pervasive.

At the second dialogue, hosted by Pacific Northwest National Laboratory in Seattle in April 2018, experts across multiple sectors gathered to assess and make recommendations on the state of cybersecurity as it relates to U.S. national security. The conversation called attention to the lack of coordination across various sectors and agencies, the need to incentivize best practices in security and the importance of leveraging local and regional assets to prepare and respond to cyber-attacks.

The third and final dialogue in the series, hosted by Carnegie Mellon University in Washington, D.C., in June 2018, sought to engage federal policymakers from Capitol Hill and the administration in this important conversation and to develop an actionable agenda to improve U.S. resilience to cyber threats.

1 *The Cost of Malicious Cyber Activity to the U.S. Economy*, The Council of Economic Advisors, February 2018.

Together, the challenges, opportunities and recommendations discussed throughout the three cybersecurity dialogues—and throughout the EMCP's six sector dialogues—formed the foundation for the Council's **National Agenda for Cybersecurity** presented in this report.

The cybersecurity work was conducted under the umbrella of the Council's Energy and Manufacturing Competitiveness Partnership (EMCP), a C-suite-directed initiative focused on the shifting global energy and manufacturing landscape and how energy transformation and demand are shaping industries essential to America's prosperity and security. Critically, the EMCP approached America's diverse industrial landscape not as a monolith but as a network of distinct but interdependent productive sectors, each with its own challenges and opportunities. Throughout the exploration of six critical sectors of the U.S. economy, it became clear that cybersecurity is a significant issue that cuts across all industries and sectors, and that the United States is in need of a coordinated strategy for addressing this growing challenge.

The genesis of Council's work in this space, however, dates back to long before the launch of the EMCP in 2015. Released in 2007, *Transform. The Resilient Economy: Integrating Competitiveness and Security* declared, "The challenge is not security; it is resilience." The report promoted a strategy of resilience for both the public and private sectors—one that called for building America's capability to survive, adapt, evolve and grow in the face of challenges. While the challenges may have changed in the last ten years, the link between competitiveness and security is stronger than ever.

The **National Agenda for Cybersecurity** has the power to secure and strengthen America's resilience to the growing cyber threat while ensuring America remains a competitive, productive and prosperous nation.

A Call to Action

(see page 19 for full recommendations)

Secure America's Critical Assets and Infrastructure Against Cyber-attacks

1. Curtail the foreign acquisition by hostile actors of American cybersecurity assets to better manage risk. Regional powers have a growing potential to use purchased cyber tools to conduct catastrophic attacks on U.S. critical infrastructure.[2] While cyber threats from state and non-state actors come in many forms, including cyber-crime and military and political espionage, the acquisition by hostile foreign governments of U.S. cyber assets constitutes a significant security risk for the United States.

2. Leverage public and private sector purchasing power to ensure cybersecurity protections are upfront requirements throughout the value chain. While U.S. Department of Defense (DoD) contractors and subcontractors are required to meet certain security protocols, there is no universal clause across federal procurement contracts. And, industry largely lacks a consistent approach to applying best practices for security design, development and deployment of Internet-connected devices.

2 *Task Force on Cyber Deterrence*, Department of Defense Defense Science Board, February 2017.

3. Establish a means of coordinating cyber R&D investments and research agendas. When it comes to cybersecurity research, there is no community-defined research agenda, resulting in duplication of efforts and inefficient use of limited financial and human resources.

4. Develop, upgrade and deploy cybersecurity technology to enhance America's resilience to cyber-attacks. The pace of technological advancement is accelerating at record speeds, increasing vulnerability to data theft and operational disruption increases. As the threat of cyber-attacks becomes more grave, products and processes must be designed to meet basic security standards.

Strengthen America's Cyber Response and Recovery Capabilities

5. Enhance coordination across departments and agencies at the federal and state levels responsible, with the goal to improve resiliency and response to cyber threats. While numerous federal agencies are factoring cybersecurity into their programming and funding, there is minimal coordination across departments.

6. Develop agile, mobile and technically trained state and/or regional coalitions of cyber first-responders. Current recovery times from cyber-attacks are long and protracted, threatening American security and economic interests. With the average cost of a data breach in the United States at an all-time high of $7.91 million,[3] efficient incident response is critical and current assets are insufficient.

"The United States is in a digital arms race with state and private actors seeking to disrupt our economy and national security. Cybersecurity must be a national priority."

Dr. Steven Ashby
Director
Pacific Northwest National Laboratory

7. Expand access to cyber resources for small and medium-sized companies. Small businesses—those with fewer than 100 workers—represent more than 98 percent of total businesses in the United States.[4] In fact, 58 percent of data breach victims are small businesses.[5] Small businesses estimated their average cost for incidents in the last 12 months to be $34,604.[6]

8. Engage corporate leadership in the development of procedures necessary to plan for, respond to and recover from cyber incidents. Cybersecurity has become an urgent concern for companies of all sizes and across all industries. Cyber threats pose significant risks to economic security and competitiveness and have become increasingly costly in terms of detection and response.

3 *2018 Cost of a Data Breach Study: Global Overview*, Ponemon Institute, July 2018.

4 *Annual Survey of Entrepreneurs*, U.S. Census Bureau, 2016.

5 *2018 Data Breach Investigations Report*, Verizon, 2018.

6 *2018 HISCOX Small Business Cyber Risk Report,* Hiscox Inc, 2018.

Develop and Deploy a 21st Century Cyber Workforce

9. Expand and upskill the cybersecurity workforce to meet the complex and growing cyber threat. The cybersecurity field faces a constant shortage of practitioners, with approximately 350,000 current cybersecurity openings unfilled, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE).

10. Reform curricula at the nations's colleges and universities to better meet the demand for cyber-savvy students and workers. The race to respond to cyber workforce needs has led to inconsistency in program quality and stove piping of expertise. The ability of academia, industry and government to address these challenges while meeting the growing workforce demand will be a key driver of American competitiveness.

11. Break down legal and organizational barriers prohibiting or limiting cybersecurity practitioners from serving as educators. While there are significant challenges around a mismatch between supply and demand of cybersecurity professionals, academia faces a compounding challenges of a lack of educators to train the workforce of tomorrow.

Boost Cyber Awareness Among Policymakers and the Public

12. Increase the awareness and understanding of cybersecurity issues among members of Congress and their staffers. With at least 36 states, D.C. and Puerto Rico having introduced and/or considered more than 265 bills or resolutions related to cybersecurity[7] and as many as 12 committees holding jurisdiction over various departments, agencies and programs addressing cyber issues, all policymakers on Capitol Hill must understand the technology and implications of cyber threats.

13. Increase the cyber awareness of the general public. An ever-evolving number of cyber threats target what is, in many ways, the weak link in the U.S. cyber ecosystem—the general public. Spam, phishing, spyware, malware, trojan horses and a litany of targeted consumer attacks can ruin personal financial security and be a gateway to a broader attack with the consumer as the entry point. Cyber savviness is no longer a luxury, but a necessity for all Americans.

7 Cybersecurity Legislation 2018, National Conference of State Legislatures, May 18, 2018.

Setting the Stage

The digitization of society, proliferation of data and increased connectedness of products and services—particularly in America's critical infrastructure sectors—have transformed the ways Americans live and organizations operate. More than 20 billion devices are expected to be connected to the Internet by 2020.[8] With this connectivity, however, comes a significant threat that can jeopardize America's critical infrastructure and, along with it, the economic viability of U.S. businesses and the freedoms Americans exercise every day: cyber-attack.

Cyber threats can come in the form of traditional cyber-crime, military and political espionage, economic espionage and cyber warfare, and carry considerable costs for the United States and the world. In fact, the White House Council of Economic Advisers estimates that malicious cyber activity—defined as an activity that seeks to compromise or impair the confidentiality, integrity or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems—cost the U.S. economy between $57 billion and $109 billion in 2016[9] and is estimated to reach $2.1 trillion globally by 2019.[10] Moreover, according to the most recent data, organizations in the United States had the highest total average cost of a data breach at $7.91 million (see Figure 1).[11]

As the potential cost of cyberattacks escalates and the reliability of networks is increasingly called into question, the need to address the growing cyber threat becomes ever more urgent. Technological advancement will continue to outpace security, forcing stakeholders across all sectors of the economy—from CEOs to academics to policymakers to consumers—to move beyond the status quo and implement strong cybersecurity strategies and practices.

Asymmetric Advantage

When it comes to cyber-attacks, adversaries have an asymmetric advantage over the target: the tools needed to launch a cyber-attack are minimal, attribution is difficult if not impossible, and the impact can be devastating. The list of actors—both state and non-state—seeking to threaten U.S. economic activity is long. Members of organized criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12 percent of cyber-attacks.[12] In 2017, the Pentagon made the decision to ban software made by Russian firm Kaspersky Lab, and in August 2018, President Trump signed into law a provision that would bar the federal government from purchasing equipment from Chinese telecommunications firms Huawei and ZTE Corp., a measure spurred by concerns over the potential of Chinese espionage.[13]

8 *Department of Homeland Security Cybersecurity Strategy*, May 15, 2018.

9 *The Cost of Malicious Cyber Activity to the U.S. Economy*, Council of Economic Advisers, February 2018.

10 *The Future of Cybercrime & Security*, Juniper Research, March 25, 2017.

11 *2018 Cost of a Data Breach Study: Global Overview.* Ponemon Institute LLC, July 2018.

12 2018 Data Breach Investigations Report, Verizon Enterprise Solutions, 2018.

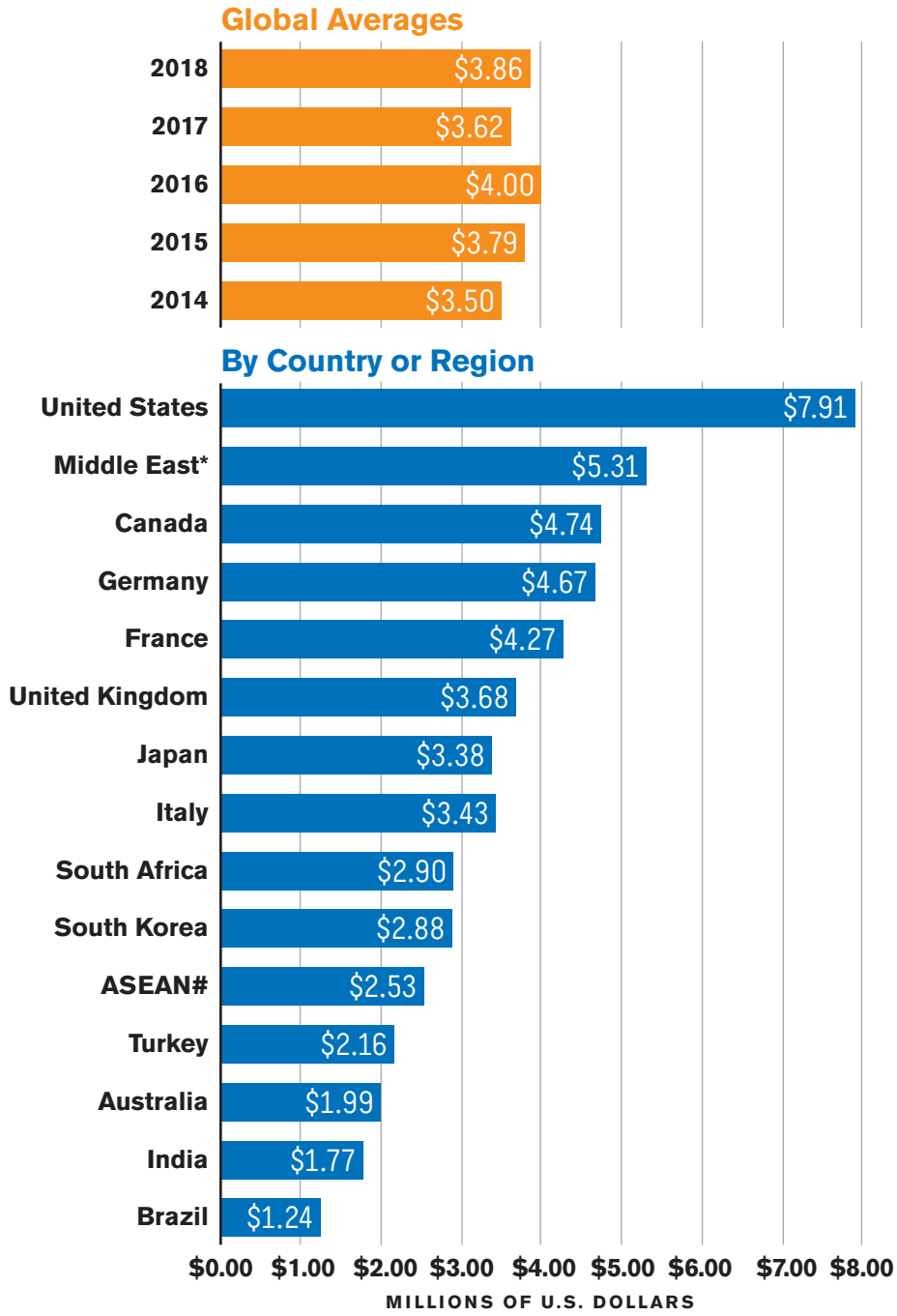
13 "Pentagon aims to shield weapons from foreign sabotage," by Ellen Nakashima, The Washington Post, August 14, 2018.

Figure 1. The Average Total Cost of a Data Breach by Country or Region
Source: *2018 Cost of a Data Breach Study: Global Overview.* Ponemon Institute LLC, July 2018.

The consolidated average per capita cost for all samples was $148, compared to an average of $141 last year.

The United States, Canada and Germany continue to have the highest per capita costs at $233, $202 and $188, respectively.

Turkey, India and Brazil have much lower per capita costs at $105, $68 and $67, respectively.



While these and other provisions are intended to shield American weapons and systems from known threats, attackers continue to hold an advantage over defenders as the first-mover that stands to incur significantly lower costs.

Critical Infrastructure

Cyber-attacks threaten American productivity and livelihoods. This is particularly true when these threats are aimed at U.S. critical infrastructure sectors, defined by the DHS as those with physical and virtual assets, systems and networks considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national and/or economic security, and national public health and/or safety.

While attacks on cyber-physical systems—smart, networked systems with embedded sensors, processors and actuators designed to sense and interact with users and support real-time, guaranteed performance in safety-critical applications—are commonly thought of as the biggest security risk to critical infrastructure, increasing reliance of business functions on IT networks has created a new frontier of vulnerabilities. And, these disruptions can be even more detrimental. As the digital and physical worlds collide, cyber-attacks have the potential to disrupt the provision of basic needs, allowing adversaries to severely harm American economic activity and daily life.

The U.S. military, in particular, has acute dependence on critical infrastructure, both domestically and internationally. The DoD has more than 15,000 computer networks among 4,000 worldwide installations, and approximately 98 percent of U.S. government communications travel over civilian owned and operated networks.[14] In fact, roughly 85 percent of U.S. critical infrastructure is privately owned or operated,[15] and these networks are highly vulnerable.

Lag in Detection Time

In the case of successful breaches, the time needed for hackers to compromise the systems under attack is most often measured in just seconds or minutes. According to Verizon's 2018 Data Breach Investigations Report (DBIR), 68 percent of breaches took months or longer to discover.[16] In 2017, it took U.S. companies an average of 201 days to detect a data breach and an average of 52 days to contain it.[17] And, it is often third parties—law enforcement, partners or customers—that discover breaches as opposed to organizations detecting breaches themselves, which was the case just 36 percent of the time in 2017.[18]

Coordination and Collaboration

Currently, multiple federal and state agencies have jurisdiction over cybersecurity in the United States. The DoD is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. The U.S. Department of Energy (DOE) leads the federal government's effort to ensure cybersecurity attacks do not have a catastrophic impact on the energy sector. The DHS claims responsibility for reducing vulnerabilities and

14 2013 DoD Task Force Report on Resilient Military Systems.

15 *Critical Infrastructure Protection, Information Sharing and Cyber Security*, U.S. Chamber of Commerce, accessed October 1, 2018.

16 *2018 Data Breach Investigations Report*, Verizon Enterprise Solutions, 2018.

17 *2018 Cost of a Data Breach Study: Global Overview.* Ponemon Institute LLC, July 2018.

18 *M-Trends 2018*, Mandant, A FireEye Company, 2018.

Some Helpful Definitions

Air gap: An absence of a direct or indirect connection between a computer and the Internet, affected for security reasons.

Malicious cyber activity: Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.—*NIST*

Data breach: An incident in which, without a system owner's knowledge, an actor steals sensitive, confidential or protected information through cyber activity.

Cyberspace: The online world of computer networks, and especially the Internet.—*Miriam-Webster Dictionary*

Closed-circuit, cyber-physical system: A system that integrates computation with physical processes in which the control logic is driven by measurements of the physical processes, and in turn drives the physical processes. This process reduces errors and improves stability through internal feedback.

Multi-factor authentication: A method of confirming a user's claimed identity in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism, such as knowledge (something the user and only the user knows), possession (something the user and only the user has), or inherence (something the user and only the user is).

building resilience, countering malicious actors in cyberspace, responding to incidents and making the cyber ecosystem more secure and resilient. The result being that, with such a large percentage of the nation's critical infrastructure owned or operated by the private sector,[19] industry is often left to wonder where to turn in the wake of an attack.

Without a single group or entity within government designated to take charge in the face of a large-scale attack, adversaries are able to maximize their already asymmetric advantage and exploit weaknesses in U.S. response capabilities and timeliness. At the federal level, this is a legislative as well as an administrative challenge. With multiple committees of jurisdiction in Congress, coordination and communication across these committees and the departments and agencies they oversee can be a challenge and an impediment to the development and implementation of a nationwide cybersecurity plan.

With the private sector operating such a large percentage of critical infrastructure, public-private partnerships are important to the success of the United States' ecosystem as it relates to cybersecurity.

19 *Critical Infrastructure Protection, Information Sharing and Cyber Security*, U.S. Chamber of Commerce, accessed October 1, 2018.

Small and Medium-Sized Businesses

Small businesses represent more than 97 percent of total businesses in the United States. According to Verizon's 2018 DBIR, 58 percent of data breach victims are small businesses.[20] This is an indication that despite security being a growing priority for organizations of all sizes, companies that sit below the "cyber poverty line", meaning they lack the resources needed to implement perceived basic security needs and therefore have significant cybersecurity risk exposure, are disproportionately targeted by attackers, creating vulnerabilities for organizations of all sizes whose operations touch these small businesses. In fact, 60 percent of smaller businesses go out of business within six months of suffering a cyber-attack.[21]

Specialized, closed-circuit cyber-physical systems have been in place in large industrial and manufacturing facilities for years. However, the economic advantages of the Internet, increasing functionality of commodity networking and information technology, and the diversification of supply chains that include many small businesses has led to new cybersecurity risks that now affect the safety and availability of the services provided by critical infrastructures.

Cyber Savviness

While the myth that cyber-attacks are often executed through air gaps—areas with indirect connections between computer and the Internet—persists, the real issue when it comes to cybersecurity is in filling knowledge gaps around information technology, research and development, and education and skills training. In fact, researchers at IBM found that 15 percent of all cyber-attacks were carried out inadvertently by insiders,[23] while as many as 24 percent of attacks may be due to employee actions or mistakes.[24]

A survey conducted by Willis Towers Watson of 92 companies from the United States found that 45 percent of 2,073 employees surveyed spent less than 30 minutes on training specific to data protection

Case Study: 140 Characters Cost U.S. Stock Market $136 Billion

In late April 2013, a tweet from the Associated Press claimed that two bombs had exploded at the White House, injuring then-President Barack Obama. The U.S. stock market reacted instantly, leading to a US$136.5 billion dip on the S&P 500 in just three minutes.

However, it was quickly discovered that the claim was false—the Twitter account had been hacked by a group calling itself the Syrian Electronic Army. When then-White House Press Secretary Jay Carney told reporters there was no explosion, the market quickly righted itself. However, not before showing the power of one tweet from a trusted source.[22]

20 2018 Data Breach Investigations Report, Verizon, 2018.

21 Champlain College, Graduate Studies, 2017; "Internet privacy in the digital age."

22 "'Bogus' AP tweet about explosion at the White House wipes billions off U.S. markets," by Peter Foster, The Telegraph, April 23, 2013.

23 2016 Cyber Security Intelligence Index, IBM X-Force Research, September 2016.

24 2016 Data Security Incident Response Report, BakerHostetler, 2016.

Transform. The Resilient Economy: Integrating Competitiveness and Security, 10 Years Later

In its 2007 report, *Transform. The Resilient Economy: Integrating Competitiveness and Security*, the Council declared, "The challenge is not security: it is resilience." This observation was made in response to the shock of 9/11, after which—for the first time in American history—it became clear that the country's economic assets and infrastructure were on the front lines of a battlefield. In 2018, while the drivers and actors may have changed in many ways, the challenges and anxieties remain the same as America finds itself standing in a new battlefield: cyberspace.

Transform identified enterprise resilience as one of three cornerstones of economic competitiveness and new value creation, along with innovation and sustainability. In the wake of 9/11, *Transform* put forth a transformational idea that there must be a business case for security and, if done right, security can lead to resilience, which has the potential to become a productivity driver and not a sunk cost.

Many of *Transform's* key findings resonate today in the context of America's cybersecurity challenges:

- Globalization, technological complexity, interdependence, terrorism, climate and energy volatility, and pandemic potential are increasing the level of risk that societies and organizations now face. Risks also are increasingly interrelated—disruptions in one area can cascade in multiple directions;
- The ability to manage emerging risks, anticipate the interactions between different types of risk, and bounce back from disruption will be a competitive differentiator for companies and countries alike in the 21st century; and
- The national objective is not just homeland protection, but economic resilience: the ability to mitigate and recover quickly from disruption.

Likewise, many of the recommendations in *Transform* are mirrored in the **National Agenda for Cybersecurity**, including:

- Leverage the government's buying clout to embed resilience criteria in the procurement selection processes and supply chains; and
- Create cutting-edge, cross-disciplinary resilience curricula that prepare students for a turbulent, interdependent work environment.

Transform also warned of turbulence ahead. For the first time, new technology and infrastructure risks were listed alongside the threat of global terrorism as major threats facing the United States. It was becoming more evident that the Internet had created an entirely new set of vulnerabilities and risks that companies had not yet mastered—and still have yet to master ten years later. While 446 data breaches were reported in the United States in 2007, that number skyrocketed to 1,579 data breaches in 2017[1]—an increase of more than 350 percent.

1 Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions), Statistia, accessed October 1, 2018.

Cybersecurity: An Initiative of the Energy and Manufacturing Competitiveness Partnership

For more than two centuries, American industry has harnessed the nation's abundance of natural resources, energy, talent and ingenuity to power the most productive economy in the world. Today, the U.S. finds itself facing a new, promising frontier shaped by two powerful transformations working in tandem:

- The generational re-emergence of advanced and highly productive manufacturing capacity; and
- The increasing abundance of innovative, sustainable, affordable and domestically-sourced energy.

To capitalize on this convergence, the Council launched the Energy and Manufacturing Competitiveness Partnership (EMCP) in 2015, which leveraged more than a decade of leadership in the energy and manufacturing fields that began with the seminal National Innovation Initiative in 2003 and continued with the Energy Security, Innovation and Sustainability Initiative (2007–2009), the U.S. Manufacturing Competitiveness Initiative (2010–2011) and the American Energy and Manufacturing Competitiveness Partnership (2012–2016). The EMCP, a C-suite-directed initiative, focused on the shifting global energy and manufacturing landscape and how energy transformation and demand is shaping industries critical to America's prosperity and security.

The EMCP was designed to approach the country's diverse industrial landscape as a network of distinct but interdependent productive sectors. Through six regional sector studies hosted by members of the Steering Committee, the EMCP identified the salient questions and challenges facing the energy-manufacturing nexus. Seeking input from a cross-section of leaders, each sector study looked at the challenges and opportunities through the Council's cross-cutting competitiveness pillars—technology, talent, investment and infrastructure.

The sector studies encompassed water, advanced materials, bioscience, agriculture, energy and aerospace, allowing the EMCP to explore how the competitiveness pillars play out within each sector, identify discrete factors shaping each sector and assess common threads that span the economy. The findings and recommendations from the sector studies informed the Council's policy agenda for manufacturing excellence, presented in *Accelerate: Turbocharging the Manufacturing Renaissance in an Era of Energy Abundance*.

As part of the evolution of the EMCP, the Steering Committee identified that stakeholders across all sectors of the U.S. economy are increasingly faced with the threat of cyber-attacks that put information, infrastructure and overall security at risk. In 2018, the Council launched a three-dialogue series on the challenges and opportunities related to cybersecurity.

The **National Agenda for American Cybersecurity**, presented in this report, is informed by those three dialogues and builds on the work of the EMCP.

and information security in the last 12 months.[25] Of that 45 percent, more than half had received no training at all. Those surveyed cite insufficient employee understanding of cyber risks, ineffective structures and processes, and insufficient budgets as the top three barriers preventing their organizations from effectively managing cyber risks.[26]

Workforce Challenges

It is vitally important that the United States has an adequate, viable cybersecurity workforce to secure critical infrastructure, but also to address a myriad of national security and domestic concerns. In 2017, the National Initiative for Cybersecurity Education (NICE) reported that 285,000 cybersecurity roles went unfilled in the United States alone.[27] The (ISC)² Global Information Security Workforce Study (GISWS) estimates that over a quarter-million positions went unfilled in the United States in 2016 and a predicted shortfall of 1.5 million cybersecurity professionals by 2020.[28] Other estimates project the demand for cybersecurity professionals will exceed the supply by as many as 3.5 million by 2021.[29]

The race to respond to cyber workforce needs has led to inconsistency in program quality and stove piping of expertise. The ability of academia, industry and government to address these challenges, while meeting current and future needs, will be a key driver of American competitiveness in this burgeoning field.

Case Study: Spear-Phishing Attack Infiltrates U.S. Universities

In 2018, nine Iranian hackers were indicted by the Department of Justice for hacking 144 U.S. universities, 47 private organizations and a handful of U.S. government agencies. The three-year campaign resulted in the loss of $3 billion in intellectual property. The hackers utilized spear-phishing emails to target professors by getting them to click on malicious links and entering login credentials. The hackers managed to successfully penetrate nearly 4,000 accounts at U.S. schools.

Nearly two years earlier, charges were brought by the U.S. Department of Justice against seven Iranians for conducting distributed denial-of-service attacks targeting Wall Street and the financial sector as well as for penetrating a dam control system. These attacks are evidence of the ability of political tension to spill into the digital world, creating a new, 21st century battlefield.

Moreover, women currently comprise just 14 percent of the information security workforce in North America—34 percentage points lower than the average of women in the workforce (see Figure 2).[30]

25 *Decoding Cyber Risk: 2017 Willis Towers Watson Cyber Risk Survey (US results)*, Willis Towers Watson, 2017.

26 Decoding Cyber Risk: 2017 Willis Towers Watson Cyber Risk Survey (US results), Willis Towers Watson, 2017.

27 *M-Trends 2018*, Mandant, A FireEye Company, 2018.

28 *(ISC)² Global Information Security Workforce Study (GISWS)*, Frost & Sullivan, April 17, 2015.

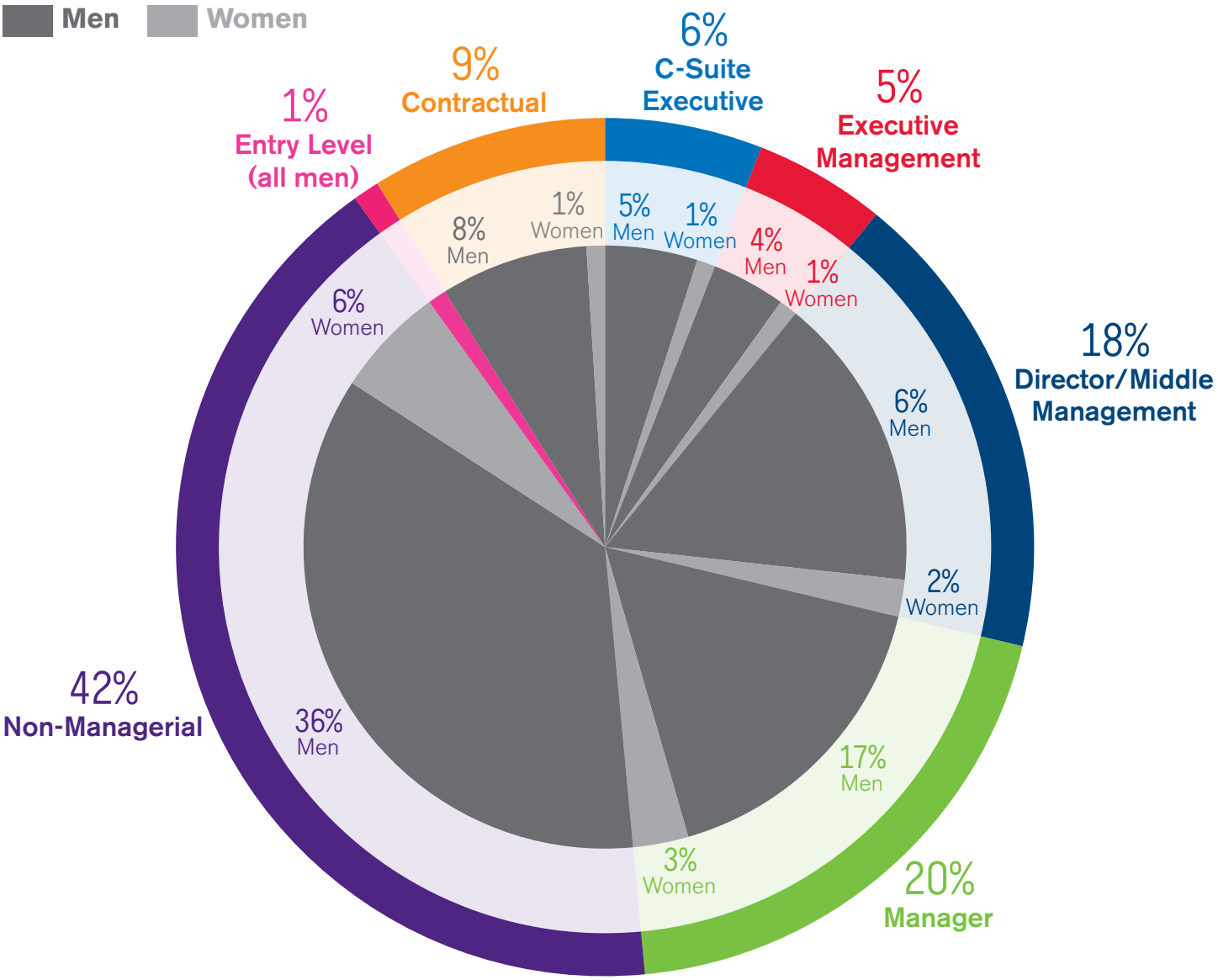
29 Cybersecurity Jobs Report, Cybersecurity Ventures, May 2017.

30 The 2017 Global Information Security Workforce Study: Women in Cybersecurity, Frost & Sullivan, 2017.

Figure 2. Gender Distribution by Organizational Position of the Cybersecurity Workforce

Source: 2017 Global Information Security Workforce Study, (Women n= 2,134; Men n=16,679)

Note: Some percentages may not add up to 100 percent due to rounding.



And, while minority representation within the cybersecurity profession (26 percent) is slightly higher than the overall U.S. minority workforce (21 percent), just 23 percent of minority cybersecurity workers hold a role of director or above, 7 percent below the U.S. average.[31] Consequently, policies that encourage greater participation in the cybersecurity workforce will be essential if the United States hopes to meet the growing demand for cyber professionals.

Conclusion

Rapid advancement in cyber technology development is being fueled by industry modernization, e-commerce and consumer entertainment. The interconnectedness and openness made possible by the Internet and broader digital ecosystem create unparalleled value for society.

But these same qualities make securing today's cyber landscape difficult. Technological advancement is outpacing security and will continue to do so unless the United States changes the way it approaches and implements cybersecurity strategies and practices. Cybersecurity requires a comprehensive, national agenda to secure, enhance and strengthen America's resilience to cyber-attacks and ensure the nation is equipped with the tools and talent needed to remain a global leader in technology and innovation.

"Cyber-attacks are a constant threat to the increasingly interconnected digital backbone of the U.S. economy and will require coordination among industry, academia and government to mitigate the risk."

Mr. George Fischer
Senior Vice President and Group President
Verizon Enterprise Solutions

31 Labor force characteristics by race and ethnicity, U.S. Bureau of Labor Statistics, 2015.

A National Agenda for Cybersecurity

A national cyber agenda must ensure the United States has the infrastructure, technology and talent needed to build resilience to cyber-attacks, along with the ability to respond and recover in the event of such attacks.

The interconnectedness and openness made possible by the Internet and the broader digital ecosystem create unparalleled value for society. The architects of the Internet could not know, however, that it would reach the breadth and scope seen today. Throughout human history, technological advancement has outpaced security. While this is unlikely to change, America's ability to remain resilient in the face of increasing cyber threats will require a shift in the understanding of—and dynamic between—innovation and security. The evolution to a new way of thinking that focuses on deliberate, risk-informed trade-offs will be essential.

What follows are a series of concrete, actionable recommendations cutting across the public and private sectors that, taken together, will strengthen U.S. cyber defenses and ensure greater resilience in the face of growing and malicious cyber threats.

Secure America's Critical Assets and Infrastructure Against Cyber-attacks

With the average cost of a data breach in the United States at an all-time high of $7.91 million and over 1,300 significant breaches in the last year, malicious cyber activity in the United States is a substantial threat to America's economic and national security.[32] The increasing sophistication of cyber-attacks poses a constant threat to critical infrastructure. And as the availability of networks is called into question every day, the economic viability of U.S. businesses and the freedoms Americans exercise daily are in jeopardy.

1. Curtail the foreign acquisition by hostile actors of American cybersecurity assets to better manage risk. Regional powers have a growing potential to use purchased cyber tools to conduct catastrophic attacks on U.S. critical infrastructure.[33] While cyber threats from state and non-state actors come in many forms, including cyber-crime and military and political espionage, the acquisition by hostile foreign governments of U.S. cyber assets constitutes a significant security risk for the United States.

Recommendations

1.1. Require under the new authorities of the Foreign Investment Risk Review Modernization Act (FIRRMA) in the National Defense Authorization Act for Fiscal Year 2019 that the Committee on Foreign Investment in the United States (CFIUS) conduct full reviews and regulatory approval for any foreign investment or ownership interest in American advanced cybersecurity startups, joint ventures or acquisitions.

32 *2018 Cost of a Data Breach Study*, Ponemon Institute, July 2018.

33 *Task Force on Cyber Deterrence*, Department of Defense Defense Science Board, February 2017.

1.2. Require all U.S. securities and SEC-registered securities and investment funds of any size to provide the U.S. Department of the Treasury and the FBI full transparency on sources of investment capital and intellectual property, and limit partners from countries deemed high-risk or sanctioned by the Treasury Department.

1.3. Expand the authority of the Bayh-Dole Act and federal tech transfer act to prevent the licensing of U.S. cyber technology developed with federal funding to foreign countries deemed high risk.

2. Leverage public and private sector purchasing power to ensure cybersecurity protections are upfront requirements throughout the value chain. While DoD contractors and subcontractors are required to meet certain security protocols, there is no universal clause across federal procurement contracts. And, industry largely lacks a consistent approach to applying best practices for security design, development and deployment of Internet-connected devices.

Recommendations

2.1. Extend Defense Federal Acquisition Regulation Supplement DFAR 252.204-7012 language mandating adequate security to all government agencies.

2.2. Call on Congress to take immediate action on the Internet of Things ('IoT') Cybersecurity Improvement Act of 2017, requiring the inclusion of specific cybersecurity protections in procurement contracts with all federal and state agencies for Internet-connected devices.

2.3. Incentivize vendors' awareness and adoption of security best practices utilizing industry purchasing power.

2.4. Promote greater uptake and use of existing cybersecurity standards to increase supply chain security.

3. Establish a means of coordinating cyber R&D investments and research agendas. When it comes to cybersecurity research, there is no community-defined research agenda, resulting in duplication of efforts and inefficient use of limited financial and human resources.

Recommendations

3.1. Establish the National Cybersecurity R&D Initiative, chaired by the White House Science Advisor, to identify challenges, solicit industry input, define priorities and, on an ongoing basis, coordinate government investment to optimize talent and resources and avoid duplication of efforts.

3.2. Convene a Basic Research Needs working group including leaders from the public and private sectors to define a set of research priorities to address the technology R&D challenges and Science Grand Challenges that, if solved, will strengthen U.S. cybersecurity capability.

3.3. Create data-driven processes to develop specific cybersecurity countermeasures unique to sectors and sub-sectors, and disseminate these processes through Information Sharing and Analysis Centers and Community Emergency Response Teams to mitigate the risk of cyber incidents.

4. Develop, upgrade and deploy cybersecurity technology to enhance America's resilience to cyber-attacks. The pace of technological advancement is accelerating at record speeds, increasing vulnerability to data theft and operational disruption increases. As the threat of cyber-attacks becomes more grave, products and processes must be designed to meet basic security standards.

Recommendations

4.1. Require that all new technology applied to the electric grid meet industry standards to ensure basic cybersecurity.

4.2. Expand funding and private sector engagement for testbeds for the creation and adoption of new cybersecurity technologies such as Digital Manufacturing Design and Innovation Institute (DMDII) Cyber Hub for Manufacturing and the Army Cyber-research Analytics Laboratory.

4.3. Expand the NIST cybersecurity framework to better guide secure development of IoT, operational technology (OT) and information technology (IT) platforms and technologies as a means to bolster private industry certification programs.

Strengthen America's Cyber Response and Recovery Capabilities

According to the latest data, in the United States, the average time required to identify a data breach incident is 201 days, while the average amount of time to contain a breach is 52 days.[34] America's ability to detect, withstand and recover from cyber events that disrupt the economy and society in a quick and coordinated manner is essential for the nation's security and competitiveness.[35]

5. Enhance coordination across departments and agencies at the federal and state levels responsible, with the goal to improve resiliency and response to cyber threats. While numerous federal agencies are factoring cybersecurity into their programming and funding, there is minimal coordination across departments.

Recommendations

5.1. The administration should reinstate and empower a White House cybersecurity czar to oversee a government-wide interagency task force to develop and implement, within 180 days, a coordinated cyber defense strategy that includes mechanisms for owners and operators of critical infrastructure to more easily share appropriate data.

5.2. Governors should convene state and local representatives from across the public and private sectors to develop statewide cyber-attack prevention and response strategies.

34 "IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses," PRNewswire, IBM Security, July 11, 2018.

35 "Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option", Testimony of Robert Luft, Owner, Surefire Innovations, National Small Business Association, July 26, 2017.

5.3. Convene biannual meetings of the private sector chairpersons of federal government advisory committees and external boards to share agency priorities, best practices and identify areas to strengthen interagency collaboration.

6. Develop agile, mobile and technically trained state and/or regional coalitions of cyber first-responders. Current recovery times from cyber-attacks are long and protracted, threatening American security and economic interests. With the average cost of a data breach in the United States at an all-time high of $7.91 million,[36] efficient incident response is critical and current assets are insufficient.

Recommendations

6.1. Institute state Cyber Protection Teams through the National Guard Bureaus and tactical analysis groups.

6.2. Governors and state legislators must provide funding and reduce legal and liability barriers to resources acting in state capacity.

6.3. Expand to additional states existing programs[37] to provide veterans with access to cybersecurity training opportunities and resources to help veterans enter the cybersecurity workforce.

6.4. Establish and fund, at the state level, "civilian reserve cyber corps" comprising volunteers from private industry security and IT professionals to be deployed in the event of a regional cyber incident.

6.5. Create a tiered technology approach to cyber that enables technically-trained cyber experts—people who are experts in using tools but that don't require advanced degrees—to obtain the technical skills needed to act in this capacity.

7. Expand access to cyber resources for small and medium-sized companies. Small businesses—those with fewer than 100 workers—represent more than 98 percent of total businesses in the United States.[38] In fact, 58 percent of data breach victims are small businesses.[39] Small businesses estimated their average cost for incidents in the last 12 months to be $34,604.[40]

Recommendations

7.1. Sustain funding for the Manufacturing Extension Partnership (MEP) National Network and expand resources available for cybersecurity tools and training and certification such as the NIST MEP Cybersecurity Assessment Tool.

7.2. State and metropolitan Small Business Administrations should establish cybersecurity training initiatives in partnership with Workforce Development Boards to reach a broad array of small and medium-sized businesses below the cyber poverty line.

7.3 Expand federal and state outreach to small and medium-sized businesses to increase knowledge of existing resources, including top resources identified by the DHS U.S. Computer Emergency Readiness Team (US-CERT).

36 *2018 Cost of a Data Breach Study: Global Overview*, Ponemon Institute, July 2018.

37 Cyber Virginia: Cyber Veterans Initiative, The Commonwealth of Virginia, July 2017.

38 *Annual Survey of Entrepreneurs*, U.S. Census Bureau, 2016.

39 *2018 Data Breach Investigations Report*, Verizon, 2018.

40 *2018 HISCOX Small Business Cyber Risk Report,* Hiscox Inc, 2018.

8. Engage corporate leadership in the development of procedures necessary to plan for, respond to and recover from cyber incidents. Cybersecurity has become an urgent concern for companies of all sizes and across all industries. Cyber threats pose significant risks to economic security and competitiveness and have become increasingly costly in terms of detection and response.

Recommendations

8.1. Corporate cybersecurity leads should report directly to executive team members and align responsibilities with risk management strategies.

8.2. Companies should embrace the Securities and Exchange Commission Guidance on Public Company Cybersecurity Disclosures[41] and take all required actions to inform investors of material cyber risks and incidents in a timely fashion.

Develop and Deploy a 21st Century Cyber Workforce

Further adding to the growing risk of cyber threats to American prosperity, the world is on pace to reach a cybersecurity workforce gap of 1.8 million by 2022.[42] It is vitally important that the United States have an adequate cybersecurity workforce to secure the nation's critical infrastructure; respond to the ever-expanding cyber threat; and equip businesses of all sizes and governments at all levels with the talent to meet the next generation of cyber challenges.

9. Expand and upskill the cybersecurity workforce to meet the complex and growing cyber threat. The cybersecurity field faces a constant shortage of practitioners, with approximately 350,000 current cybersecurity openings unfilled, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE).

Recommendations

9.1. Ensure NSF funding for the CyberCorps®: Scholarship for Service (SFS) program meets the growing demand.

9.2. The National Science Foundation should expand and expedite the implementation of the Community College Cyber Pilot Program (C3P) under the CyberCorps® SFS program.

9.3. Congress should take immediate action to pass S. 754, Cyber Scholarship Opportunities Act of 2017 to permanently extend support for cybersecurity education in primary and secondary schools.

9.4 Expand cybersecurity awareness programs in secondary schools to increase interest and awareness of students from diverse backgrounds regarding career opportunities in the cybersecurity field.

41 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 2018.

42 *2017 Global Information Security Workforce Study*, Frost & Sullivan, 2017.

10. Reform curricula at the nations's colleges and universities to better meet the demand for cyber-savvy students and workers. The race to respond to cyber workforce needs has led to inconsistency in program quality and stove piping of expertise. The ability of academia, industry and government to address these challenges while meeting the growing workforce demand will be a key driver of American competitiveness.

Recommendations

10.1. Expand the number of colleges and universities with programs and credentials that meet the criteria required for designation as National Centers of Academic Excellence in Cyber Operations or Cyber Defense by the National Security Agency and the DHS.

10.2. Embed cybersecurity concepts into a broad range of existing degree programs at the university level.

11. Break down legal and organizational barriers prohibiting or limiting cybersecurity practitioners from serving as educators. While there are significant challenges around a mismatch between supply and demand of cybersecurity professionals, academia faces a compounding challenges of a lack of educators to train the workforce of tomorrow.

Recommendations

11.1. States and educational institutions must reduce barriers to allow cybersecurity practitioners to serve as professors of practice.

11.2. Establish industry-academia-national laboratory exchange programs to facilitate cross-pollination between cyber experts and practitioners.

Boost Cyber Awareness Among Policymakers and the Public

Human error is one of the most significant challenges when it comes to protecting against cyber-attacks. In fact, 90 percent of cyber incidents are human-enabled,[43] while as many as 24 percent of attacks may be due to employee actions or mistakes. [44]

12. Increase the awareness and understanding of cybersecurity issues among members of Congress and their staffers. With at least 36 states, D.C. and Puerto Rico having introduced and/or considered more than 265 bills or resolutions related to cybersecurity[45] and as many as 12 committees holding jurisdiction over various departments, agencies and programs addressing cyber issues, all policymakers on Capitol Hill must understand the technology and implications of cyber threats.

Recommendation

12.1. Members in the House of Representatives and Senate should reinvigorate the bipartisan House and Senate Cyber Caucuses, which have been largely dormant in recent years, to provide members of Congress and their staffers with access to experts in the field.

43 Shifting the Human Factors Paradigm in Cybersecurity, Calvin Nobles, Ph.D., March 15, 2018.

44 2016 Data Security Incident Response Report, BakerHostetler, 2016.

45 Cybersecurity Legislation 2018, National Conference of State Legislatures, May 18, 2018.

13. Increase the cyber awareness of the general public. An ever-evolving number of cyber threats target what is, in many ways, the weak link in the U.S. cyber ecosystem—the general public. Spam, phishing, spyware, malware, trojan horses and a litany of targeted consumer attacks can ruin personal financial security and be a gateway to a broader attack with the consumer as the entry point. Cyber savviness is no longer a luxury, but a necessity for all Americans.

Recommendations

13.1. Fund, develop and implement a major national cyber-awareness campaign, that builds on existing efforts, to increase the general public's awareness and capability to prepare for and respond to cyber threats.

13.2. Call on local economic development authorities to put in place programs that encourage cybersecurity education at the K-12 level.

13.3. Implement and enforce basic cybersecurity protocols throughout industry, government and academia including patching, multi-factor authentication and identity management as standard business practices.

"With the proliferation of interconnected devices, industries and organizations, the need for cyber expertise is quickly outpacing supply, creating an urgent need for colleges and universities to innovate curricula and program offerings in this field."

Dr. Farnam Jahanian
President
Carnegie Mellon University:

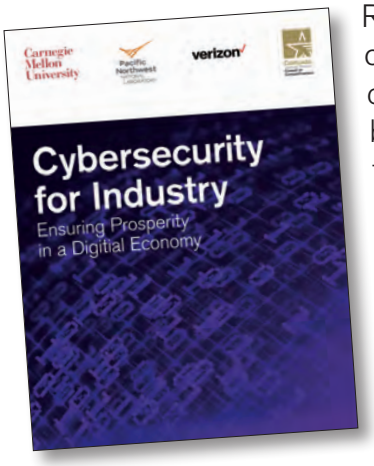
Cybersecurity Dialogue Series

DIALOGUE 1

Cybersecurity for Industry: Ensuring Prosperity in a Digital Economy

February 2, 2018
Basking Ridge, NJ

Hosted by: Mr. George Fischer
Senior Vice President & Group President
Verizon Enterprise Solutions



Rapid advancement in cyber technology development is being fueled by industry modernization, e-commerce and consumer entertainment. The interconnectedness and openness made possible by the Internet and the broader digital ecosystem creates unparalleled value for society. Advancements in computing, networking and communications technology permeate through every sector of the economy and are being made at a pace that is both breathtaking and unprecedented in human history. But these same qualities make securing today's cyber landscape extremely challenging. Technological advancement is outpacing security and will continue to do so unless the United States changes the way it approaches and implements cybersecurity strategies and practices.

With attribution of cyber-attacks becoming more difficult, and with these events happening at increasing rates, companies and organizations need a revised tool set to handle cyber-attacks quickly and effectively. And as adversarial AI becomes significantly more sophisticated in the next three to five years, the need to promote a cyber moon shot becomes increasingly more urgent. Cybersecurity is no longer a predominantly tech-related problem—due to the tremendous financial burden of cyber-attacks incurred as a consequence of disruption to operations, loss of data and cost of security, among other concerns, cyber-attacks have become a risk management issue, while strong cyber defense/response can be a productivity enabler.

Despite the clear importance of cybersecurity in the current technological and political climate—and the threat cyber-attacks pose to critical infrastructure and intellectual property, and therefore to business operations and national security—resource constraints, both financial and human, are pervasive. Small and medium-sized companies often face budgetary constraints that preclude them from affording the latest security technology. And firms of all sizes see talent shortages and knowledge gaps that leave them vulnerable to cyber risks and slow to recover from cyber-attacks.

These are just a few of the multidimensional security challenges companies in the United States face in an era marked by transformational innovation and the digitization of an exponential amount of data. These challenges, while difficult and numerous, are not insurmountable. They will, however, require collaboration on the parts of both the public and private sectors to improve America's mitigation, adaptability and resilience to the growing number of cyber threats from state and non-state actors.

Initial Findings

Voluntary, industry-led cybersecurity standards, created in partnership with the government, are needed. While risk management frameworks and industry guidelines around cybersecurity exist, there is a need for industry-sponsored standards that define basic cybersecurity terms, and set security thresholds for products and systems. These standards could be used to benchmark security posture and create a competitive advantage for companies. The National Institute of Standards and Technology (NIST) could act as an umbrella infrastructure for these standards.

Security must be integrated into products and processes early on in the development cycle, rather than being considered an add-on component. As the pace of technological advancement accelerates at record speeds and products become increasingly connected through the proliferation of sensors and data, vulnerability to data theft and operational disruption increases. As the threat of cyber-attacks becomes more grave, products and processes must be designed with cyber resiliency in mind.

An overwhelming amount of data creates challenges with regard to credibility of cyber threats and ability to operationalize data. With the volume of useful, actionable information greater than ever before, a balance must be struck between information sharing required for legitimate policy interests and guarding private enterprise interests. Standardizing the gathering and valuation of cybersecurity data would improve security across all industries, but building trusted relationships is currently the best way to facilitate sharing of high-quality data on cybersecurity threats and attacks.

Cybersecurity must be transformed into a competitive advantage rather than a sunk cost by focusing on the confluence of risk, capabilities and resources. By treating cybersecurity as a precompetitive issue, being proactive in addressing threats rather than reactive to attacks, and looking at cyber technologies and cybersecurity posture as valued capital rather than as a liability, companies can raise their security posture and insulate themselves from cyber threats. This requires more research into quantifiable risk that can enable a meaningful regulatory approach and insurance market that should in time be rewarded by the market.

All organizational levels, including company boards and C-suite leaders, must be engaged in cyber planning, response and recovery efforts. Cybersecurity is often considered the job of policy and IT experts. A shift in organizational culture across all organizational functions and levels to view cybersecurity as an issue of larger corporate relevance, rather than simply a technology problem, is necessary to improve companies' ability to protect against, respond to and recover from cyber-attacks.

Industry and academia must work together to create a baseline curricula to educate a knowledgeable, cyber-savvy workforce. It is vitally important for the United States to have an adequate, viable cybersecurity workforce with a consistent, baseline level of knowledge. Diversity and inclusion will be essential in order to meet the burgeoning needs in this field. Hands-on experience and mentorship programs would also help increase interest while combatting the slow pace of curriculum change. It would also be mutually beneficial for industry and academia to cross-pollinate and cycle practitioners and educators through both worlds.

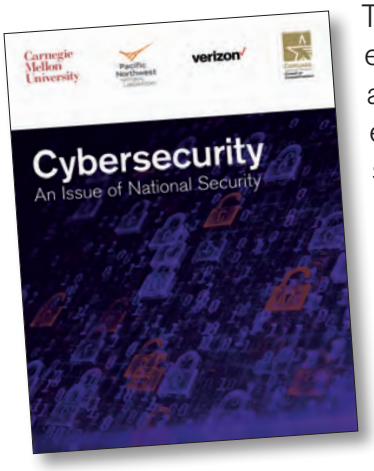
Cybersecurity must be integrated into educational curricula outside traditional four-year universities and post-grad studies, including high schools and community colleges. The responsibility of educating on cybersecurity and computer science should not rest entirely on college and universities. College-level courses in cyber or computer science at the high school level would help expand the talent pool. Community colleges, with the support of industry executives, should also be considered a viable option for students and a viable recruitment pool for employers.

DIALOGUE 2

Cybersecurity: An Issue of National Security

April 25, 2018
Seattle, WA

Hosted by: Dr. Steven Ashby
Director
Pacific Northwest National Laboratory



The digitization of society, proliferation of data and increased connectedness of products and services—particularly in America's critical infrastructure sectors—have transformed the ways Americans live and organizations operate. Yet, the tremendous growth in the level of connectivity poses risks to U.S. global competitiveness as firewalls become the next frontline for battle in the United States. As a result, cybersecurity has become an issue of national security.

The United States is facing a steady increase in the volume, types and sophistication of cyber-attacks. Organizations of all types—including industry, government, academia and national laboratories—are assailed relentlessly by efforts from state and private entities to disrupt operations, steal information and increase their own competitiveness. These threats, which come in the form of traditional cyber-crime, military and political espionage, economic espionage and cyber warfare, carry considerable costs for the United States and the world. In fact, a study by Juniper Research suggests the annual cost of data breaches will reach $2.1 trillion globally by 2019, an increase of almost four times the estimated cost of breaches in 2015.[46]

Cyber-attacks are particularly concerning when it comes to the 16 critical infrastructure sectors as defined by the DHS[47]—each of which plays an integral role in America's economic and national security. A reliable energy grid, for example, is essential for any institution to operate. And while the DOE currently has plans to improve preparedness, response and recovery capabilities, 90 percent of the energy grid is operated by private companies—requiring strong public and private partnerships to ensure

46 The Future of Cybercrime & Security, Juniper Research, March 25, 2017.

47 PPD-21 identifies 16 critical infrastructure sectors: chemicals; commercial facilities; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors; materials and waste; sector-specific agencies; transportation systems; and water and wastewater systems. https://www.dhs.gov/critical-infrastructure-sectors.

these suppliers are resilient against and have the tools needed to respond quickly to potential cyber-attacks.[48]

The increasing sophistication of cyber-attacks poses a constant threat to critical infrastructure. And as the availability of networks is called into question every day, the economic viability of U.S. businesses and the freedoms Americans exercise daily are in jeopardy.

Initial Findings

Cybersecurity should be built into industry and government contracts to incentivize broader adoption. Cybersecurity must be better incentivized using new, innovative market mechanisms. This could include building security into procurement mechanisms or advancing how technologies are measured for security in order to institutionalize the adoption of security measures across the supply chain.

A unified, clear research agenda across industry and government is needed in the cybersecurity space. When it comes to cybersecurity research, there is no clear, community-defined research agenda, resulting in duplication of efforts and inefficient use of limited financial resources. A mechanism is needed to organize the research community and marshal appropriate stakeholders and topics to shape the research agenda.

Effort is needed to connect industry with laboratory and academic research to ensure knowledge transfer and reduce duplication. Discoverability of existing capabilities—both on the part of industry and the R&D community—is a significant challenge. Better coordination would reduce duplication of efforts—both within and across these communities—and help better align research priorities and commercial needs to scale-up security solutions.

There must be a clearly-articulated federal model for cyber response to critical infrastructure attacks. While numerous government agencies are factoring cybersecurity into their programming and funding, there is minimal coordination across these programs. This would decrease duplication of efforts and improve resiliency and response capabilities in the face of cyber threats.

There is an opportunity at the state or regional level to capitalize on the patriotism, altruism and tech savviness of younger generations to create coalition(s) of cyber first-responders. Current recovery times from cyber-attacks are long and static, threatening American security and economic interests. The United States needs a coordinated first-response effort to further regional cyber protection and response. One potential home for this effort could be within the National Guard.

Globally-defined, security baselines are needed and must be informed by relevant stakeholders. Useful and practical security baselines would level the playing field and set basic expectations around how systems and networks can be deployed in recommended, secure configurations. Advances must be made through the product lifecycle to improve design, default and deployment, thereby building assurance around the resiliency of critical infrastructure to cyber-attacks and disruption.

48 https://www.energy.gov/oe/activities/cybersecurity-critical-energyinfrastructure.

Applying automated security monitoring to critical infrastructure sectors would significantly improve cyber defense. When applied to the observe-orient-decide-act loop, continual evaluation of security through artificial intelligence and machine learning can enable adversary detection, attribution and action prediction and improve response in a way that would reduce the asymmetric advantage of attackers and level the cyber defense playing field for critical infrastructure providers.

Cybersecurity must be integrated into the academic curricula of related topics. While training cybersecurity professionals is a valuable endeavor, cybersecurity must be a key educational component for computer scientists, engineers and other professions in which security is a foundational concern. This will increase the pool of professionals with relevant and applicable cybersecurity skills across the most critical areas of need and ensure that future engineers across all disciplines are able to design and build secure systems.

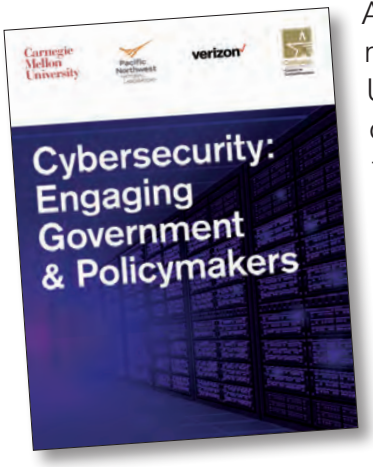
Barriers prohibiting practitioners to serve as educators must be reduced. While there are significant challenges around a mismatch between supply and demand of cybersecurity professionals, academia faces the compounding challenge of a lack of educators to train the workforce of tomorrow. A strategic effort on the part of industry and academia is needed to fill this gap.

DIALOGUE 3

Cybersecurity: Engaging Government & Policymakers

June 19, 2018
Washington, D.C.

Hosted by: Dr. Farnam Jahanian
President
Carnegie Mellon University



As computing power rapidly increases, the United States faces the challenge of protecting the latest technology from the increasing threat of cyber-attacks. This task will only become more difficult given the rising number of devices connected to the electric grid as smart homes and buildings become the norm. Although the United States is progressively making cybersecurity a higher priority for the nation, there is still much work to be done to secure critical infrastructure.

With the United States already at a disadvantage in comparison to its adversaries, U.S. policymakers must act to build resilience to the increasing threat and occurrence of cyber-attacks. Without a single group or entity within government designated to take charge in the face of a large-scale attack, adversaries are able to maximize their already asymmetric advantage and exploit weaknesses in U.S. response capabilities. And while agencies like the DOE have taken critical steps to protect America's energy

infrastructure, coordination and effective communication with Congress is necessary to ensure efficient use of the limited resources available to support nationwide cybersecurity.

Simultaneously, the challenges posed by the increasing cyber threat from state and non-state actors continue to outpace the size of the workforce equipped with the skills to mitigate the growing risk. While programs exist throughout the federal government—including the National Science Foundation's CyberCorps®: Scholarship for Service, a scholarship program to recruit and train the next generation of information technology professionals, industry control system security professionals and security managers—these efforts must be amplified in order to keep pace with the growing need for cybersecurity professionals.

Together, policymakers across all federal agencies must address the growing threat of cyberattack to the United States. Coordination and collaboration are essential if the United States is to secure itself against the threat of attack, enhance cyber resilience, strengthen the cyber workforce and boost the awareness needed to remain competitive.

Initial Findings

There must be a clear, practical model for cyber response that identifies roles and responsibilities of the public and private sectors. Numerous federal agencies currently have jurisdiction over different aspects of cybersecurity, leaving uncertainty as to where responsibilities lie in the wake of an attack. Similarly, there is a lack of clarity on the part of industry as to the requirements. Clear leadership in the cybersecurity space would help the United States maintain its competitive advantage by thwarting cyber threats.

Small and medium-sized businesses often lack access to the knowledge and resources needed to maintain an appropriate level of cybersecurity. Much of industry is below the cyber "poverty line," meaning they do not have access to the resources needed for basic cyber hygiene, much less defense against nation-states. These businesses can serve as a gateway into larger organizations for attackers. Tools and guidance for small and medium-sized businesses would improve supply chain cybersecurity overall.

Tools for assessing the performance, benefit and risk associated with cyber tools must be developed. Independent consumer reports, tests or assurance programs that correlate to improved cybersecurity posture would improve supply chain security and enable the uptake of proven security technologies.

The current talent pool cannot meet the rising demand for cybersecurity workers. Without intervention, the United States will experience a debilitating lack of talent to fill cybersecurity needs essential for maintaining competitive advantage globally. Tools must be developed to train cybersecurity professionals at all levels—from first response practitioners to experts.

Cybersecurity must be incentivized as a risk management issue to raise the overall security posture of American industry and critical infrastructure. When cybersecurity is perceived by businesses as a cost, decisions are made from a cost-benefit perspective rather than a risk management vantage point. This becomes a challenge as cybersecurity risks span beyond the source of the incident. Cyber protections and processes must be valued as capital rather than cost.

Security must be built into products and systems from the very earliest stages of development. The pace of innovation and technology uptake by the general public has historically been driven by convenience and functionality, as opposed to security. This creates a situation where technology is used long before its security implications are understood. Creating a basic blueprint that provides a succinct path for security-enabled technologies to transition from research to market will minimize stranded research and increase the overall security posture of the United States by facilitating the introduction of new, more secure products to the market.

About the Council on Competitiveness

For more than three decades, the Council on Competitiveness (Council) has championed a competitiveness agenda for the United States to attract investment and talent, and spur the commercialization of new ideas.

While the players may have changed since its founding in 1986, the mission remains as vital as ever—to enhance U.S. productivity and raise the standard of living for all Americans.

The members of the Council—CEOs, university presidents, labor leaders and national lab directors—represent a powerful, nonpartisan voice that sets aside politics and seeks results. By providing real-world perspective to Washington policymakers, the Council's private sector network makes an impact on decision-making across a broad spectrum of issues from the cutting-edge of science and technology, to the democratization of innovation, to the shift from energy weakness to strength that supports the growing renaissance in U.S. manufacturing.

The Council's leadership group firmly believes that with the right policies, the strengths and potential of the U.S. economy far outweigh the current challenges the nation faces on the path to higher growth and greater opportunity for all Americans.

Council on Competitiveness
900 17th Street, NW
Suite 700
Washington, D.C. 20006
+1 (202) 682-4292
Compete.org

APPENDIX A

Compete.
Council on Competitiveness

Ensuring Prosperity and National Security in a Digital Economy
An initiative of the Energy and Manufacturing Competitiveness Partnership

Background

America's critical infrastructure is an integral part of national security and homeland security. Maintaining the 16 critical infrastructure sectors, which include critical manufacturing, energy, financial services and transportation, requires coordinated action on the part of government (federal, state, and local), the private sector, and the U.S. military.

The U.S. military has acute dependence on critical infrastructure both domestically and internationally. The Department of Defense has over 15,000 computer networks among 4,000 worldwide installations, and approximately ninety-eight percent of U.S. government communications travel over civilian owned and operated networks.[1] In fact, roughly eighty-five percent of U.S. critical infrastructure is privately owned or operated, and these networks are highly vulnerable. The significant cybersecurity threat jeopardizes America's critical infrastructure and, along with it, the economic viability of U.S. businesses and the freedoms Americans exercise every day.

Despite the notable risk cyber threats pose to American prosperity, there is a wide disparity in investment, maturity, coordination and training on cybersecurity across the various critical infrastructure sectors. According to the US Bureau of Labor Statistics, in 2016 the cybersecurity field experienced an increasing shortage of practitioners with over a quarter-million positions remaining unfilled in the US alone and a predicted shortfall of 1.5 million cybersecurity professionals by 2019. Yet cyberspace is the nervous system of critical infrastructure sectors– both in terms of traditional information technology and operational technology.

According to the Department of Homeland Security, 56 percent of all cyber incidents against critical infrastructure in 2013 were directed at energy infrastructure, mostly the electric grid. In the 2017 Verizon Data Breach Investigations Report, it reported that 63% of breaches of manufacturing and utilities were cyber-espionage related with the majority of those attacks were triggered by phishing. Almost ¾ of breaches were attributed to state-affiliated threat actors.[2] This figure has declined as cyber-attacks against other critical infrastructure have grown, but the threat to our energy infrastructure remains high. Failure to take responsible action leaves the U.S.

[1] 2013 DoD Task Force Report on Resilient Military Systems
[2] 2017 Verizon Data Breach Investigations Report

vulnerable to a variety of threats. Nation-states such as Russia, China, and Iran threaten U.S. critical infrastructure and assets in the interest of furthering their objectives. Cyber espionage is rampant, with U.S. companies estimated to be losing a staggering $300 billion every year in intellectual property.

Rapid advancement in cyber technology development is being fueled by industry modernization, e-commerce and consumer entertainment. The interconnectedness and openness made possible by the Internet and broader digital ecosystem create unparalleled value for society. But these same qualities make securing today's cyber landscape difficult. Technological advancement is outpacing security and will continue to do so unless we change the way we approach and implement cybersecurity strategies and practices.

Objectives

The Council, in partnership with Pacific Northwest National Laboratory, Verizon Enterprise Solutions and Carnegie Mellon and key representatives from other National Labs, industry, academia, propose to host three dialogues, each with 30-40 experts, focused on the challenges and cybersecurity coordination required in each of the following areas:

- *Industry* – examining both the role of the private sector in U.S. critical infrastructure, the differences in priorities across various sectors, and U.S. industry reliance on critical infrastructure operations.
- *Government* – examining the role of government in bridging the gap with private industry, encouraging appropriate information sharing, and modeling their correct role(s) and responsibilities in the innovation cycle.
- *Military* – with specific focus on the domestic critical infrastructure dependence and challenges in cybersecurity collaboration with OGA and the private sector; along with a unified concept of operations and cybersecurity coordination (detection through response).

Crosscutting Themes

In each of the planned dialogues a series of inter-related topics will be explored. These topics not only have direct correlation to the cybersecurity challenges in U.S. critical infrastructure protection, but without a clear doctrine to drive U.S. action the isolated improvements in one area may have minimal effect nationally. The themes we will explore include:

Cyber-physical Systems

Cyber-Physical Systems (CPS) are smart, networked systems with embedded sensors, processors, and actuators designed to sense and interact with the users and support real-time, guaranteed performance in safety-critical applications. CPS systems are an increasing part of all national critical infrastructures, finding new applications of CPS technology to improve everyday life and even transforming views of a society and community. A 2014 NSTCA report projected a staggering 26-

to-50 billion cyber-physical devices will be deployed in manufacturing, business, and home applications by 2020.

Cyber-physical systems use dedicated communication channels to enable remote control of large industrial and manufacturing equipment such electrical generators and power transmission and distribution. These early systems were very specialized proprietary systems, separated from the Internet and its risks. The economic advantages of the Internet and increasing functionality of commodity networking and information technology, however, have incentivized the re-architecting of these systems, leading to new cybersecurity risks that now affect the safety and availability of the services provided by critical infrastructures. The threats include purposefully coordinated existential threats to national critical infrastructures. Cybersecurity will be a daunting challenge at this unprecedented scale with billions of unprotected low-end commodity networked devices in many diverse applications.

The Innovation Cycle

Sound cybersecurity research must have a basis in controlled and well-executed experiments with operational relevance and realism. That requires tools and test environments that provide access to datasets at the right scale and fidelity, ensure integrity of the experimental process and support a broad range of interactions, analysis and validation methods. Efforts to ground the research and provide protections to those organizations that voluntarily share their sensitive data with researchers remain problematic.

A well-articulated, coordinated process that transitions research discoveries into practice is essential to ensure high-impact federal cybersecurity R&D. The research community, which focuses on developing and demonstrating novel and innovative technologies, and the operational community, which needs to integrate solutions into existing industry products and services, are not always aligned. An effective technology transfer program must be an integral part of our national strategy and rely on sustained and significant public-private participation.

Workforce Development

The Quadrennial Review highlights workforce development as an area of required focus in order to protect critical infrastructure, such as the energy grid, from cyber-attacks. Given the increasing role technology plays in our critical infrastructure, it is vitally important that our nation has an adequate, viable cybersecurity workforce to ensure the security of our critical infrastructure, but also to address a myriad of national security and domestic issues.

This is a multi-dimensional challenge requiring concerted effort across many areas in which academia, national labs, and the government all must play a role. The race to respond to cyber workforce needs has led to inconsistency in program quality and stove piping of expertise. There is a need for consistent, high-quality cybersecurity curricula that is integrated with science and engineering programs at all levels in the university system and continual education and training exercises given the fast-moving nature of cybersecurity, as well as availability of practical training opportunities and outside-the-classroom activities that provide real-work experience.

Unified Concept of Operations

Recent data breaches suffered by companies including JPMorgan Chase, FedEx, Target, Sony, and health insurer Anthem – have spurred past Presidential action to call for stricter cybersecurity measures, including higher legal penalties for hackers and legislation that would facilitate better sharing of threat information between companies and government. Examples of both good and poor collaboration between government and industry post an attack exist, but efforts to date have left most companies uncertain about the best way to engage government, who to engage, how far to extend trust, and where the cyber risk management becomes an individual corporate issue vs. a national issue.

While the National Institute for Standards and Technology published a Framework for Improving Critical Infrastructure Cybersecurity in 2016,[2] there is currently no proven and adopted framework for U.S. industry and government in the event of cyber-attack on one or more corporate entities.

Information Sharing

One of the key findings from the 2013 PCAST cybersecurity report was the need to improve government in industry's capacity to respond, in real time, to cyber threats by sharing data on these threats more extensively—in appropriate circumstances and with publicly understood interfaces—between private-sector entities and Government. The importance of information sharing for critical infrastructure was also highlighted in PPD-21, and the Administration has encouraged legislative initiatives to address information sharing in all sectors.

But while pockets of excellence exist in effective information sharing and collaboration between industry and government (e.g. CRISP in the electrical sector), the expansion to and adoption by other critical infrastructures has been far too slow. Where scalable models exist, and have been proven over years of usage, there is a need for broader application and better definition of the role of the government in

[2] https://www.nist.gov/sites/default/files/documents/cyberframework/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf

encouraging and incentivizing scale-up and of industry's role in prioritizing and organizing for success. While President Trump's recent executive order seeks to protect critical infrastructure from cyber attacks by mandating a top-down review of cybersecurity and holds agencies accountable for safeguarding digital information,[3] there still lacks a mechanism for communication across different agencies and sectors.

Valuation of Cyber Security and Best Practices

Traditionally, cyber defenses and practices have been viewed as a cost that must be balanced against a risk that is being mitigated. This has led to a risk-based approach to identifying cyber vulnerabilities and threats that warrant the associated investment. This approach can lead stewards and owners of critical infrastructure to opt out of cyber defenses and best practices they view as cost-prohibitive given an assumption of likelihood or threat of cyber attack. This approach has proven to be costly when breaches occur. According to IBM's 2016 Cost of Data Breach Study, the total average cost of data break incidents for U.S. companies is $7.01 million, up from $6.53 million in 2015.[4]

If instead of viewing cyber technologies and practices through the lens of cost and benefit they were treated and valued as capital, owners and operators of critical infrastructure might arrive at very different priorities for investing in state of the art cyber capabilities. Providing a model for valuation of cyber security and best practices would require input from a diverse group that includes owners, operators and stewards of critical infrastructure, government regulators and oversight representatives, consumers of critical infrastructure services and products, the R&D and engineering community tasked with innovating in this area, and military and other representatives tasked with defending the infrastructure outside a profit motive.

Outcomes

The findings and recommendations around the six key themes garnered from each of the three dialogues will be synthesized into a national agenda articulating a policy doctrine on American cybersecurity.

From that doctrine, we will identify the "tent pole" actions that must be taken by specific organizations to meet the challenges and capitalize on the opportunities presented in the doctrine.

This doctrine will be shared widely with Congress, the Administration industry leaders and academia to drive action and protect American interests from the growing threat of cyber attack.

[3] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal
[4] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094USEN

APPENDIX B

Council on Competitiveness Membership, Fellows and Staff

BOARD

Chairman
Mr. Samuel R. Allen
Chairman and Chief Executive Officer
Deere & Company

Industry Vice-chair
Dr. Mehmood Khan
Vice Chairman and Chief Scientific Officer of Global Research and Development
PepsiCo, Inc.

University Vice-chair
Dr. Michael M. Crow
President
Arizona State University

Labor Vice-chair Emeritus
Mr. William P. Hite
Former General President
United Association

Chairman Emeritus
Mr. Charles O. Holliday, Jr.
Chairman
Royal Dutch Shell plc

President & CEO
The Honorable Deborah L. Wince-Smith
Council on Competitiveness

FOUNDER

Mr. John A. Young
Former Chief Executive Officer
The Hewlett Packard Company

EXECUTIVE COMMITTEE

Mr. Jim Balsillie
Co-founder
Institute for New Economic Thinking

Mr. Thomas R. Baruch
Managing Director
Baruch Future Ventures

Dr. Gene D. Block
Chancellor
University of California, Los Angeles

Mr. William H. Bohnett
President
Whitecap Investments LLC

Dr. James P. Clements
President
Clemson University

Mr. James K. Clifton
Chairman and CEO
Gallup, Inc.

Dr. John J. DeGioia
President
Georgetown University

Mr. George Fischer
Senior Vice President and Group President
Verizon Enterprise Solutions

Mr. Mike Fucci
Chairman
Deloitte LLP

Dr. William H. Goldstein
Director
Lawrence Livermore National Laboratory

Mr. James S. Hagedorn
Chairman and CEO
The Scotts Miracle-Gro Company

Dr. Sheryl Handler
President and CEO
Ab Initio

The Honorable Shirley Ann Jackson
President
Rensselaer Polytechnic Institute

Dr. Farnam Jahanian
President
Carnegie Mellon University

Dr. Pradeep K. Khosla
Chancellor
University of California, San Diego .

Mr. Brian T. Moynihan
Chairman and Chief Executive Officer
Bank of America

Gen. Richard B. Myers (Ret.)
President
Kansas State University

The Honorable Janet Napolitano
President
The University of California System-Regents

Dr. Harris Pastides
President
University of South Carolina

Mr. James M. Phillips
Chairman and CEO
NanoMech, Inc.

Mr. Nicholas T. Pinchuk
Chairman and CEO
Snap-on Incorporated

Professor Michael E. Porter
Bishop William Lawrence University Professor
Harvard Business School

Mr. Jonas Prising
Chairman and Chief Executive Officer
ManpowerGroup

Mr. Robert L. Reynolds
President and CEO
Putnam Investments

Dr. Mark S. Schlissel
President
University of Michigan

Mr. Lonnie Stephenson
International President
International Brotherhood of Electrical Workers

Mr. Steve Stevanovich
Chairman and Chief Executive Officer
SGS Global Holdings

Mr. Lawrence Weber
Chairman
W2 Group, Inc.

Ms. Randi Weingarten
President
American Federation of Teachers, AFL-CIO

Dr. W. Randolph Woodson
Chancellor
North Carolina State University

Mr. Paul A. Yarossi
President
HNTB Holdings Ltd.

Dr. Robert J. Zimmer
President
The University of Chicago

GENERAL MEMBERS

Dr. Jonathon R. Alger
President
James Madison University

Dr. Joseph E. Aoun
President
Northeastern University

Dr. Aziz Asphahani
Chief Executive Officer
QuesTek Innovations LLC

Dr. Dennis Assanis
President
University of Delaware

Dr. Eric Barron
President
Pennsylvania State University

The Honorable Sandy K. Baruah
President and Chief Executive Officer
Detroit Regional Chamber

Dr. Mark P. Becker
President
Georgia State University

Dr. Richard Benson
President
University of Texas at Dallas

Ms. Stephanie W. Bergeron
President
Walsh College

The Honorable Rebecca M. Blank
Chancellor
University of Wisconsin—Madison

Dr. Lee C. Bollinger
President
Columbia University

Dr. Robert A. Brown
President
Boston University

Mr. Al Bunshaft
Senior Vice President, Global Affairs
Dassault Systèmes Americas

The Honorable Sylvia M. Burwell
President
American University

Mr. John Chisholm
Chief Executive Officer
John Chisholm Ventures

Mr. Christopher Crane
President and Chief Executive Officer
Exelon Corporation

Mr. Bruce Culpepper
U.S. Country Chair & President
Shell Oil Company

The Honorable Mitchell E. Daniels, Jr.
President
Purdue University

Mr. Ernest J. Dianastasis
CEO
The Precisionists, Inc.

Dr. Joseph A. DiPietro
President
The University of Tennessee

Rev. Peter M. Donohue
President
Villanova University

Dr. Michael V. Drake
President
The Ohio State University

Dr. Taylor Eighmy
President
The University of Texas at San Antonio

Dr. Carol L. Folt
President
The University of North Carolina at Chapel Hill

Mr. Robert Ford
Executive Vice President, Medical Devices
Abbott

Mr. Kenneth C. Frazier
Chairman and Chief Executive Officer
Merck & Co., Inc.

Dr. Julio Frenk
President
University of Miami

Dr. W. Kent Fuchs
President
University of Florida

The Honorable Patrick D. Gallagher
Chancellor
University of Pittsburgh

Dr. E. Gordon Gee
President
West Virginia University

Dr. Amy Gutmann
President
University of Pennsylvania

Ms. Marillyn A. Hewson
Chairman President and CEO
Lockheed Martin

Rev. John I. Jenkins
President
University of Notre Dame

Dr. Jim Johnsen
President
University of Alaska System

Dr. Paul Johnson
President
Colorado School of Mines

Mr. R. Milton Johnson
Chairman and Chief Executive Officer
Hospital Corporation of America

Dr. Robert E. Johnson
Chancellor
University of Massachusetts Dartmouth

Dr. Eric Kaler
President
University of Minnesota

Dr. Timothy L. Killeen
President
University of Illinois System

Dr. Steven Leath
President
Auburn University

Dr. Laurie Leshin
President
Worcester Polytechnic Institute

Dr. Michael Lovell
President
Marquette University

Dr. Gary S. May
Chancellor
University of California, Davis

Mr. Sean McGarvey
President
North America's Building Trades Unions

Brig. Gen. John Michel
Director, Executive Committee
Skyworks Global

Mr. Jere W. Morehead
President
University of Georgia

Gen. Richard B. Myers
President
Kansas State University

Mr. Eloy Ortiz Oakley
Chancellor
California Community Colleges

Dr. Eduardo J. Padrón
President
Miami Dade College

Dr. Christina Hull Paxson
President
Brown University

Dr. Neville Pinto
President
University of Cincinnati

Mr. Scott Pulsipher
President
Western Governors University

Mr. John Pyrovolakis
CEO
Innovation Accelerator Foundation

Dr. L. Rafael Reif
President
Massachusetts Institute of Technology

Mr. Clayton Rose
President
Bowdoin College

Mr. Rory Riggs
Managing Member
Balfour, LLC

Mr. John Rogers
President and CEO
Local Motors

Mr. Douglas Rothwell
President and Chief Executive Officer
Business Leaders for Michigan

Dr. David Rudd
President
University of Memphis

Vice Admiral John R. Ryan USN (Ret.)
President and Chief Executive Officer
Center for Creative Leadership

Dr. Timothy D. Sands
President
Virginia Polytechnic Institute and State University

Mr. John Sharp
Chancellor
The Texas A&M University System

Mr. Frederick W. Smith
Chairman and Chief Executive Officer
FedEx Corporation

Dr. Charles Staben
President
University of Idaho

Dr. Joseph E. Steinmetz
Chancellor
University of Arkansas

Dr. Elisa Stephens
President
Academy of Art University

Dr. Claire Sterk
President
Emory University

Dr. Elizabeth Stroble
President
Webster University

Dr. Kumble R. Subbaswamy
Chancellor
University of Massachusetts Amherst

Dr. Satish K. Tripathi
President
State University of New York at Buffalo

Dr. Ruth Watkins
President
University of Utah

Dr. Adam Weinberg
President
Denison University

Dr. Kim A. Wilcox
Chancellor
University of California, Riverside

Mr. Keith E. Williams
Chief Executive Officer
Underwriters Laboratories Inc.

Dr. Mark S. Wrighton
Chancellor
Washington University in St. Louis

NATIONAL LABORATORY PARTNERS

Dr. Steven F. Ashby
Director
Pacific Northwest National Laboratory

Dr. Paul Kearns
Director
Argonne National Laboratory

Dr. Martin Keller
Director
National Renewable Energy Laboratory

Dr. Mark Peters
Director
Idaho National Laboratory

Dr. Michael Witherell
Director
Lawrence Berkeley National Laboratory

Dr. Thomas Zacharia
Director
Oak Ridge National Laboratory

CORPORATE PARTNERS

Baker Hughes

Intel Corporation

Morgan Stanley

Intrexon Corporation

UNIVERSITY PARTNERS

Oklahoma University

Texas A&M University

University of California, Irvine

NATIONAL AFFILIATES

Mr. C. Michael Cassidy
President and Chief Executive Officer
Georgia Research Alliance

Dr. Jonathan Fanton
President
American Academy of Arts and Sciences

Mr. Jeffrey Finkle
President
International Economic Development Council

Mr. Matthew Loeb
Chief Executive Officer
ISACA

Dr. Anthony Margida
Chief Executive Officer
TechGrit AMX2 LLC

Mrs. Sandra Robinson
President
IEEE-USA

Ms. Andrea Purple
President
ARCS Foundation Inc.

FELLOWS

Mr. Bray Barnes, Senior Fellow
Director, Global Security & Innovative Strategies,
Washington, DC

Ms. Jennifer S. Bond, Senior Fellow
Former Director, Science & Engineering Indicators
Program
National Science Foundation

Dr. Thomas A. Campbell, Senior Fellow
Former National Intelligence Officer for Technology,
Office of the Director of National Intelligence

Ms. Dona L. Crawford, Senior Fellow
President, Livermore Lab Foundation; and Former Associate Director, Computation, Lawrence Livermore National Laboratory

The Honorable Bart J. Gordon, Distinguished Fellow
Partner, K&L Gates LLP; and Former United States Representative (TN)

Mr. Thomas Hicks, Distinguished Fellow
Principal, The Mabus Group; and Former Undersecretary of the Navy, U.S. Department of Defense

Dr. Paul J. Hommert, Distinguished Fellow
Former Director, Sandia National Laboratories; and Former President, Sandia Corporation

Dr. Lloyd A. Jacobs, Distinguished Fellow
President Emeritus, The University of Toledo

Dr. Ray O. Johnson, Distinguished Fellow
Executive in Residence, Bessemer Venture Partners; and Former Senior Vice President and Chief Technology Officer, Lockheed Martin

The Honorable Martha Kanter, Distinguished Fellow
Executive Director, College Promise Campaign

The Honorable Alexander A. Karsner, Distinguished Fellow
Managing Partner, Emerson Collective

Mr. Dominik Knoll, Senior Fellow
Former Chief Executive Officer
World Trade Center of New Orleans

The Honorable Steven E. Koonin, Distinguished Fellow
Director, Center for Urban Science and Progress, and Professor, Information, Operations & Management Sciences, Leonard N. Stern School of Business, New York University; and Former Second Under Secretary of Energy for Science, U.S. Department of Energy

Mr. R. Brad Lane, Distinguished Fellow
Co-Founder & Chief Executive Officer
RIDGE-LANE Limited

The Honorable Alan P. Larson, Distinguished Fellow
Senior International Policy Advisor, Covington & Burling LLP; and Former Under Secretary of State for Economics, U.S. Department of State

Mr. Alex R. Larzelere, Senior Fellow
President, Larzelere & Associates LLC; and Former Director, Modeling and Simulation Energy Innovation Hub, Office of Nuclear Energy, U.S. Department of Energy

Mr. Abbott Lipsky, Senior Fellow
Former Partner, Latham & Watkins LLP

Mr. Edward J. McElroy, Distinguished Fellow
Former Chief Executive Officer, Ullico, Inc.

The Honorable Julie Meier Wright, Senior Fellow
Former Chief Executive, San Diego Regional Economic Development Corporation; and Former First Secretary of Trade & Commerce, State of California

Mr. Mark Minevich, Senior Fellow
Principal Founder, Going Global Ventures

Ms. Michelle Moore, Senior Fellow
Chief Executive Officer, Groundswell; and Former Senior Advisor to the Director, Office of Management and Budget, Executive Office of the President of the United States

Dr. Luis M. Proenza, Distinguished Fellow
President Emeritus, The University of Akron
Ms. Jody Ruth, Senior Fellow
CEO, Redstones

Ms. Jody Ruth, Senior Fellow
Chief Executive Officer
Redstones LLC

Mr. Reuben Sarkar, Senior Fellow
Former Deputy Assistant Secretary for Transportation, U.S. Department of Energy

Mr. Allen Shapard, Senior Fellow
Senior Director, Chair of Public Engagement Strategies
APCO Worldwide

Dr. Branko Terzic, Distinguished Fellow
Managing Director, Berkeley Research Group, LLC

Dr. Anthony J. Tether, Distinguished Fellow
Former Director, Defense Advanced Research Projects Agency, U.S. Department of Defense

Ms. Maria-Elena Tierno, Senior Fellow
Former Vice President, International Business Development, CH2M

Dr. Thomas M. Uhlman, Distinguished Fellow
Founder and Managing Partner, New Venture Partners LLC

Dr. William Wescott, Senior Fellow
Managing Partner, BrainOxygen, LLC.

Dr. Mohammad A. Zaidi, Distinguished Fellow
Member, Strategic Advisory Board, Braemer Energy Ventures; and Former Executive Vice President and Chief Technology Officer, Alcoa, Inc.

STAFF

Mr. William Bates
Executive Vice President & Chief of Staff

Mr. Chad Evans
Executive Vice President

Ms. Marcy Jones
Special Assistant to the President & CEO and Office Manager

Ms. Patricia Hennig
Vice President for Finance

Mr. Chris Mustain
Vice President for Innovation Policy and Programs

Mr. Gourang Wakade
Vice President

Mr. Michael Bernstein
Senior Policy Director for Innovation Policy and Programs

Ms. Katie Sarro
Senior Policy Director for Energy and Manufacturing Initiatives

Ms. Ta Tanisha Scott-Baker
Director for Information Technology and Services

Mr. Joshua Oswalt
Policy Analyst

Mr. Ross Jablon
Program Assistant

Mr. Alex Temple
Program Assistant

Mr. DeWayne Johnson
Finance Manager

APPENDIX C

EMCP Steering and Advisory Committees

EMCP STEERING COMMITTEE

Mr. Samuel Allen
Chairman and CEO
Deere & Company

Dr. Steven Ashby
Director
Pacific Northwest National Laboratory

Dr. Aziz Asphahani
Chief Executive Officer
QuesTek Innovations

Dr. Eric Barron
President
Pennsylvania State University

Dr. Richard Benson
President
University of Texas at Dallas

The Honorable Rebecca Blank
Chancellor
University of Wisconsin—Madison

Dr. Gene Block
Chancellor
University of California, Los Angeles

Mr. William Bohnett
President
Whitecap Investments LLC

Dr. James Clements
President
Clemson University

Mr. Christopher Crane
President & CEO
Exelon Corporation

Mr. Jeff Fettig
Chairman
Whirlpool Cororpation

Mr. George Fischer
Senior Vice President and Group President
Verizon Enterprise Solutions

Dr. Carol Folt
Chancellor
University of North Carolina Chapel Hill

Mr. Robert Ford
Executive Vice President Medical Devices
Abbott Laboratories

Mr. Craig Giffi
Vice Chairman Leader U.S. Consumer
& Industrial Products
Deloitte LP

Howard Gillman
Chancellor
University of California, Irvine

Dr. William H. Goldstein
Director
Lawrence Livermore National Laboratory

Mr. Jim Hagedorn
Chairman & CEO
The Scotts Miracle-Gro Company

Dr. Mark Hussey
Vice Chancellor
Texas A&M University

Dr. Gregory Hyslop
Chief Technology Officer
The Boeing Company, and
Senior Vice President
Boeing Engineering, Test & Technology

Dr. Farnam Jahanian
President
Carnegie Mellon University

Dr. Robert E. Johnson
Chancellor
University of Massachusetts Dartmouth

Dr. Paul Kearns
Director
Argonne National Laboratory

Dr. Martin Keller
Director
National Renewable Energy Laboratory

Dr. Laurie Leshin
President
Worcester Polytechnic Institute

Dr. Michael Lovell
President
Marquette University

Mr. Blake Moret
President and Chief Executive Officer
Rockwell Automation

Dr. Harris Pastides
President
University of South Carolina

Dr. Mark Peters
Director
Idaho National Laboratory

Mr. James Phillips
Chairman & CEO
NanoMech, Inc.

Mr. Ajita Rajendra
Chairman and CEO
A. O. Smith Corporation

Dr. Horst Simon
Deputy Director
Lawrence Berkeley National Laboratory

The Honorable Subra Suresh
Former President
Carnegie Mellon University

Dr. Kim Wilcox
Chancellor
University of California, Riverside

Mr. Keith Williams
President & CEO
Underwriters Laboratories Inc.

Dr. W. Randolph Woodson
Chancellor
North Carolina State University

Dr. Thomas Zacharia
Director
Oak Ridge National Laboratory

EMCP ADVISORY COMMITTEE

Dr. Diran Apelian
Alcoa-Howmet Professor of Engineering, Metal Processing Institute
Worcester Polytechnic Institute

Dr. Glenn Baker
Director of Engineering, Technology & Quality Services
Deere & Company

Dr. John Ballato
Vice President Economic Development
Clemson University

Dr. M. Katherine Banks
Vice Chancellor for Engineering
Texas A&M University System

Ms. Margaret Brooks
Office of Customer Success
Verizon Enterprise Solutions

The Honorable Nora Brownell
Founding Partner
ESPY Energy Solutions, LLC

Dr. Todd Combs
Associate Laboratory Director for Energy and Environment Science & Technology
Idaho National Laboratory

Ms. Dona Crawford
Associate Director for Computation Emeritus
Lawrence Livermore National Laboratory

Dr. James Davis
Vice Provost, Information Technology
University of California, Los Angeles

Mr. Chris Gould
Senior Vice President—Corporate Strategy
& Chief Sustainability Officer
Exelon Corporation

Mr. Scott Godwin
General Manager, National Security Directorate
Pacific Northwest National Laboratory

Dr. Klaus Hoehn
Vice President, Advanced Technology
& Engineering
Deere & Company

Dr. Gene Huang
Vice President & Chief Economist
Abbott Laboratories

Dr. Glen Lewis
Principal
Glen Lewis Group, LLC; and
Operations, Energy & Supply Chain Management
Advisor
University of California, Davis

Dr. Sethuraman Panchanathan
Executive Vice President, Office of Knowledge
Enterprise, and Chief Research and Innovation
Officer
Arizona State University

Mr. Robert Pleasure
Senior Advisor to the President
North America's Building Construction Trades
Department, AFL-CIO

Mr. James Porter
Founder & President
Sustainable Operations Solutions, LLC

Dr. Ramamoorthy Ramesh
Associate Laboratory Director for Energy
Technologies
Lawrence Berkeley National Laboratory

Dr. Douglas Rotman
Program Director
Lawrence Livermore National Laboratory

Dr. Carmel Ruffolo
Associate Vice President for Research
and Innovation
Marquette University

Dr. Mark Slavens
Vice President of Environmental Affairs
The Scotts Miracle-Gro Company

Mr. Dave Swihart
Senior Vice President Global Technology
& Operations
The Scotts Miracle Gro Company

Mr. David Szczupak
Executive Vice President Global Product
Organization
Whirlpool Corporation

Dr. Satish Udpa
Executive Vice President for Administrative
Services
Michigan State University

Dr. Bodgan Vernescu
Professor of Mathematical Sciences & Vice Provost
for Research
Worcester Polytechnic Institute

Dr. Mohammad A. Zaidi
Senior Advisor
Braemar Energy Ventures

APPENDIX D

Cybersecurity Dialogue Series Participants

Cybersecurity for Industry

February 7, 2018
Basking Ridge, NJ

Mr. Michael Baker
Director, Information Security and IT Risk, CISO
General Dynamics Information Technology

Dr. Ram Balasubramanian
Dean of Engineering
University of Massachusetts, Dartmouth

Mr. William Bates
Executive Vice President and Chief of Staff
Council on Competitiveness

Mr. John Battista
Assistant Regional Underwriting Manager
AIG

Mr. Michael Bernstein
Senior Policy Director
Council on Competitiveness

Mr. Randy Bishop
General Manager—Energy Infrastructure
Guardtime

Mr. Andrew Bochman
Senior Grid Strategist
Idaho National Laboratory—Boston

Ms. Margaret Brooks
Senior Manager, Risk Management
Verizon

Ms. Diane Brown
Vice President of Global Operations
Verizon Enterprise Solutions

Mr. James Carrigan
Managing Director—Security Solutions
Verizon

Dr. Jim Curtis
Assistant Professor, Department of Math and Computer Science
Webster University

Mr. Anthony Dagostino
Global Head of Cyber Risk
Willis Towers Watson

Ms. Martha Delehanty
Senior Vice President, HR Operations
Verizon

Mr. Seth Edgar
CISO
Michigan State University

Mr. George Fischer
Senior Vice President and Group President
Verizon Enterprise Solutions

Mr. Robert Ford
Executive Vice President—Medical Devices
Abbott Medical

Mr. Scott Godwin
General Manager, National Security Directorate
Pacific Northwest National Laboratory

Mr. Randy Hansen
Director—Homeland Security Programs
Pacific Northwest National Laboratory

Ms. Trina Huelsman
Vice Chairman
Deloitte LP

Dr. Farnam Jahanian
President
Carnegie Mellon University

Mr. Martin Kessler
Director
Information Security Officer, Verizon

Ms. Maria Koller
Director, Risk Management
Verizon

Mr. Mike Kosonog
Partner—Audit and Enterprise Risk Services Practice
Deloitte

Dr. Peng Liu
Director, Center for Cybersecurity, Information Privacy and Trust
Pennsylvania State University

Mr. John Loveland
Director—Product Marketing
Verizon

Ms. Annette Lowther
Director—HR
Verizon

Ms. Mary Ludford
Vice President, Deputy Chief Security Officer
Exelon Corporation

Mr. Michael Maiorana
Senior Vice President, Sales Public Sector
Verizon

Mr. Michael Mason
Senior Vice President, Chief Security Officer
Verizon

Ms. Chandra McMahon
Senior Vice President, Chief Information Security Officer
Verizon

Mr. Timothy McNulty
Associate Vice President—Government Relations
Carnegie Mellon University

Mr. Mark Minevich
Senior Fellow
Council on Competitiveness

Mr. Chris Novak
Director—VRTAC/Investigative Response
Verizon

Mr. Chris Oatway
Associate General Counsel
Verizon

Ms. Amber O'Rourke
Former Policy Analyst
Council on Competitiveness

Ms. Sara Orr
Senior Vice President, Chief Financial Officer
Verizon

Mr. Mark Petri
Electric Power Grid Director
Argonne National Laboratory

Ms. Margaret Powell
Senior Manager—Real Time Systems Security Engineering and Operations
Exelon Corporation

Dr. John Pyrovolakis
Founder and CEO
Innovation Accelerator Foundation

Mr. Scott Rauschenberg
Executive Director—Financial Planning and Analysis
Verizon

Mr. Daniel Roat
Senior Client Executive
Verizon

Dr. Carmel Ruffolo
Associate Vice President, Research & Innovation
Marquette University

Ms. Katie Sarro
Senior Policy Director
Council on Competitiveness

Mr. Alex Schlager
Executive Director—Security
Product Management
Verizon

Mr. Per Solli
CEO
PowerOn

Mr. Philip Susmann
President
Norwich University Applied
Research Institutes

Mr. James Taneyhill
Managing Principle
Verizon

Dr. Thomas Uhlman
Managing Partner
New Venture Partners

Ms. Vandana Venkatesh
Senior Vice President, General Counsel
Verizon Enterprise Solutions
Verizon

Ms. Eliza White
Former Vice President
Council on Competitiveness

The Honorable Deborah L. Wince-Smith
President & CEO
Council on Competitiveness

Cybersecurity: An Issue of National Security

April 25, 2018
Seattle, WA

Dr. Heidi Ammerlahn
Director, Homeland Security & Defense Systems
Sandia National Laboratories

Dr. Steven Ashby
Director
Pacific Northwest National Laboratory

Mr. Jeffery Baumgartner
Senior Advisor, Infrastructure Security and Energy Restoration
Department of Energy

Ms. Marie Benz
Client Partner
Verizon

Mr. Randy Bishop
General Manager—Energy Infrastructure
Guardtime

Mr. Craig Bowman
Vice President and Managing Director
Verizon

Dr. Lloyd Wayne Brasure
Director, Defense Programs
Pacific Northwest National Laboratory

Ms. Margaret Brooks
Senior Manager, Risk Management
Verizon

Mr. James Carrigan
Managing Director—Security Solutions
Verizon

Mr. Samuel Clements
Cyber Security Researcher
Pacific Northwest National Laboratory

Mr. Jerry Cochran
Chief Information Security Officer
Pacific Northwest National Laboratory

Mr. Paul Cunningham
Chief Information Security Officer
Department of Energy

Dr. Jim Davis
Vice Provost, Information Security
University of California, Los Angeles

Mr. Paul Dodd
Senior Technical Fellow
The Boeing Company

Mr. Seth Edgar
Chief Information Security Officer
Michigan State University

Dr. Barbara Endicott-Popovsky
Executive Director
Center for Information Assurance
and Cybersecurity

Mr. Mark Estberg
Senior Director
Microsoft

Mr. Chad Evans
Executive Vice President
Council on Competitiveness

Mr. Daniel Freedman
Fellow—Cyber Security
Lockheed Martin

Mr. Michael Furze
Assistant Director
Washington State Department
of Commerce

Mr. Scott Godwin
Strategic Partnerships and Delegate Initiatives
Pacific Northwest National Laboratory

Mr. Victor Gonzalez
Chief Information Security Officer
South Texas College

Mr. Robert Hanson
Director, Prioritization and Modeling
Office of Cyber and Infrastructure Analysis,
Department of Homeland Security

Mr. Carl Imhoff
Manager, Electricity Infrastructure Sector
Pacific Northwest National Laboratory

Dr. Susan Jeffords
Vice Chancellor of Academic Affairs
University of Washington-Bothell

Ms. Kristen Lantz
CTO Operations Lead
Lockheed

Ms. Aimee Larsen-Kirkpatrick
Global Communications Officer
Global Cyber Alliance

Mr. Steve LeFrancois
Director, Solutions Architecture
Verizon

Dr. Sukarno Mertoguno
Program Officer
Office of Naval Research

Mr. Matthew Myrick
Deputy Chief Information
Security Officer
Lawrence Livermore National Laboratory

Mr. Alex Nicoll
Industrial Security Architect
Rockwell Automation

Dr. James Peery
Global Security Directorate Associate Laboratory
Director (ALD)
Oak Ridge National Laboratory

Dr. William Pike
Director, Computing and Analytics Division
Pacific Northwest National Laboratory

Mr. Daniel Roat
Senior Client Executive
Verizon

Ms. Katie Sarro
Senior Policy Director
Council on Competitiveness

Ms. Heather Scott
Office of Cyber and Infrastructure Analysis
U.S. Department of Homeland Security

Ms. Bobbie Stempfley
Director, SEI CERT Division
Carnegie Mellon University

Mr. Clay Storey
Senior Security Manager
Avista Corporation

Rep. Gael Tarleton
Representative
Washington State Legislature

Mr. Zachary Tudor
Associate Laboratory Director, National & Homeland Security
Idaho National Laboratory

Mr. David Walter
Chief Operating Officer
Leisnoi, Inc.

Col. Gent Welsh
Commander, 194th Wing
Washington National Guard

Dr. William Wescott
CEO
Brainoxygen LLC

Ms. Jamie Winterton
Director of Strategy, Global Security Initiative
Arizona State University

Ms. Morgan Zantua
Director, Professional Workforce Development
Center for Information Assurance and Cybersecurity

Cybersecurity: Engaging Government & Policymakers

June 19, 2018
Washington, DC

Dr. Rosio Alvarez
Chief Information Officer
Lawrence Berkeley National Laboratory

Dr. Steven Ashby
Director
Pacific Northwest National Laboratory

Mr. Michael Baker
Chief Information Security Officer
GDIT

Mr. Bill Bates
Executive Vice President
Council on Competitiveness

Mr. Michael Bernstein
Senior Policy Director
Council on Competitiveness

Mr. Randy Bishop
General Manager—Energy
Guardtime

Ms. Margaret Brooks
Senior Manager—Risk Management
Verizon Enterprise Solutions

The Honorable Dan Brouillette
Deputy Secretary
U.S. Department of Energy

Mr. Dean Carpenter
Enterprise Account Manager
ISACA

Mrs. Andrea Cohen
Vice President, Federal Civilian
Verizon Enterprise Solutions

Ms. Sonya Cork
Vice President
Verizon Enterprise Solutions

Dr. James Curtis
Professor of Cybersecurity
Webster University

Ms. Megan Doscher
Senior Policy Advisor
U.S. Department of Commerce—NTIA

Mr. Chad Evans
Executive Vice President
Council on Competitiveness

Dr. Nathaniel Evans
Strategic Cyber Analysis and Research Lead
Argonne National Laboratory

Mr. George Fischer
Senior Vice President and Group President
Verizon Enterprise Solutions

Mr. David Gillers
Senior Counsel
U.S. Senate Committee on Energy and Natural Resources

Mr. Doug Grindstaff
Global New Business and Market Development
CMMI Institute

Ms. Karen Grunstra
Global Government Affairs
UL LLC

Ms. Sabra Horne
Director, Stakeholder Engagement for Cyber Infrastructure Resilience
U.S. Department of Homeland Security

Mr. Robert Ivanauskas
Federal Energy Regulatory Commission (FERC) Detailee
U.S. Senate Committee on Energy and Natural Resources

Dr. Farnam Jahanian
President
Carnegie Mellon University

Dr. Mark Johnson
Thomas L. Hash Endowed Chair for Sustainable Development & Director, Center for Advanced Manufacturing
Clemson University

Mr. Martin Kessler
Information Security Officer
Verizon Enterprise Solutions

Ms. Diana Liu
Statistician
Gallup, Inc.

Mr. Mike Maiorana
Senior Vice President—Public Sector
Verizon Enterprise Solutions

Ms. Anne McKenna
Distinguished Scholar—Cyber Law & Policy
Penn State University

Mr. Mark Minevich
Senior Fellow
Council on Competitiveness

Mr. Tim McNulty
Associate Vice President, Government Relations
Carnegie Mellon University

Colonel Ed Monarez
Strategic Advisor, Computing and Analytics Division
Pacific Northwest National Laboratory

Mr. Kevin Nally
Chief Information Officer
U.S. Secret Service

Mr. Matthew Noyes
Cyber Policy and Strategy Director
U.S. Secret Service

Dr. Chris Oehmen
Chief Scientist for Cyber
Pacific Northwest National Laboratory

Dr. John Pyrovolakis
Founder & CEO
Innovation Accelerator Foundation

Dr. Richard Raines
Director—Electrical and Electronics Systems Research
Oak Ridge National Laboratory

Mr. Scott Regalado
Director—Information Security
The Boeing Company

Ms. Evelyn Remaley
Deputy Associate Administrator—Office of Policy Analysis and Development
U.S. Department of Commerce—NTIA

Dr. Chuck Romine
Director—Information Technology Laboratory
National Institute of Standards & Technology

Ms. Katie Sarro
Senior Policy Director
Council on Competitiveness

Brig. Gen. Robert Spalding
Senior Assistant to VCSAF
U.S. Air Force

Ms. Bobbie Stempfley
Director, SEI CERT Division
Carnegie Mellon University

Mr. James Taneyhill
Managing Principal
Verizon Enterprise Solutions

Mr. Zach Tudor
Associate Laboratory Director
Idaho National Laboratory

Mr. Ellison Urban
Special Assistant to the Director
Defense Advanced Research Projects Agency (DARPA)

Mr. Roland Varriale
Cybersecurity Analyst
Argonne National Laboratory

Ms. Bridgette Walsh
Chief of Staff, Office of Cybersecurity and Communications
U.S. Department of Homeland Security

The Honorable Deborah L. Wince-Smith
President & CEO
Council on Competitiveness

Council on Competitiveness
900 17th Street, NW, Suite 700, Washington, D.C. 20006, T 202 682 4292
Compete.org

@CompeteNow
facebook.com/USCouncilonCompetitiveness
linkedin.com/company/council-on-competitiveness/