Carnegie Mellon University

Pacific Northwest NATIONAL LABORATORY

verizon

Compete. Council on Competitiveness

Cybersecurity for Industry

Ensuring Prosperity in a Digitial Economy

Overview

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 we change the way we approach and implement 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 3-5 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 risk 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.

CO-CHAIRS

Dr. Steven Ashby
Director
Pacific Northwest National Laboratory

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

Dr. Farnam Jahanian
President
Carnegie Mellon University

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

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 pre-competitive 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.

Key Themes

The State of Cyber-Physical Systems

Voluntary, industry-led cybersecurity standards, created in partnership with government, are needed.

Specialized, closed-circuit cyber-physical systems have been in place in large industrial and manufacturing equipment for years. 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.

In recent years, there has been exponential growth in these systems—particularly in the electric grid, oil and gas infrastructure, and transportation systems—through the proliferation of smart vehicles, and even household appliances. These new technologies, while increasing their functionality through digitization, have created new challenges. Integrity, availability and confidentiality of information begin to shift while security, vigilance and resilience on the part of industry become increasingly more important.

While the myth that cyber-attacks are often executed through air gaps—areas with indirect connections between computers 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, human error is one of the most significant challenges when it comes to securing critical infrastructure from cyber-attacks. Researchers at IBM, for example, found that 15 percent of all cyber attacks were carried out by insiders inadvertently,[1] while as many as 24 percent of attacks may be due to employee action/mistakes.[2]

Conversely, the rush to unmanned systems with little focus on security poses its own challenges. As the electrical grid and manufacturing facilities in the United States become more digitized and automated, human oversight is replaced by technological systems, and security risks increase as remote access to and monitoring of these systems is frequently done on unsecure networks that can be exploited easily by attackers. Basic blocking and tackling, including patching software, understanding where threats exist and monitoring employee practices must be improved to secure critical infrastructure in the United States.

In addition to its clear relevance to advanced manufacturing and critical infrastructure like the grid, cybersecurity has become an essential dimension of numerous other industries. Automation can cut manufacturing costs and increase profits for U.S. industry. The use of cyber-physical systems in biological science has the potential to reduce healthcare costs and increase access to care through the availability of remote medicine and automation. But in order to capitalize on these opportunities, systems integrity must be built into the configuration of devices, and processes developed for securing and reporting attacks on these new systems.

In many industries, including the medical device industry, there is a lack of clarity in federal guidelines on definitions for key terms such as encryption and communication. Companies are also relying on outdated risk matrices and would benefit significantly from industry-specific cybersecurity standards that go beyond the industry-level "guidance" that exists today. These standards would be a productivity enabler for enhanced global market share and would contribute significantly to U.S. competitiveness.

While standards are important, industry cannot wait for them to be put in place, as there is significant critical infrastructure that requires protection now. Of note, the introduction of 5G services may help push forward security measures more quickly and effectively.

1 *2016 Cyber Security Intelligence Index*, IBM X-Force Research, September 2016.

2 *2016 Data Security Incident Response Report*, BakerHostetler, 2016.

The Innovation Cycle: From Idea to Implementation

Security must be integrated into products and processes early on in the development cycle rather than being considered an add-on component.

Innovation is at the core of U.S. productivity and prosperity. But innovation-based competition, growing global innovation capacity and rising internal challenges in the U.S. innovation system create challenges around guiding new products from idea to implementation.

When it comes to funding research and innovation in the United States, bureaucratic processes make it difficult to transfer government R&D findings into the hands of industry effectively and quickly to create new products, industries and jobs. Funding is also often provided for a fixed period and tapers off, or even ceases, as government interest dwindles. This leaves potential game-changing innovation stranded prior to its release to market. Importantly, to underfund the federal commitment to research now is to create an innovation gap later that cannot easily be filled. The United States is in a moon race around innovation, and risks losing global leadership in critical technologies from artificial intelligence (AI) to big data to automation, while other countries make the necessary investments in these key areas hoping to assert global leadership and reap economic and societal value.

Academic institutions have recently become more progressive when it comes to sharing intellectual property as opposed to taking a more traditional, protectionist approach. This has allowed more products to secure the needed funding and to reach the market. However, universities must gain a greater understanding of the venture capital landscape and what these investors, and other industry funding sources, are looking for: projects with quick return on investment that have the potential to change the security landscape.

But research and patents are not, in themselves, a proxy for innovation and competitiveness. Sound research must have a basis in controlled, well-executed experiments with operational relevance and realism. A well-articulated, coordinated process that prioritizes large-scale implementation and experimentation and guides products to market using creative push- and pull-based models is important. An effective technology transfer program that relies on sustained and significant public-private participation is essential to ensuring high-impact federal R&D and, consequently, United States competitiveness not only in the cybersecurity space but across various industries.

Countries like China and Russia, for example, have driven innovation by seeking out the best and brightest talent and incentivizing them to develop products and services in these respective countries that can then be used to create a competitive advantage in the security sphere. While Russia becomes a leading offender in the use of cyber-attacks through deployment of artificial intelligence technologies and China increasingly invests in AI patents, the United States risks falling behind. Artificial intelligence is often cited as one of the most important drivers of future productivity and is a main security focus due to its rapid advancement. With AI coming online more quickly on the offensive side than on the defensive side, the need for innovation becomes greater than ever, but grows increasingly more challenging.

Given the widespread and deep integration of cyber-enabled systems in our society, cybersecurity must be recognized both as a multidisciplinary research problem and one that goes beyond just technological innovation. Security must become part of the normal development cycle as opposed to being a separate, or add-on, component. Additionally, as innovative ideas lead to new products and technologies, there is a growing need to protect intellectual property from theft by cyber-attack. Economic espionage through hacking costs the United States an estimated $400 billion a year, with some estimates ranging as high at $600 billion.[3] While the United States still outshines its competitors in many areas of research and technological development, rivals are increasingly pilfering and weaponizing intellectual property, and this has dire implications for cybersecurity.

Coordination and Collaboration in an Age of Cyber Threats

An overwhelming amount of data creates challenges with regard to credibility of cyber threats and ability to operationalize data.

Recent data breaches have spurred a government call for stricter cybersecurity measures, including legislation that would facilitate better sharing of threat information

3 Update to *The Report of the Commission on the Theft of American Intellectual Property*, National Bureau of Asian Research, February 2017.

between companies and the government. Examples of both good and poor collaboration post-attack between government and industry exist. But efforts to date have left many companies (especially SMEs) uncertain how best to engage government, who to engage, how far to extend trust and where the cyber risk management becomes an individual corporate issue versus a national issue.

Security is a collaborative game that is being played out as though it is everyone for themselves. Information sharing across companies and industries is essential, but requires standardization in the way organizations operationalize data—and value high-quality data—to internalize it and incorporate it into their operations in a meaningful way that improves security. With the volume of useful, actionable information greater than ever before, building relationships between entities that have a vested interest in sharing this information is critical.

Bureaucracy also often prevents rapid response and renders gathered intelligence outdated before it can be received and implemented in a useful manner. Many existing frameworks are very academic and are difficult to implement in large companies. Additionally, corporate responsibility to shareholders makes companies reluctant to disclose information about threats or attacks that could damage their public image. A balance must be struck between information sharing required for legitimate policy interests and guarding private enterprise interests, including obligation to shareholders and customers.

Cybersecurity: From Cost to Competitive Advantage

Cybersecurity must be transformed into a competitive advantage rather than a sunk cost by focusing on the confluence of risk, capabilities and resources.

All organizational levels, including company boards and C-suite leaders, must be engaged in cyber planning, response and recovery efforts.

As the benefits of technological advances like the Internet of Things and artificial intelligence are realized, cybersecurity can become a true competitive advantage rather than a sunk security cost. But currently, cybersecurity relies too heavily on fear, uncertainty and doubt. It should instead should focus on the confluence of risk, capabilities and resources with a level of transparency and honesty.

Part of transforming cybersecurity from a cost into a competitive advantage is being proactive in addressing threats rather than reactive to attacks. Scenario planning around theoretical attacks shows how vulnerable certain technologies can be to cyber-attacks, resulting in a panic response from board rooms. This is particularly true in industries where brand reputation plays a significant role—such as in the medical device industry. But standardizing the risk matrix grid and creating standard encryption and data storage at the industry level should be a pre-competitive issue essential to industrial and economic stability and can mitigate the fear of an attack.

Looking at cyber technologies and cybersecurity posture as valued capital rather than as a liability would alter the way owners and operators of critical infrastructure arrive at investment priorities. Companies must also ensure members of their leadership have comprehensive knowledge and understanding of security risks, threats and attacks. This includes providing full, candid disclosure of cybersecurity status to corporate board members. In some cases, it may also require organizational restructuring at the C-suite level to reflect the nature of cybersecurity as an issue of larger corporate relevance, rather than simply a technology problem. That shift means the chief information and security officer role is, in its current form, more aligned with the responsibilities of a chief risk officer.

Integrating cybersecurity into corporate operations in this way will generally produce a higher security posture that should, in time, be rewarded by the market. But there is also a need to benchmark companies' security posture based on adherence to cybersecurity standards. This would better allow for companies to turn cybersecurity management into a metric that can be reported to shareholders to create additional value that can be added to the bottom line.

Next-Gen Talent: A Cybersecurity Imperative

Industry and academia must work together to create a baseline curricula to educate a knowledgeable, cyber-savvy workforce.

Cybersecurity must be integrated into educational curricula outside traditional four-year universities and post-grad studies, including high schools and community colleges.

Protecting critical infrastructure from cyber-attacks is not only a technological issue, but a talent issue. It is vitally important for the United States to have an adequate, viable cybersecurity workforce to address a myriad of national security and domestic issues. 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 collectively, while meeting current and future needs will be a key driver of American competitiveness in this burgeoning field.

As technology continues to evolve and cybersecurity becomes more mainstream, there is a growing demand for cyber-savvy professionals across all organizational areas. By some estimates, the number of unfilled cybersecurity positions will top 1.5 million by 2020.[4] Other estimates have the projected shortfall of cybersecurity professionals as high as 3.5 million by 2021.[5]

Additionally, small- and mid-sized companies often have difficulty competing with the Googles, Amazons and Apples of the world to attract talent from an already limited pool, particularly at lower organizational levels. In such instances, it could be beneficial for these companies to embrace a shorter tenure among entry-level professionals and allow for new talent to circulate throughout the organization and bring in new ideas and perspectives.

To create enough talent to fill the growing number of cybersecurity jobs, diversity and inclusion will be essential. Currently, women comprise just 14 percent of the information security workforce in North America. This is 34 percentage points lower than the average of women in the workforce.[6] Increasing gender diversity in the cyber workforce will increase the overall pool significantly. Immigration policies will also be important to expanding the workforce and ensuring companies are able to secure the talent needed to build resilience to the growing threat of cyber-attack.

Cybersecurity cannot, however, be delegated to a few individuals. It must instead be part of a skill set held by the many. All employees, not just at the policy level, need to be more cyber-savvy. A survey conducted by Willis Towers Watson of a combined 163 U.S. and U.K. employers found that about half of over 4,000 employees surveyed spent less than 30 minutes on training in the last year.[7] Many companies and organizations do not practice simple security hygiene, such as implementing two-factor authorization. Laptops and mobile devices are often not patched properly, creating added risk. Mechanical experts, while skilled in developing systems, often lack basic security knowledge and vice-versa. Cyber-informed engineering at the convergence of these two key spheres is essential.

At the university level, new programs focusing specifically on cybersecurity are increasingly being added to existing curricula. But educating the future cybersecurity workforce also will require a multidisciplinary approach that include cross-training and hands-on experience, as well as interaction with cybersecurity professionals and graduate-level students. This provision of additional opportunities outside the classroom would help combat the slow pace of curriculum change. Partnerships between industry and academia to create cybersecurity internship programs like, for example, Verizon's three-week "winternship" program or the idea of "scholarships for service," would be particularly useful.

While unfilled cybersecurity positions in industry pose a significant challenge, academia faces a similar issue in recruiting the talent necessary to train students in cybersecurity. Both industry and academia would benefit from cross-pollination and the cycling of cybersecurity professionals through both worlds. Not only would this help universities build the capacity to teach their cybersecurity curricula, it would ensure students are equipped with industry-relevant skills needed to enter the workforce.

Finally, educating on cybersecurity and computer science is not only the responsibility of colleges and universities. The introduction of college-level courses in cyber or computer science at the high school level would help bridge the digital divide and properly prepare students for the fast pace of change in the sector, while illuminating new career paths for future workforce participants. Community colleges, with the support of industry executives, are another option, but are often overlooked and underutilized.

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

5 *Cybersecurity Jobs Report*, Cybersecurity Ventures, May 2017.

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

7 *2017 Cyber Risk Survey Report*, Willis Towers Watson, June 2017.

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/

Cybersecurity Dialogue Participants

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. John Battista
Assistant Regional Underwriting Manager
AIG

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
Group President
Verizon Enterprise Solutions

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

Mr. Scott Godwin
Strategic Partnerships and Delegate Initiatives
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
Fellow
Council on Competitiveness

Mr. Chris Novak
Director—VRTAC/Investigative Response
Verizon

Mr. Chris Oatway
Associate General Counsel
Verizon

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

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

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

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

Mr. Michael Bernstein
Senior Policy Director
Council on Competitiveness

Ms. Amber O'Rourke
Policy Analyst
Council on Competitiveness

Ms. Katie Sarro
Senior Policy Director
Council on Competitiveness

Ms. Eliza White
Vice President
Council on Competitiveness