APPENDIX A

Ten Cybersecurity Items for the President's First 100 Days

Some of the recommendations in this volume are tonal (act with greater urgency) and hard to immediately measure, while others clearly could take substantial time to implement (government reorganization). Here is a short list of items that the new administration can announce in its agenda for the first 100 days and can be accomplished within the first year or sooner.

- Leverage existing partnership structure in the National Infrastructure Protection Plan to begin pilot testing the NIST Cybersecurity Framework for cost effectiveness and prioritization for small companies.
- Require all federal agencies to demonstrate cost effectiveness for all cybersecurity regulations programs promulgated on the private sector.
- Initiate reform of cyber compliance model to reflect cyber maturity improvements as opposed to pass-fail compliance.
- Using the same model that created the NIST framework in conjunction with federal agencies, develop menus of market incentive programs for cybersecurity, as called for in Executive Order 13636.
- Federal agencies shall coordinate among themselves and with states and localities and eliminate duplicative cyber regulations among jurisdictions.
- Initiate public awareness program on law enforcement cyber roles and responsibilities by leverage private sector associations.
- Initiate a cybersecurity education program for senior government officials modeled on the program run by National Association of Corporate Directors.
- Require federal agencies operating cyber partnership programs to follow best practices for private-sector engagement as reported in the *Journal of Strategic Security* in Winter 2015.[1]
- Reform clearance process allowing for ability to transfer the holding of clearances to different government agencies and retaining them with U.S.-based employment changes.

[1] See Clinton, Larry. "Best Practices for Operating Government-Industry Partnerships in Cybersecurity." Journal of Strategic Security 8, no. 4 (2015): 53-68.

Appendix B – Briefing Memos

Chapter 1: A Brief History of the Cybersecurity Problem and Policies That Have Attempted To Address It

Larry Clinton, President and CEO, Internet Security Alliance

The Problem: It's Really Bad—and About to Get Much Worse

The Internet was designed in the '70s and '80s to be an "open" system, not a secure system. The core protocols that the Internet is based on are insecure by design. In addition, new software services and applications tend to be built on these core protocols and so modern innovative products inherit the original vulnerabilities. This trend will be exacerbated by the explosion in mobile devices and the Internet of Things.

The Attack Community is Growing Much More Sophisticated

Nearly a decade ago, the National Security Agency coined the term Advanced Persistent Threat. APT was originally used to describe the ultra-sophisticated, multi-staged cyber-attacks we had begun to see between nation states and the defense establishment. We are now seeing these same sorts of attacks being launched throughout the cyber ecosystem. The Advanced Persistent Threat has now become the Average Persistent Threat.

All the Economic Incentives in Cybersecurity Favor the Attackers

When one considers the economic balance—the cost benefits of cybersecurity—it quickly becomes apparent that the economic balance overwhelmingly favors the attackers. Cybercriminals have an extremely attractive business model. Unlike many traditional illicit enterprises that require the use of a large, unreliable workforce and long supply-chains, cyberattacks require comparatively small workforces that can be safely located far from disruptive civil forces. Attackers generally have first mover advantage in deciding who, when and how to attack, often based on stealthy reconnaissance. Defense is historically a generation behind the attacker. Complicating the economic imbalance, many of the technologies and business practices that are required for enterprises to operate successfully in a worldwide competitive market tend to undermine cybersecurity.

Why Traditional Mechanisms Are Failing to Provide Security

They Were Designed for a Different Type of Problem

Traditional mechanisms such as independent regulatory agencies, consumer lawsuits and government regulation are proving ineffective in adequately bolstering our security in light of the modern threats. Much of our traditional regulatory processes and judicial enforcement are designed to address malfeasance. However, the core problem with cybersecurity is not that the technology is poorly constructed or companies are unwilling to invest in reasonable security. It's that the technology is under attack.

Government Doesn't Have the Credibility Needed to Regulate For Cybersecurity

There is no evidence that government has attained that degree of expertise in cybersecurity. In fact, the data suggests the opposite. Greg Wilshusen, director for info security at the Government Accountability Office, explained in congressional testimony some of the reasons why. Among them, "Government agencies follow what IT pros call a policy based approach to cybersecurity where agencies check off a list of requirements set by lawmakers and regulators that they have to follow."

Government is Not Properly Structured to Deal with the Digital Age

A Bank of America Merrill Lynch 2015 report found that "The U.S. government is still in the process of determining who will have jurisdiction in cyberspace. As the Department of Defense, DHS, and their subordinate organizations like the Air Force, Navy, Army, Defense Agencies and Commands battle for jurisdiction and funding. The result is a fragmented system muddled with a political agenda which hinders the development of a more secure system."

Even If Government Were Up To the Task, the Regulatory Model Doesn't Fit the Problem

The expert agency regulatory model, wherein an elected body empowers a regulatory agency to specify requirements for the private sector essentially attempt to locate a static standard that assures safety wherever producers are in compliance. Technology and attack methods change constantly and quickly. The traditional regulatory process cannot keep up with the evolution of what constitutes the required cybersecurity at any given time.

There is a role for regulation in certain spaces, such as requirements to notify citizens when their personal data has been compromised, or in industries where the core economics of the industry are already intimately involved in regulation, such as municipal water services. But traditional regulation is generally falls short as an effective sustaining private sector cybersecurity, due to the nature of government and the nature of the problem itself.

Other Industrial Age Control Mechanisms Are Not Working, are Inappropriate and May Be Counterproductive

Disclosure Models Don't Fit the Digital Age

While citizens have an obvious right to know if their personal data has been compromised (as virtually every state now demands), disclosure as a motivator for improved security is too blunt an instrument to achieve our broader goals.

Court Action Is Proving Ineffective

Notwithstanding the hype from the plaintiff's bar, the predicted (for 10 years) avalanche of lawsuits by consumers harmed by cyberattacks and the resulting improvements in security to avoid such suits has not materialized. One of the main reasons for this mechanism's failure to promote the needed security upgrades is that the suits are usually unsuccessful.

The Path Forward I: The Cybersecurity Social Contract

The concept of the social contract initially focused on the relationship between the individual and the state and what each would exchange with the other in order to achieve broader social order and benefit for the community. In the early 20th century, the social contract was adapted to the exchange between corporations and the state in order to achieve mutual and greater benefit for the social order.

At the time, the hot technologies were telecommunications (phones) and distributed electricity. Initially these services were provided where the economies justified them: urban and affluent areas. The policymakers of the era understood that universal service of these technologies would have broad social benefit, but also realized government couldn't accomplish this on its own. Moreover, compelling the private sector to provide the services without adequate compensation would be an unsustainable model.

So, a “social contract”—essentially an economic deal—was developed. Private companies agreed to provide universal service at regulated rates. In exchange, the government agreed to guarantee a substantial rate of return on their investments. Thus was born rate-of-return regulation and the private investor owned public utility.

Critical to understanding the social contract as applied to infrastructure development in the United States is the realization that not only did it enhance the greater public good, but that there was an economic exchange in return for this societal benefit. Moreover, the infrastructures, adequately supported by the economic incentives imbedded in the contract, were continually made more sophisticated and innovative. The rapid development of these infrastructures provided the foundation for accelerated industrialization, job creation and innovation.

In its 2008 and 2009 publications, The Cybersecurity Social Contract and the 2.0 versions, ISA argued that a similar situation exists today with respect to cybersecurity.

In the ensuing years we have seen substantial progress at the conceptual level as the private sector and both political parties have gravitated toward embracing the Cyber Social Contract model.

President Obama’s signature policy paper on cybersecurity, “The Cyber Space Policy Review” made ISA’s Social Contract publication it’s first and most frequently cited reference. In 2013, the president issued an executive order on cybersecurity that also embraced the principles in the Cyber Social Contract. The president abandoned the traditional regulatory approach and instructed the National Institute of Standards and Technology to identify the appropriate standards and practices which ought to be voluntarily adopted by the private sector and reinforced by the development of market incentives.

Although we have now developed a broad consensus on the conceptual approach we need to follow progress on implementation has been slow. As we turn to a new administration and Congress, there is still a great deal of work to be done, at both the macro and micro level, to build on the consensus that has been developed and implement a secure cyber system that is both technologically responsive to the evolving threat and economically sustainable.

Chapter 2: A Twelve-Step Program for Implementing the Cybersecurity Social Contract

Larry Clinton, President and CEO, Internet Security Alliance

1. We Need to Attack the Cybersecurity Problem with Much Greater Urgency

Compared to the speed with which our information technology systems are being compromised, federal policymaking has moved at a glacier pace, due to bureaucratic processes and constant turf battles. A new president can do a lot to set the proper aggressive tone to address the issue. Cybersecurity needs to figure prominently in the new president's first hundred-day agenda.

2. Government Needs to Recognize the Importance of Economics in Cybersecurity

The critical factor for addressing cyber risk is cost. Economics is the driving force for private sector behavior yet in cybersecurity virtually all economic incentives favor the attacker. Government needs to integrate cybersecurity issues into its broader infrastructure programs. In recent years, government has appropriated billions of dollars for innovative digital programs without properly apportioning funds to assure these new systems are secure. Cybersecurity is more of an economic issue than an IT issue yet government policy ignores the economics. The new administration needs to expand the focus on cybersecurity beyond the IT silo, embrace the broader nature of the problem, and rebalance the economic incentive structure.

3. Government Needs to Dramatically Increase Funding for Cybersecurity

The private sector spends twice as much on cybersecurity than the entire departmental budget for DHS. Improving cybersecurity will cost money and government funding needs to increase in order to improve security for the entire system. In a digital environment where systems are shared, government must partner with industry, even spending public monies to support private systems whenever the latter are vital to the national interest.

4. Government Needs to be Organized to Reflect the Current Digital Realities

The chaotic and disorganized governmental structures are inefficient, and most of government's organizational problems emanate from the lack of responsiveness to the digital age. All current and future government cybersecurity programs need to have clear objectives that are subject to a cost benefit analysis. The incoming administration and Congress need to seize the opportunity to reorganize for the digital age, and government needs to fully integrate the private sector into its cybersecurity planning and operations.

5. We Need to Focus More on Cybersecurity from a Law Enforcement Perspective

Law enforcement efforts for cybercrime are minimal. Law enforcement agents are vastly overmatched in terms of scope of the problem compared to resources available. Plus, the legal structure, particularly internationally, has not adapted to deal with modern cybercrime. The new administration should engage in a multi-tiered program to bolster cyber law enforcement, review legacy law enforcement spending, and help create a practical, operational international legal structure to address international cybercrime.

6. Pilot Test the NIST Cybersecurity Framework

One of the most positive and popular cybersecurity initiatives of the Obama administration was the creation of the NIST Cybersecurity Framework in 2013. We need to test the NIST Framework for effectiveness, cost effectiveness and prioritization. These elements are called for in Executive Order 13636 yet virtually nothing has been done on them. No private sector organization launches a new product or service without testing it, yet three years into the NIST Framework and still no single objective piece of evidence exists to show it has changed behavior, or if such change has been for the better and at what cost.

7. Government Priority for Working with the Private Sector Should be Reversed to Emphasize Smaller Companies Instead of Large Ones

We need to focus more on smaller companies. Smaller companies are more vulnerable than larger ones, understand the issue less, are investing less and are probably the segment that most needs government help. Small companies are used as access points for sophisticated attacks on larger firms. We cannot develop a sustainably secure system by focusing exclusively on large companies. While government must continue to work with larger companies, it must also increase emphasis on smaller companies, and make cybersecurity easier and cheaper for SMBs.

8. Workforce Development: Awareness Yields to Understanding and Making Cybersecurity Cool

We need to be much more creative in terms of workforce development. We need to leverage the private sector far more, use the gaming community to attract kids, and integrate cybersecurity into existing programs rather than treating like separate issues. We need an integrated, multi-faceted and targeted program with research based messaging. Career influencers, such as high school, community college and university guidance counselors, need to be targeted with proper messaging so they can assist in cyber career development. The new administration should prioritize coordination of outreach programs with the private sector, facilitate partnerships, and allow the private sector to lead workforce development programs.

Government should focus on training at the top. The National Association of Corporate Directors operates a highly successful (independently verified) program to train corporate boards about cybersecurity. We need a similar training program for members of Congress, agency heads, and cabinet officials.

9. Modernize and Streamline Regulation

The explosion of cyber regulations has occurred regardless of policies promoting voluntary usage of the guidance like the NIST Cybersecurity Framework. Companies now often face multiple inconsistent regulatory and quasi-regulatory systems that more likely hinder cyber efforts than help. Security professionals are routinely diverted away from actual security to compliance, making regulations counter-productive to security efforts. Governmental turf battles and bureaucratic inertia have stymied any significant measures to streamlining the regulatory process. The new president ought to charge the Office of Information and Regulatory Affairs with developing a cross-government program for streamlining regulations. Congress should aggressively require federal agencies to reduce duplicative regulations and eliminate those that have not been proven to be cost effective as a condition of their annual appropriations.

10. Develop Market Incentives to Promote Sound Cybersecurity Behavior

Policy makers have not thought through the incentive discussion broadly or creatively. Most view incentives as taxes or tax breaks. However, taxes are too limited in perspective. Some may even incentive innovation by the attack community while disincentivizing corporations to improve cybersecurity. Altering the assessment and compliance process and moving away from a "pass-fail" audit model to a more useful maturity model can create incentives without increasing government spending. The private sector has offered multiple proposals for consideration including liability incentives, procurement incentives; insurance incentives; and good actor benefits such as streamlined regulation, patent or trademark preferences, forbearance, and streamlined auditing.

11. Articulate Clearly the Role for Government when Industry Faces a Nation-State Attack

Many cyberattacks are affiliated with nation-state actors. Virtually no private institution can adequately defend itself from a concentrated nation-state attack. Legal precedent going back decades in the nuclear industry by virtue of the design basis threat theory provides that private entities are not responsible for securing themselves from nation-state activity, but rather the federal government is. However, there is no clear policy or systemic assistance private companies can expect from the federal government when dealing with nation-state cyber threats. The federal government should offer (on request) equivalent federal assistance to private companies that suffer a cyberattack by a nation-state as if it were a physical attack.

12. Government and Industry Need to Partner to Rethink the Cybersecurity Compliance Model

The traditional regulatory model is ill-suited to the cyber space. Instead of the current backward-looking, finance-based, pass-fail, blame-the-victim model, we need to create a forward looking, risk management model powered by growth and incentives, not penalties and compliance. The new administration must work collaboratively with the private sector to develop this model.

Chapter 3: Cybersecurity in the Defense Industrial Base

Jeff Brown, Chief Information Security Officer, Raytheon
JR Williamson, Corporate Chief Information Officer, Northrup Grumman

What Makes the DIB Sector Unique

The defense industry has a different economic model than most industries, and investing in cyber protection is not a function of traditional economic risk management. Top tier defense companies sell to national governments with few alternatives, and the Pentagon is unlikely to opt for lower cost products from rival nations, especially should the design suspiciously resemble American-made technology.

The defense industry invests in cybersecurity despite the lack of traditional economic out of a fundamentally patriotic sense of responsibility to our warfighters and because strong data and network security is essential to brand credibility when doing business with the military.

However, small- and medium-sized companies lower in the defense supply chain have a greater proportion of commercial business than defense business, The greater the commercial component of a business, the more traditional economic risk assessment calculations predominate. Financial conditions facing SMBs do not afford them the luxury of uneconomic investments in cybersecurity

Differences in incentive structures has created a two-tiered defense ecosystem. One tier contains the large, well-funded system integrators; the other, everyone else. Into this mix, DoD has introduced new compliance requirements, in an attempt to artificially influence traditional economic-based risk management calculations.

Challenges Facing the New Administration

Modern weapons systems are built via a supply chain hundreds of companies long, spanning multiple countries, and subject to cyber manipulation. Defense developers and innovators are at risk of intellectual property theft through cyberespionage. Second level nations skip generations of research development, becoming competitive with U.S. weaponry, and the economic losses portend negative downstream effects on future investment and innovation.

Government reporting and information sharing requirements are confusing and divert resources away from security to compliance. New regulations have significantly increased costs of doing business with the government, and shifted cybersecurity focus from incentives, as called for in Executive Order 13636, to compliance with standards. These increased costs dwarf information technology budgets for small businesses. However, compliance alone will not generate security and must not be confused with it.

The collaboration process codified in the Defense Industrial Base Framework Agreement has been successful, but is labor intensive. Cyber threats have expanded to attack the defense supply chain, an ecosystem of smaller, less cyber-capable companies, ill-suited for such processes.

Cybersecurity policies assume U.S.-based companies operating on American soil. Yet, reductions in defense spending led many companies to expand their presence overseas, creating a very different set of dynamics for cyber defense in the sector. The requirements levied by the International Trafficking in Arms Regulations drives the defense industry into maintaining two distinct networks—one for U.S. persons and one for non-U.S. employees—making a unified cyber defense both difficult and expensive. Privacy laws of many of countries also make a unified monitoring environment difficult.

Most countries now require co-production or offset suppliers. As the demand for co-production rises in the value chain, so does the need to defend the networks of suppliers, resulting in policy challenges to the defense industry in two areas: first, current information sharing policies preclude open sharing of information with foreign partners; and second, the Defense Federal Acquisition Regulation Supplement rules on safeguarding defense information mandate application of NIST controls to overseas suppliers anytime covered information is involved. But, few foreign companies are likely to submit themselves to DoD imposed standards, leaving defense companies to choose between continuing with a foreign supplier who is out of compliance or abandoning the supplier and failing to meet contractual offset requirements.

Recommendations

Institute a tiered model for grading cybersecurity competency

The current regulatory compliance model is binary – either comply with everything or fail. Turn it into an incentive model with different tiers of compliance, where each level represents a concrete improvement in security. Companies will then prioritize efforts, and the government and larger defense contractors could tailor contract requirements to a certain level of security, incentivizing suppliers to move to the next tier to gain eligibility for larger contracts. This would transform the compliance environment to a competitive one, which will then incentivize defense companies to advance tiers in order to set themselves apart from their peers or gain market share. A maturity model would also allow small and medium-sized defense contractors to realistically participate.

Information Sharing Beyond the Elites

Current close-hold information sharing methods are designed for companies with the infrastructure and staff capable of manually receiving complex threat data, evaluating it for their environment, and applying it to any number of defensive systems. Small companies cannot do this. Instead, sharing with small companies requires a passive model where the company can accept threat data in an automated system and have it applied to their network. The Pentagon needs to work with industry to create a broader information sharing environment that is affordable and passive. Defense can allow large system integrators to share DoD-provided, unclassified threat indicators with defense contractors in their supply chain via automated monitoring systems. Extending to the supply chain can have a high payoff at a low cost.

DoD should move to better accommodate a global defense industrial base

Defense needs to work with industry to develop operating concepts for cyber defense in an increasingly global market. Compliance regimes and information sharing processes must both be modified to accommodate overseas suppliers and co-production agreements. They must also work to develop a way to share cyber defense information with foreign suppliers of critical items. DoD should work with NIST to find an acceptable international standard that can serve as an overseas substitute for defense controlled information cybersecurity controls.

The Pentagon needs to increase its focus on small businesses

Defense depends on small businesses to support its missions, spark innovation, and develop technologies to support soldiers. While the Office of Small Business Programs has acknowledge that cybersecurity is an important and timely issues for small businesses, it has not identified or disseminated any cybersecurity resources in its outreach and education efforts to defense small businesses. The next

administration should ensure cybersecurity is a part the OSBP outreach and take steps to stabilize the office's performance and leadership team.

Chapter 4: Cybersecurity in the Healthcare Industry

Dustin Wilcox, Vice President and Chief Information Security Officer, Centene

What Makes the Healthcare Sector Unique

Patient data is uniquely valuable to criminals. The cost to purchase stolen patient records on the cyber black market is approximately ten times the cost of purchasing that same individual's stolen credit card data, and includes all data elements necessary to impersonate the victim. Hackers further monetize health records by compromising weaknesses in the healthcare system, billing fraudulent claims to Medicaid and Medicare, potentially prescribing narcotics, and even filing fraudulent tax returns.

Perhaps the most interesting evolution in the cyber-threat facing healthcare industry is the rise of the nation-state threat. Governments of other countries direct their cyber warriors to hack into hospitals and health insurers to steal medical records. It's likely that nation-state actors are stealing patient data to build databases on American citizens for espionage activities.

Insider threats are particularly insidious in the healthcare sector. Healthcare data processors say malicious insiders for just about 10 percent of data breaches but are the root cause of double the percentage of medical identity thefts. Accidental insiders cause more, albeit smaller, breaches.

The number of individuals who have access to data during a healthcare transaction represents another point of vulnerability. Even a routine visit to the doctor exposes medical data to a dozen people or organizations as diagnostic and billing information makes its way through various systems. Each hand represents another potential point of vulnerability or attack.

Challenges Facing the New Administration

Two major laws governing healthcare cybersecurity practices are not functioning as intended. The massive 2013 omnibus rule updating HIPAA, mandated by the HITECH Act, has failed to have the desired effect of making the healthcare industry more secure. In the years since its implementation, massive health payer data breaches have occurred.

Moreover, the regulations take a retributive approach to cybersecurity, punishing organizations that get breached. Breaches spawn audits, and audits spawn punitive outcomes in the forms of substantial fines and other penalties, regardless of much time and money was put into trying to prevent a breach.

The cost of security is a great obstacle for healthcare organizations. Large organizations have the ability to fund teams dedicated to both implementation of security best practices and regulatory compliance. Small practices have minimal resources. While all organizations must abide by the same rules and regulations, not all have equivalent access to the financial resources and expertise necessary to comply. The high cost of compliance, and the higher cost of failure, further exacerbates the problem.

The doctor-patient relationship is unique—patients are unlikely to abandon their medical provider over a data breach, so there is little incentive beyond regulatory consequences to spend time and effort defending against potential breaches.

The proliferation of technology in healthcare is another obstacle. Like most disruptive technologies, the uses for mobile enabled practice management systems multiplied long before any serious thought was given to securing the technology.

Escalating ransomware attacks on the healthcare industry creates another challenge. For now, ransomware attacks appear unconnected to data theft. But given the real value of patient data—in its theft for exploitation or resale—ransomware attacks will become the nasty second jab of what really are one-two punch attacks.

Possible cyberterrorist attacks against newly-networked medical devices coming onto the market could cause significant disruptions, some even fatal. Life-sustaining devices once isolated away from public networks are now exposed to them. Medical equipment is now part of the mix of databases and hard drives once thought impervious to hackers.

There's also a lack of urgency within the healthcare industry. The idea that medical data had value to criminals is novel, and it took significant healthcare data breaches to convince the industry to get serious about committing resources to secure itself against cyberattacks.

Recommendations

Incentivize Healthcare to Implement Best Cybersecurity Practices

Healthcare needs a shift in focus away from prescriptive regulation toward regulation that encourages security best practices. An incentive-focused regulatory approach would encourage more healthcare companies to invest in necessary protections to information assets, possibly even driving broad adoption of controls necessary to solve the aforementioned data problems. What's needed is a sliding scale of liability protection based on company's progress toward implementing an objective set of practices based on the company's progress toward implementing an objective set of practices. The NIST Cybersecurity Framework, and the process used to develop it, could provide a good starting point for determining those practices.

The system should allow a company to accrue credits tied to its investments in security that it could use against future audits and fines in the event of a breach. This could be taken further by also offering modest tax incentives for certain high-value, but often overlooked security best practices, such as employee awareness training.

Reduce Regulatory Complexity

Congress should pursue legislation that harmonizes privacy, security and information risk management requirements to eliminate the complex patchwork of regulations. Streamlining HIPAA audit requirements put into place by the HITECH Act. Audits drain resources from security budgets. Passing an audit, combined with proof of on-going investment into cybersecurity, should result in a less strenuous audit the next time around—a HIPPA-Lite version, as it were—or increased time interval between audits.

Replace Social Security Numbers as a Patient Identifier

Congress should remove language placed annually in federal spending bills that prohibits the Department of Health and Human Services from using any federal funds to promulgate or adopt any such standard. Technology has provided for alternatives to a numeric or alphanumeric identifier as a solution, and the government does not need to be the arbiter of the identification solution.

Use Security as a Factor of Reimbursement

Congress should allow the Centers for Medicare and Medicaid to use security as a factor in reimbursement. Similarly, improving an organization's cybersecurity readiness should be considered a recognized activity under the clinical practice improvement performance category under the Medicare Access and CHIP Reauthorization Act Merit-based Incentive Payment System reimbursement scheme.

Chapter 5: Cybersecurity in the Banking and Finance Sector

Daniel Crisp, chief Information Risk Officer and Head of Technology Compliance, BNY Mellon
Larry Trittschuh, Threat and Vulnerability Leader, Synchrony Financial
Gary McAlum, Chief Security Officer and Senior Vice President, USAA

What Makes the Financial Services Sector Unique

Banks and other financial institutions remain a top target for cyberattacks, whether for financial gain, data theft, or retaliation. Today's consumers have higher expectations about service, given the proliferation of technologies available to them. Consumers are more likely to shop around for products and be more interested in direct and mobile channels. However, while the use of innovations such as mobile devices, the exploitation of these devices has increased significantly.

Commercial banking, too, has seen tremendous benefits from technology, and is poised to reap even more as the new distributed ledger system known as blockchain enters the mainstream. More than half of exchanges surveyed by the International Organization of Securities Commissions and the World Federation of Exchanges in 2013 reported experiencing a cyberattack during the previous 12 months. Neither is the insurance industry is immune to the changes in how business is conducted in today's contemporary and interconnected society. Insurers are prime targets to be victimized given the richness of data—credit card information, medical information, and other underwriting information.

Challenges Facing the New Administration

The current regulatory model for cybersecurity does not work. Cyber technology and attack methods change constantly and the regulatory process is inherently time consuming and cumbersome.

The financial services sector continues to see an increase in disparate and fragmented cybersecurity regulation. For many institutions, it began with the Federal Financial Institutions Examination Council released in June 2015 a Cybersecurity Assessment Tool incorporating concepts from the voluntary NIST Cybersecurity Framework. Member agencies use the tool in regulatory inquiries. As a result, many large financial institutions expend immense amounts of time and resources determining how to demonstrate compliance.

Complicating matters further, financial institutions receive similar cybersecurity inquiries from different regulators, even from different offices of the same regulator. These duplicative reporting requirements ask largely the same questions, but require exhaustive tailoring for each regulator. And the SEC is becoming ever more assertive in monitoring the cybersecurity of broker-dealers and registered investment advisers, even testing firms' implementation of cybersecurity controls

Technology innovations have eliminated borders for criminal enterprises. Attackers can exploit vulnerabilities from anywhere and impact entire networks in a matter of seconds. This poses a tremendous risk of cascading failure across the sector. Phishing is a main pathway for cyber theft, and spear-phishing is even more pernicious. The use of phishing is widespread, unrelenting, and a low-cost, high-payoff technique for attackers.

Mobile banking is a boon for consumers, but opens up a new front for attackers to exploit. Cyber thieves craft malicious apps targeting banking data, but it's not just banking apps that pose a cybersecurity challenge.

Recommendations

Government Should Rethink Its Approach to Cybersecurity

The federal government's credibility in educating, let alone regulating and mandating, cybersecurity practices is severely undermined by its track record of inefficiency. Agencies have yet to adjust to the interconnected nature of cybersecurity, approach it as if it were a static problem addressable through existing formulations. Punitive checklist compliance is a waste of resources. The number of regulatory agency examiners with specialized information technology training is low, and much of government's shared cyber threat data is out-of-date and stripped of context as to be useless.

Harmonize, Streamline and Improve Regulations

Regulatory and legislative mandates and compliance frameworks that address information security for the financial sector, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Fair and Accurate Credit Transactions Act, as well as state compliance regimes, must be consolidated and streamlined.

Regulations should encourage banks to take a risk-based approach, which is customized to the threats they face and takes into account the bank's business model and resources available. Utilizing a standard mechanism such as the NIST Cybersecurity Framework to align the proliferation of different legal and regulatory cybersecurity requirements enables harmonization and adopts unified fundamental guidance for developing cybersecurity policies and practices within the industry.

Operational Improvements

Toss the password into the dustbin of history

"Killing the password" has been a long-standing Obama administration priority, one that it reiterated in the National Cyber Action Plan unveiled in February 2016. The new administration should accelerate the work of the National Strategy for Trusted Identities in Cyberspace, a program charged in 2011 with charged with creating market conditions favorable to a wholesale replacement of passwords. Today, it's clear today the effort has stalled.

Incentivize ISPs to Become More Active In Cybersecurity

ISPs are critical players in improving cybersecurity across the internet, but are not incentivized to implement well-established security protocols that would make launching cyberattacks harder for hackers such as DNS Security Extension and BGPSec. We are not advocating for heavy-handed regulation but a common set of strong security standards that ISPs can be evaluated against in the market place, much like the "5-star safety rating" system developed years ago by the National Highway Traffic Safety Administration.

Adopt anti-phishing technology

The existing internet technology standard known as DMARC (Domain-baes Message Authentication, Reporting and Conformance) should be implemented by the federal government and even further in the private sector.

Encourage Development of More Cybersecurity Experts

The new administration should consider leveraging the federal science, technology, engineering and mathematics program to promote wider interest among students in technology jobs. The current national goal of graduating an additional 1 million students with STEM majors should be reassessed with

an eye toward increasing both that number as well as the number of technology graduates represented within it.

Chapter 6: Cybersecurity in the Power Utility Sector

What Makes the Utilities Sector Unique

Over the past decade, the bulk power system has seen improvements and increased investment in resiliency and cybersecurity. However, local power distribution assets are not only more vulnerable to cyberattack but also more critical to national electricity delivery than previously contemplated.

While products to protect information technology infrastructure are readily available and mature, there are far fewer products in the marketplace that provide security for the highly connected operational technologies that control physical assets on the power grid.

To add complexity, many power utility executives struggle with the uncertainties associated with recovery of security related costs and overhead based on traditional state rate making procedures.

Even if there were adequate funding by utilities to address their normal (i.e. “commercial”) cybersecurity risk, there will inevitably be a gap between vulnerabilities that can be cost-effectively mitigated and the residual risk posed by sophisticated nation-state powers seeking to disrupt the grid. Even utilities, duty-bound by public-good considerations, are still private sector businesses that are unlikely to invest far beyond the thresholds of normal commercial risk.

Exacerbating the situation is how utility asset vendors sell closed-source devices and software solutions, which typically come bundled with significant contractual prohibitions against tampering or reverse-engineering. This results in a difficult situation, preventing utilities from processes which might allow them to verify the integrity of hardware and software they purchase.

Challenges Facing the New Administration

Over the past 15 years, the electric power industry has invested heavily in making the distribution system smarter, more efficient and more connected. Smart grid technologies have been incentivized and implemented with little regard for the increased cyber risk. Equally concerning is that utilities are sourcing advanced technologies and products from multiple vendors with little or no ability to properly assess supply chain risks.

The possibility of terrorist attacks will grow. The level of sophistication required to affect widespread damage to the grid has typically suggested that only nation states will be effective. However, a growing community of post-national actors are being contracted by states as an extension of their offensive capabilities, which is creating an international marketplace for sophisticated disruption capabilities.

Recommendations

Enhance information sharing between utilities and the federal government

Greater federal government transparency in managing data will foster trust and confidence in relationship building and communication. The next president should instruct the existing utility industry sector coordinating council and the corresponding government coordinating council established under the National Infrastructure Protection Plan to engage on these information sharing issues and report back to the administration within three months on their plan to create greater clarity and transparency regarding information sharing within the sector, including any legislative adjustments that may be needed.

Reform the clearance attainment process for private sector executives

Long processing times and an insufficient number of security clearances being made available are significantly hindering the utility industry's ability to support the U.S. cybersecurity mission. The next president should instruct DHS to coordinate among security clearance granting agencies and develop an expedited "TSA pre-check" style system to enable already cleared individuals to maintain their clearances more easily and generally modernize the clearance process to include the use of transferable clearances from department to department.

Ensure DOE remains the primary liaison between utilities and the federal government

While DHS plays a critical role as utilities face cybersecurity challenges, the Department of Energy remains best suited as the main point of contact due to decades of working to provide meaningful, contextual and actionable analysis. The next president and Congress should consider amending the Cybersecurity Act of 2015 to expand the benefits currently granted for sharing information with DHS to other appropriate agencies such as Energy.

Catalyze and accelerate the development of the private cybersecurity insurance market

Cybersecurity insurance is an undervalued tool and critical to the future safeguarding of utilities, but to date the market has focused on data breach fallout. To expand coverage, the administration and Congress should replicate the success of the Terrorism Risk Reduction Act to create a similar reinsurance backstop for cyberattack-caused real-world damage to utilities and their customers.

Promote innovation through government grants

Initiatives such as Rapid Attack Detection, Isolation and Characterization Systems at DARPA and Cybersecurity for Energy Delivery Systems at Energy encourage investment in commercial products by appropriately reducing risk for potential vendors and helping bring together all relevant stakeholders. These programs should be continued and expanded.

Increase cybersecurity focus of state-level regulators and legislatures

The federal government should pass a cybersecurity "states-must-consider" law so that states must demonstrate they have considered appropriate cost effective cybersecurity standards for their electric utility ratemaking proceedings. Doing so will effectively increase the focus on distribution cybersecurity at the state level without imposing new regulations on distribution utilities.

Encourage Public-Private Collaboration to Manage Vendor Risks

Vendors must play their part in the security of the grid. A new balance needs to be struck between the commercial needs of vendors, who would prefer not to reveal the workings of their products, and the needs of electric utilities to both ensure assets are not pre-packaged with malware. Solving this requires a dialogue between utilities, vendors, and the government to evaluate possible solutions that cost-effectively increase confidence in U.S. grid assets and help utilities prepare for cyberattacks. The Obama administration's proposal for a National Center for Cybersecurity Resilience, where companies could test the security of systems under controlled conditions, is a good start in this direction. So is the Federal Energy Regulatory Commission's proposed rulemaking regarding supply chain risk management. The government and utilities themselves could play a valuable role incentivizing vendors to adopt the

Underwriter's Laboratories model—this would insure that all vendor products are rigorously and transparently inspected to ensure they meet baseline cybersecurity standards.

Cybersecurity and the Information Technology Industry

Art Coviello Jr., Executive Chairman (retired), RSA

What Makes the IT Sector Unique

In the digital age, virtually all sectors rely on the IT sector, and no industry has escaped transformation due to IT innovations. The internet changed virtually every aspect of modern life. Approximately 12 percent of global trade is conducted via international e-commerce. Even the political process has changed due to social media interactions.

Computing power doubles every two years, and interconnected devices communicate and deliver instructions and intelligence to machinery, creating the Internet of Things and amassing huge amounts of data. However, this increase in surface creates amble opportunities for security breaches and the misuse of privacy information that will be felt by all sectors, not just IT.

These same innovations also create ample opportunities for advances in cybersecurity technologies. Development of products with artificial intelligence and the use of machine learning gives us the ability to prevent, predict, detect, and respond to attacks as never before.

However, do not mistake improved technical abilities for a true solution to the bad state of computer security. The challenges are imbedded in policy and management. The IT industry has flourished in a generally unregulated environment, which has been essential to its historic growth and productivity. An unhappy byproduct of this growth is a system prone to outside attacks. The sector must find a mechanism to sustainably secure it without killing innovation.

Challenges Facing the Next Administration

Internet of Things: In the IoT, humans are the ultimate thing, and will generate multitudes of personal data. We know better than to create this world without securing it first, yet we continue to do so.

Cyber War and Terrorism: Even absent direct escalation into a shooting war, cyberattacks will cross the plane from bits to atoms and become kinetic in the damage they cause.

Commercial Espionage: Intellectual property theft is an act of economic war and harms drivers of global economic growth.

Proposals for Backdoors: Adoption of proposals to build encryption backdoors into IT products for law enforcement and intelligence communities would benefit adversaries, provoke legitimate privacy concerns among citizens and further deteriorate trust between the U.S. and world community.

Government Cybersecurity: Government systems repeatedly fail at security. Federal information technology infrastructure is obsolete yet government continues to spend resources on legacy systems rather than funding upgrades.

Information Sharing: We cannot seem to navigate the legitimate concerns of privacy groups around information that can be shared and the business community around legal liability. Moreover, liability protections are available only for sharing through DHS and no other preferred entities such as the FBI.

Public-Private Partnership: Trust and cooperation between IT and government is at an all-time low. This will persist so long as government continues to threaten industry.

Data Breach Notification: Forty-seven states plus the District of Columbia maintain separate laws for data breach notification, creating an undue burden on industry and increasing costs for notification of breaches.

Recommendations

Create A Cabinet Like Position to Upgrade Civilian IT and Security Infrastructure

Given the importance of IT in the running of our government, the need to manage and secure critical infrastructure, and the ongoing productivity benefits of continued innovation, appointing a Cabinet-level position to manage an IT transformation should be one of the highest priorities for the next administration. The position needs full authority and funding.

Workforce Development

Government should work with colleges and universities across the country to obtain a steady flow of recruits for cybersecurity positions by providing scholarships to students willing to commit a specified number of years in government cybersecurity positions.

Increase and Improve International Law Enforcement and Cooperation to Prevent Cyberwar and Terrorism

This should start with the president instituting a full review of national law enforcement spending to assure that fighting digital crime is far better resourced. The commander-in-chief should also also initiate a concerted process to modernize international law and procedures with respect to clarifying criminal laws internationally.

Increase Government Research and Development Funding for Risky Technology Research

Rather than routinely cut research and development funding, the United States should emulate what our competitors are doing in other countries by providing increased government support for basic IT research and general-purpose digital programs.

Public-Private Partnership

Collaboration between the public and private sectors to test the effectiveness of the NIST Cybersecurity Framework is needed to define what using the Framework entails. By testing the Framework, cost effective aspects will be discovered. Cooperation would also allow the Enduring Security Framework to be reenergized and expanded to include allies.

Law Enforcement Should Stop Pushing the “Going Dark” Narrative

New enabling capabilities for the IoT, and advancements in computer power and storage capacity for big data applications can be used by law enforcement, defense and intelligence communities in lawful ways. Law enforcement should spend more energy in adjusting their investigative techniques to this new world than fighting the inevitable onset of encryption, which is good for cybersecurity by preventing data theft and cyberespionage.

Chapter 8: Cybersecurity in Telecommunications

Richard Spearman, Group Corporate Security Director, Vodafone

What Makes the Telecommunications Sector Unique

The global telecommunications sector is a mix of government, former government, and commercial operators. The networks are a critical part of the business infrastructure and increasingly seen as part of the critical national infrastructure. They deliver services for customers, but also wider benefits for society.

The telecommunications industry stores, manages and transports a vast amount of valuable data for individuals and society, digital commerce and critical national infrastructure.

The threat from cyber actors is increasing in sophistication, persistence and variety—and the risks posed are not easily mitigated. Cybersecurity needs to be multidimensional, transcending the risk management and response capabilities of any single enterprise, industry or government. The damage inflicted by successful cyberattacks is not just financial and commercial but can also lead to long-term reputational damage and regulatory action.

Customer confidence is crucial. Customers need to know that their data is safe and to understand how companies will use it and the basis on which the government can secure access to it. Customers need to trust service providers to behave responsibly in this regard. Telecommunications is a regulated business. Service providers are required to give government's access to customer traffic and data in accordance with licensing regulations and the laws of the jurisdictions in which they operate. Our policy is clear: telecommunications companies should not hand over customer data unless they are lawfully required to do so.

Challenges Faced By the Next Administration

Maintaining Trust between Business, Government and Society

We need to align the interests of customers with those of business and government. The experience of Apple versus the FBI might suggest that the interests of industry, government and society are divergent. We would argue absolutely not. It is about reaching an agreed compromise, a question of balance not absolute choices. Crucially it is about trust and transparency.

Regulation Lags behind Globalization and the Pace of Change

In a globalized information economy, telecommunications companies will often deliver products and services using centralized platforms and infrastructure located across multiple jurisdictions. Regulations that unduly restrict the cross-border transfer of personal and machine-generated data are likely to impede service delivery and distort investment decisions.

The speed of technology change challenges existing regulation. Services come and go rapidly and the development cycle is shortening. Legislation should clearly outline the purpose and offer clarity about the types of government agency who can require access to customer data, along with the process by which that data can be secured. The process should be auditable and it should be possible, through that audit, to verify that the lawful system is being used.

The Need to Keep Up With Those Who Threaten Our Networks

The scale and changing nature of the challenge is disrupting industry attempts to build internationally compatible safeguards and making it more difficult to have a mature debate with customers about privacy and security.

Recommendations

Incident Reporting and Information Sharing

Following an incident, everyone needs to be clear and precise about what has happened, but government decisions about incident notification and public disclosure of major incidents (or audits) should not be allowed to disrupt or undermine industry attempts to mount an appropriate and proportionate response.

For the industry to make meaningful headway on standards and standardization we need to see more inter-government coordination on standards work to deliver globally accepted outcomes that strike at the heart of the issues

The telecommunications industry also requires a legal and regulatory framework to promote and uphold technology neutrality and provide a legal framework to encourage investment in future-capable networks that will carry exponentially growing data in virtualized cloud-based environments.

Take a Light Hand with Regulation

Government needs to lead and support national and international conversations required to find the appropriate balance between the need to protect the privacy of the individual and the need to ensure the collective security of society. Policy and regulation must be developed with the specific needs of the enterprise sector in mind, rather than as a by-product of regulation designed for consumer needs.

Broaden the Vision of the Public-Private Partnership between Telecommunications and Government

In the digital age private companies are on the frontline of defense when it comes to cyber threats. Many attacks are not launched at telecommunications companies but through them, in some cases against government or national security targets. Third parties may struggle to manage the impact of high-level attacks if their prevailing business models don’t allow for further investment in cybersecurity. In these situations it might be cost effective for government to use telecommunications companies to provide enhanced security in situations where further investment is needed to reduce the impact of high-level threats and provide a broader common level of defense that it beyond the reach of some organizations but ultimately in the national interest.

Chapter 9: Winning the Cyber Talent War: Strategies to Enhance Cybersecurity Workforce Development

Dr. David Brumley, Professor of Electrical and Computer Engineering and Director of Carnegie Mellon's CyLab Security and Privacy Institute

Examining Progress to Date in Efforts to Strengthen the Cybersecurity Workforce

A Partnership for Building the Future Public Sector Workforce—The Scholarship for Service program

Funded by the National Science Foundation and operated in partnership with DHS, the Cyber Corps of the Scholarship for Service program has demonstrated significant impact in encouraging students to pursue cybersecurity careers and creating a pipeline of talent for the public sector

National Centers of Academic Excellence in Cyber Defense

This program sets criteria and mapping curricula to assist institutions in building effective cybersecurity education and research programs—helping to establish a national framework for cybersecurity education. All four-year baccalaureate, graduate education and two-year institutions are eligible.

Presidential Innovation Fellows

The fellows program is designed to engage early career IT professionals and engage them in short stints in government. While not focused exclusively or even predominantly on cybersecurity, the Presidential Innovation Fellows program provides a window on a future where an improved flow of critical cybersecurity talent could be a vital resource for meeting major short term challenges and raising the overall level of skills in the cyber workforce.

National Guard and Military Reserve Cyber Operations

Regional centers being developed by the National Guard and Reserve are creating a nexus of talent within states and cities that draws on professionals engaged in industry and academia who can be mobilized to support government needs in the case of major incidents.

Engaging Veterans in Cybersecurity Careers

A number of promising initiatives have also been launched in the last few years to focus cybersecurity education on veterans. These efforts include specific outreach and degree programs—including those launched by the state of Virginia and boot camp programs launched by companies such as PricewaterhouseCoopers, among others.

Initial Steps to Nurture Cybersecurity Career Paths for Young Americans

As part of the National Initiative for Cybersecurity Education (more often known as NICE), federal agencies collaborate to strengthen K-12 student and teacher engagement. One of the leading examples of this effort is the GenCyber initiative supported by NSF and the NSA. GenCyber supports collaborations with academic institutions to conduct cybersecurity summer camps for students and teachers.

Shaping an Agenda for the Next Administration: Principle Building Blocks of an Effective National Cyber Workforce Strategy

Focus a National Initiative on Building the Talent Pipeline

Attracting students into the federal government must be augmented by an aggressive strategy to build the pipeline of interest in earlier grade levels. This will require a broad range of engagement with K-12 education that includes classroom initiatives, expanded teacher education and after-school competitions to spark interest.

Embrace the Positive Elements of the Hacker Dynamic

Hackers are ultra-curious, highly imaginative professions who are able to spot even the most hidden vulnerabilities in systems. Meeting the nation's cybersecurity talent needs will require nurturing the natural curiosity and imaginative creativity that defines the hacker experience.

Create New Vehicles for Industry, Government, Education Collaboration

While policies to date have focused on the needs of the federal government, the national cybersecurity workforce is a challenge for the private sector as well. Opportunities must be explored to foster closer coordination among government, industry and the higher education community as the nature of the cybersecurity challenge evolves.

Policy Recommendations for New National Federal Cybersecurity Workforce

Intensify Initiatives to Create a Cyber-Aware Generation

Incorporating basic cybersecurity education into curricula at all education levels and work experiences would enhance this first line of defense. Along with this effort, we need to invest in research and applied development of innovations that continue to make security and privacy easier for consumers.

Develop a Core Cybersecurity Curriculum That Can Be Adapted and Applied At All Education Levels and Start Building Cybersecurity into STEM Programs

Recognizing the importance of cybersecurity as a fundamental element of STEM education will also enhance the growth of programs and stronger student interest.

Engage Industry and the Higher Education Community In Commitment to Train 100,000 High School and Middle School Teachers In Basic Cybersecurity Education In the Next Five Years

This component can tap the development of new online and gamification tools that have the potential to significantly impact the ability to bring cost-effective education resources to schools throughout the nation. Carnegie Mellon experienced the success with picoCTF, and nationwide adoption of this model, specifically aimed at educators who can run their own versions of the contest, could have an exponential impact.

Using the FIRST Robotics League as a Model, Advance a National Strategy For Middle School And High School Hacking Contests to Excite the Next Generation of Cybersecurity Professionals

Now in its 25th year, FIRST reaches 75,000 students around the world each year and provides a broader portal to STEM careers. 13 A national hacking contest initiative can have a similar impact.

Expand the Scholarship for Service Program and Foster Even Deeper Cross-Institutional Collaboration

The proposal to increase the number of institutions in the program is a valuable component of a talent initiative. One model for such an effort is the Cyber Stakes program, which has fostered collaborative education and exercises between Carnegie Mellon and service academies.

Explore Creation of a Cybersecurity ROTC Program

A cyber-specific ROTC-like initiative would underscore the sense of national mission that is vital to addressing the environment for strengthening the cybersecurity talent pipeline. A key to this effort would be to create a strong network among institutions operating this program to ensure that the development of these students included both deep technical and operational experiences.

Additionally, consideration should be given to development a "2+2" model for this effort, where a student who has a potential interest in cybersecurity can receive a modest financial aid supplement in their first and second year. At the end of the second year, these students (and any other students in the program) can choose to apply for acceptance into a program fully funding their tuition during the third and fourth year, if they commit to a cybersecurity minor in addition to their computer science or electrical and computer engineering major. In return, the student would be required to sign up for three years of service in a government cybersecurity position.

Create New Mechanisms for Industry, Government, Higher Education Collaboration

One strategic approach to fostering these new mechanisms would be to support the development regional test beds for collaboration on the emerging Internet of Things. These test beds could focus both on innovation in cyber applications and advancing opportunities for formal education programs as well as ongoing training initiatives.

Manufacturing Sector Briefing Memo

What Makes the Manufacturing Sector Unique

Manufacturers are the creators, users, servicers and installers of the Internet of Things. This technology is creating enormous opportunity and driving transformative change. It has made all manufacturers into technology companies.

The days of interacting with the customer only during a single transaction are over. Connected technology enables manufacturers to provide real-time performance monitoring and usage patterns for their customers throughout the entire lifespan of a product. A tire manufacturer won't just sell tires, but a package to reduce costs through sensors that collect data on fuel consumption and tire pressure.

While connected technology drives innovation in the manufacturing sector, it is also creates new challenges. Manufacturers are now the first line of defense in securing our nation's most critical online assets. They place cybersecurity at the highest priority level.

One of the primary targets for cyberattack inside the manufacturing ecosystem are industrial control systems. This is the class of computers that help manage the shop floor. ICS systems are configured in growing numbers to be reachable through the Internet, including systems retrofitted with modern networking capabilities.

Even when companies take measures to secure their Internet-addressable ICS systems, they often link their factory production and enterprise information technology networks. That connection results in benefits such as increased productivity, but a new class of malware is exploiting those links to target ICS, likely for espionage.

Challenges Facing the New Administration

The IoT is going faster than security can keep up

Many IoT devices will possess minimal processing power. That is the nature of the thing—ubiquitous and cheap devices everywhere whose power comes through networking. As a result, many devices may not have capability for basic cybersecurity best practices, such as encryption and operating system updates. Even where capacity exists, manufacturers might not find it economical to patch devices made on a slim margin in a market relentlessly focused on the next generation of products.

Cyber espionage

Only the government tops the manufacturing sector as a victim of cyber espionage. Espionage isn't just a matter of lost revenue. It's a threat to economic security with implications for national security.

Industrial control system security is underrated

Attackers seeking to disrupt industrial processes don't need to exploit an underlying software vulnerability, the way that sophisticated hackers do when attacking enterprise IT systems. They simply need to gain access to the ICS system (perhaps through the corporate IT network) and use the exposed digital controls to manipulate the system into failure. No further hacking required.

The Department of Homeland Security stood up in 2009 the Industrial Control Systems Cyber Emergency Response Team in recognition of this challenge, but the years since have proved disappointing. Its main output is further transmitting alerts already widely available to industry.

Recommendations

Incentives for improving cybersecurity

Small and medium-sized manufacturers in particular face bad economics when it comes to achieving a level of cybersecurity robust enough to stand up to nation-states, manufacturing's main cyber threat. This gap between commercially-sustainable levels of cybersecurity and what's necessary to counteract foreign adversaries isn't just a market-failure. It's the space that federal government was designed to fill by dint of its constitutional charge to provide for the common defense.

What's necessary is a public-private partnership that uses economic tools to encourage investment beyond ordinary levels of commercial cybersecurity spending. Specifically, the government should complete the task begun with creation of the National Institute of Standards and Technology Cybersecurity Framework in determining what the most cost-effective elements of cyber defense are.

Fund IoT security research

No amount of incentives can overcome a key characteristic of the Internet of Things: Ubiquity of cheap computers with minimal computing power. The ability to seed the environment with cheap computers is what makes the IoT possible.

This is an irreducible problem that requires a different approach to cybersecurity, one premised on building secure systems from insecure components. This isn't a new notion, but it's one that's needs urgent revitalization. The National Science Foundation, the Defense Advanced Research Projects Agency and the research arm of the Department of Homeland Security should make funding research into this a priority.

ICS-CERT should be strengthened

The Industrial Controls Systems Cyber Emergency Response Team performance needs to enhance its focus on development of best practices and on research. The organization's outreach to the manufacturing sector also should be improved.

"We tend to count things—how many alerts, how many advisories, how many incidents do you respond to," said ICS-CERT Director Marty Edwards in May 2016. "I think we have to get to the point of measuring what impact did we make inside of a company, or how is a sector improving or degrading over time in the cybersecurity area," he added. The manufacturing sector concurs.

Chapter 10: Cybersecurity in the Manufacturing Sector

Brian Raymond, Director of Innovation Policy, National Association of Manufacturers

What Makes the Manufacturing Sector Unique

Manufacturers are the creators, users, servicers and installers of the Internet of Things. This technology is creating enormous opportunity and driving transformative change. It has made all manufacturers into technology companies.

The days of interacting with the customer only during a single transaction are over. Connected technology enables manufacturers to provide real-time performance monitoring and usage patterns for their customers throughout the entire lifespan of a product. A tire manufacturer won't just sell tires, but a package to reduce costs through sensors that collect data on fuel consumption and tire pressure.

While connected technology drives innovation in the manufacturing sector, it is also creates new challenges. Manufacturers are now the first line of defense in securing our nation's most critical online assets. They place cybersecurity at the highest priority level.

One of the primary targets for cyberattack inside the manufacturing ecosystem are industrial control systems. This is the class of computers that help manage the shop floor. ICS systems are configured in growing numbers to be reachable through the Internet, including systems retrofitted with modern networking capabilities.

Even when companies take measures to secure their Internet-addressable ICS systems, they often link their factory production and enterprise information technology networks. That connection results in benefits such as increased productivity, but a new class of malware is exploiting those links to target ICS, likely for espionage.

Challenges Facing the New Administration

The IoT is going faster than security can keep up

Many IoT devices will possess minimal processing power. That is the nature of the thing—ubiquitous and cheap devices everywhere whose power comes through networking. As a result, many devices may not have capability for basic cybersecurity best practices, such as encryption and operating system updates. Even where capacity exists, manufacturers might not find it economical to patch devices made on a slim margin in a market relentlessly focused on the next generation of products.

Cyber espionage

Only the government tops the manufacturing sector as a victim of cyber espionage. Espionage isn't just a matter of lost revenue. It's a threat to economic security with implications for national security.

Industrial control system security is underrated

Attackers seeking to disrupt industrial processes don't need to exploit an underlying software vulnerability, the way that sophisticated hackers do when attacking enterprise IT systems. They simply need to gain access to the ICS system (perhaps through the corporate IT network) and use the exposed digital controls to manipulate the system into failure. No further hacking required.

The Department of Homeland Security stood up in 2009 the Industrial Control Systems Cyber Emergency Response Team in recognition of this challenge, but the years since have proved disappointing. Its main output is further transmitting alerts already widely available to industry.

Recommendations

Incentives for improving cybersecurity

Small and medium-sized manufacturers in particular face bad economics when it comes to achieving a level of cybersecurity robust enough to stand up to nation-states, manufacturing's main cyber threat. This gap between commercially-sustainable levels of cybersecurity and what's necessary to counteract foreign adversaries isn't just a market-failure. It's the space that federal government was designed to fill by dint of its constitutional charge to provide for the common defense.

What's necessary is a public-private partnership that uses economic tools to encourage investment beyond ordinary levels of commercial cybersecurity spending. Specifically, the government should complete the task begun with creation of the National Institute of Standards and Technology Cybersecurity Framework in determining what the most cost-effective elements of cyber defense are.

Fund IoT security research

No amount of incentives can overcome a key characteristic of the Internet of Things: Ubiquity of cheap computers with minimal computing power. The ability to seed the environment with cheap computers is what makes the IoT possible.

This is an irreducible problem that requires a different approach to cybersecurity, one premised on building secure systems from insecure components. This isn't a new notion, but it's one that's needs urgent revitalization. The National Science Foundation, the Defense Advanced Research Projects Agency and the research arm of the Department of Homeland Security should make funding research into this a priority.

ICS-CERT should be strengthened

The Industrial Controls Systems Cyber Emergency Response Team performance needs to enhance its focus on development of best practices and on research. The organization's outreach to the manufacturing sector also should be improved.

"We tend to count things—how many alerts, how many advisories, how many incidents do you respond to," said ICS-CERT Director Marty Edwards in May 2016. "I think we have to get to the point of measuring what impact did we make inside of a company, or how is a sector improving or degrading over time in the cybersecurity area," he added. The manufacturing sector concurs.

Chapter 11: Cybersecurity in the Food and Agriculture Sector

Dr. Robert Zandoli, Global Chief Information Security Officer, Bunge Limited

What Makes the Agriculture Sector Unique

Whether it's wired-up off-road equipment and machinery, high-tech food and grain processing, radio frequency ID-tagged livestock, or Global Positioning System tracking, the agriculture sector depends on information systems to sustain and improve operations, competiveness, and profitability.

Wringing out even more efficient yields is a global and domestic necessity. Population growth and rising living standards will increase future demands for agricultural products. Breadbasket countries like the United States need to find sustained growth in yields and more efficient ways to farm to meet these demands. Without making use of remote sensing and computer science, significant increases in agricultural yields will be impossible.

Embracing technology comes with risks, and the sector finds itself targeted as never before, thanks to its intellectual property being coveted by foreign competitors and hacktivists. Until recently, most food and agriculture companies did not invest in cybersecurity defense, and were lax in fortifying their infrastructure and developing sound cybersecurity practices. That's beginning to change.

The delay in grasping the threat wasn't limited to the private sector. In 2010, two federal oversight agencies, USDA and FDA, classified cybersecurity as a low priority. However, in 2015, the agencies reversed course.

This past lack of urgency in the agriculture sector was a mistake, as it missed its chance to get ahead of the threats. All sectors of critical infrastructure are interlaced with dependencies, but the biological requirement of food is arguably at the root of them all. An extreme, coordinated cyberattack on agricultural companies would have human and financial consequences.

Challenges Facing the New Administration

Between the seed seller and the supermarket shopper lies a huge, complex and volatile supply chain, one of the most complex worldwide. Its components are vastly different in size and sophistication and compete in an economy that optimizes for the lowest possible cost. This level of diversity and size, combined with small budgets for overhead, isn't the best recipe for robust cybersecurity since it results in huge disparities among individual components. As a result, the agriculture sector will be confronted with the same weakest link problem facing other sectors.

Agricultural production and operations will only increase dependency on software and hardware applications vulnerable to cyberattacks. Smart farm machinery will handle many of the labor-intensive and repetitive jobs still requiring manual work. Smarter, more robust automation will expand into food processing as machines become more apt to deal with irregular size, shape, and quality-control problems.

This new level of connectivity creates vulnerabilities that the sector hasn't fully contended with, especially not in the operational environment. Foreign nations are trying to illegally get ahold of American agricultural technology, particularly data on genetic engineering, improved seeds and fertilizer as well as information related to organic insecticide and irrigation equipment. While most recent cases

of intellectual property espionage were done the old-fashioned way, it's naïve to assume cyberespionage will not become a major element of commercial espionage.

Prospects of agroterrorism also concern the sector. A sophisticated terrorist attack could wreck America's status as a trusted food exporter and undermine domestic confidence in the food supply chain. The sector's growing digitization brings with it new opportunities for terrorists to attack places that previously have been too remote or difficult to strike. Cyberterrorism is a relatively low cost venture with high payoff potential, making the risks of agroterrorism too large to ignore.

Recommendations

Increase Awareness

Neither branch of government gives food and agriculture cybersecurity the attention it demands. While new regulations from the federal government are not necessary, agencies that interact with the sector should recognize cybersecurity for the priority issues it is. The FDA and USDA should start educational programs promoting good cybersecurity practices among sector industries.

There is no congressional subcommittee charged with food and agriculture cybersecurity oversight, or deals with communication technology's new dominant role in sector growth. Committees within the full House and Senate agricultural committees must be assigned this task.

Define what constitutes a nation-state attack against the agriculture sector

Despite widespread attacks by foreign powers, the federal government has yet to define at what point a cyberattack constitutes an act of war or what type of defense it will offer against such attacks. Nor has it updated and adjusted its defense spending in light of this modern threat.

Incentives

Increasing cybersecurity will cost money, and finding the additional funding will not be simple for the sector since it is governed by tight margins and faces a highly competitive world market. Federal involvement in correcting food and agriculture market failures goes back to the New Deal, and this is a new market failure that need correction. Loan forgiveness or grants tied to cybersecurity practices measured against benchmarks such as the NIST Cybersecurity Framework should be implemented, as should new or modified incentive programs for standards, practices and technologies that are not cost effective, but necessary for national security.

Improve Information Sharing

Agricultural cybersecurity information sharing lacks a center. The sector needs a dedicated cyber threat information sharing mechanism, designed for chief information security officers at large corporations, industry associations and agricultural cooperatives. For smaller, individual enterprises, this mechanism should provide the option of automated updates to threat protection software. There are plenty of data exchanges dedicated to various threats, such as food-borne illnesses or crop diseases, but cyber gets lost.

Chapter 12: The Evolving Role of Boards in Cyber Risk Oversight

Ken Daly, CEO, National Association of Corporate Directors
Larry Clinton, president and CEO, Internet Security Alliance

One of the core roles of a board of directors in any organization is to oversee risk. This oversight has always encompassed physical assets, human capital, and the like. Over the last two decades, the nature of enterprise asset value has shifted away from the physical to into the digital sphere. In the private sector, for example, up to 80 percent of total value of the Fortune 500 now consists of intellectual property and other intangibles.

In 2014 the National Association of Corporate Directors, in conjunction with AIG and the Internet Security Alliance, published the NACD Director's Handbook on Cyber risk Oversight. The Handbook was unique in that it shifted focus away from the operational information technology issues that had traditionally dominated cybersecurity discussions, and instead placed cyber risk in the strategic context that directors are most familiar with—including mergers and acquisitions, new product and service launches, strategic partnerships and so on.

In the 2016 edition of *its Global Information Security Survey*, PricewaterhouseCoopers credited the Handbook, by name, with contributing to significant improvements in how corporations were understanding, managing and overseeing cyber risk.

Understanding the Specific Cyber Threats That Are Most Material to the Organization

Members of management and the board of directors must treat cybersecurity as an enterprise-wide risk issue, not a "technology issue" that can be relegated to an IT department.

The implications for boards of directors are twofold. First, directors should ask members of management to translate "cyber risks" into business and strategy risks, and assess them in the context of the company's overall risk appetite. Aspects of those risks will likely be very different among consumer retailers, biotech companies, traditional manufacturers, high-tech startups, utilities, law firms, and banks. Second, boards need to set the expectation with management that success is defined by how quickly the organization can detect—and respond to—cyberattacks and data breaches. When it comes to cyber threats, protection is essential, but total prevention is unrealistic.

Establishing Board Processes That Support High-Quality Dialogue on Cyber Matters

The *Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward* recommended that risk oversight ought to be part of the duties of the full board. The full board should be briefed at least semi-annually, or as situations warrant. The allocation of cyber risk oversight responsibilities should be clearly outlined in the board's governance guidelines and committee charters to avoid either duplication of activities or gaps in oversight.

Maintaining Access to Current Information and Expertise about Cyber Risks

Depending on their industry circumstances and threat profile (among other things), some organizations will choose to include a board member with specific cyber-related experience, and others will not. All boards can and should take steps to bring cutting-edge cyber-expertise into boardroom discussions, by requesting briefings on a regular basis from independent advisors such as external audit firms and

outside counsel, third-party consultants, or law enforcement. This information should be viewed as complementary to—not a replacement for or a signal of mistrust in—reports from management.

Coordination with Government

Individually and together, NACD and ISA have conducted a large number of roundtable dialogues with directors, senior executives, and leaders from government and law enforcement. Several themes have emerged from these discussions.

One-Size-Fits-All Mandates for Board-Level Cyber Oversight Are Not Helpful

Proposals aimed at requiring all boards to have a director who is a "cybersecurity expert"—even setting aside the fact that the severe shortage of senior-level cybersecurity talent, with hundreds of thousands of positions vacant in the United States. alone, making such proposals impossible to implement—would take the important responsibility for board composition and director recruitment out of the hands of the only group with firsthand knowledge about a specific board's current and future skill requirements

Information-sharing between the public and private sectors is highly beneficial

Directors and senior executives alike are interested in gaining a clearer understanding of what government agencies such as the departments of Homeland Security and Justice, the FBI, and the Secret Service do—and what they don't do—for companies in the cyber risk arena, both in general and in the aftermath of a specific breach or attack. Because relationships with government and law enforcement are in management's domain, NACD has encouraged directors to ask the CIO, CISO, CEO and other executives to provide the board with updates about those relationships and corresponding public-private sector communication activities related to cybersecurity. Expanding safe-harbor provisions related to information sharing is also important.

Identify opportunities to coordinate and streamline regulatory requirements

Current cyber-regulations differ and in some cases, contradict one another on multiple dimensions: from state to state, state versus federal, and domestic versus foreign jurisdictions, to name just a few. Industry-specific requirements add another layer of complexity. The associated cost burden is significant, especially for emerging-growth companies. More uniformity would enable management teams and boards to provide better information, more efficiently. Another point of difficulty is that companies and boards are frequently faced with conflicting demands after a cyber-breach. On the one hand, demand for prompt disclosure to satisfy requirements from the Securities and Exchange Commission and regulators for investor and consumer protection, and on the other hand, requests from law enforcement to refrain from going public in order to help an active investigation.

Chapter 13: A New Model for Cybersecurity and Auditing

Center for Audit Quality

The Center for Audit Quality's members are audit and consulting firms that perform financial statement audits of public companies. Because these firms provide a wide range of audit and consulting services across all industry sectors, they have the opportunity to observe cyber readiness in a variety of situations. We also describe our thoughts on a more comprehensive approach to assess and provide assurance over internal controls related to cybersecurity risk management. Work is currently being undertaken by the American Institute of CPAs and the CAQ to operationalize this new approach.

Key Considerations from the Auditor's Vantage Point

Initially, all things “cyber” were relegated to the information technology department in most companies. Today, the trend has shifted and the C-suite and boards of directors are increasingly taking ownership of cyber risk. While there continues to be considerable discussion of what management and board responsibilities are related to cybersecurity and corporate cyber readiness, many organizations are still working to find the most comprehensive structure. There are a few leading frameworks, but numerous standards, methodologies, and processes that have been put forth by federal and state governments, industry specific groups, independent agencies, and other stakeholders. We believe the options available to better manage cyber risks would benefit greatly from enhanced consistency across this myriad of approaches.

Developing a More Comprehensive Approach

We see a need for organizations to conduct ongoing, strategic, enterprise-wide assessments of their cyber risk and the adequacy of their programs and internal controls. Existing financial statement audit process and related internal control assessments do not extend to controls specifically related to cybersecurity procedures and controls unless they impact the financial statements.

We proposed a new, comprehensive approach driven by the internal control structure of the company and that can be delivered with independence and objectivity. The American Institute of CPAs has begun development of a new and comprehensive process to examine internal controls related specifically to cybersecurity risk management. This cybersecurity examination would be separate and apart from the existing financial statement audit process.

The objective of a process would should be to provide the user with three key pieces of information about the entity’s cybersecurity risk management program: (1) a description of the entity’s cybersecurity risk management program; (2) management’s assertion about whether that description is fairly presented and whether the controls are suitably designed and operating effectively, and; (3) the practitioner’s opinion on fair presentation of the description and on the suitability of design and operating effectiveness of the controls.

The examination that the AICPA is contemplating would be entirely voluntary on the part of companies and audit firms. The criteria that are being developed are a customized version of the AICPA Trust Services Criteria that have been enhanced for cybersecurity considerations and closely aligned with the seventeen principles in the Internal Control-Integrated Framework, an internal control framework issued in 2013 by the Committee of Sponsoring Organizations of the Treadway Commission, known as COSO.

The criteria will be mapped to the existing National Institute of Standards and Technology Cybersecurity Framework, and the International Organization for Standardization Information Security Management standard (ISO/IEC 27001). In this way, companies can choose from among multiple cybersecurity internal control frameworks for their cybersecurity risk management programs, and not be required to move to different standards to avail themselves of an independent and objective assessment of their cybersecurity internal control environment. However, reports issued under this new approach would benefit from the consistency, rigor, independence and objectivity of the practitioners.

The Audit Profession: A Strong Foundation to Build On

One of the cornerstones of such a new approach would be the application of the core elements of services from an independent auditor: independence and objectivity.

The audit profession, through performing internal control over financial reporting audits, has further honed existing expertise in evaluating the design and implementation of internal controls. As part of the ICFR audit, auditors look at a flow of transactions and ask, "What could go wrong?" They critically assess whether management has a control in place that is sufficiently designed to timely prevent or detect a potential material misstatement. The auditor then tests those controls to determine whether they operate effectively to address the assessed risk of misstatement.

Auditors also have experience in performing independent, objective assessments of an entity's privacy and security practices through other attest engagements which are already trusted in the capital market. The audit profession brings a multidisciplinary skill set and approach to these engagements, involving subject matter expertise in cybersecurity and information technology. The proposed service would be an extension of this existing knowledge and experience.

Principles for Better Cybersecurity Outcomes

We believe there are several overall principles that must undergird all efforts at improving cybersecurity.

- Avoid blaming the victim. To date, the prevailing attitude when a breach has been discovered and disclosed is to see view the customers and shareholders as the only victims

- The regulatory systems that come into play in breach situations should allow for an appropriate assessment of cyber defenses deployed by management, including the timeliness of remediation and the resiliency of the company.

- Improvements driven by the private sector significantly increase the opportunity to produce meaningful and timely improvements in current practice.

Chapter 14: The Role of Cyber Insurance in Promoting Cyber Security

Tracie Grella, Global Head of Cyber Risk Insurance, AIG

Market Overview

Cyber insurance take-up rates vary based on company size, industry sector, value of data assets and regulatory requirements. Differences are particularly pronounced when contrasting large and small businesses. Coverage limits are relatively modest. A recent survey of risk managers suggests that nearly 60 percent are buy less than $20 million of coverage.

Large losses have also led to supply shortages in certain pockets of the market. For example, several cyber insurers stopped offering insurance to retailers following a string run of large high-profile 2014 consumer data breaches. Additionally, insurers are approaching other high risk sectors with caution, e.g., hospitality and hotels, universities and healthcare companies.

Cyber insurance improves cyber preparedness and resilience. Companies that leverage use these services report significant progress in improving their pre-breach cybersecurity posture and post-breach preparedness and resilience.

Market Challenges

Disparate Company Preparedness and Investment

Company preparedness and investment in security varies greatly. Larger publicly-traded companies generally invest more than mid-sized and smaller companies.

Uncertainty about Future Attack Methods and Outcomes

Attackers continually shift targets and attack modes, rendering past attack data of questionable use. It is essential to have a platform of timely and detailed information sharing on attack modes, trends and information to drive on-going improvements in cybersecurity.

Geopolitical Factors Such As Terrorism and War

Geopolitically motivated attacks from nation-states are well-funded, highly engineered and powerful. The insurance industry needs greater certainty about what constitutes an official act of cyber terrorism and acts of war in cyberspace. Acts of war are generally excluded from insurance coverage.

Lack of suitable data for modeling

Cyber risk is particularly challenging to model for two reasons: a short time series of data and attack heterogeneity.

Challenges of Risk Aggregation and Correlation

Insurance is based on the law of large numbers which suggests that expected losses for a pool of homogeneous, independent risks can be estimated based on average losses in past data. However, this principle breaks down for risks that are highly dependent or connected to one another. This is true in the cybersecurity realm because many companies could be subject to the same loss.

Weak public understanding of cyberattack importance

Cyber insurance is also constrained by a general lack of understanding and awareness of the importance of cybersecurity.

Competing priorities and opportunity cost of insurance purchases

Insurance is generally perceived as a low value product, at least before a loss occurs. Most companies would spend their next dollar to in increasing sales over rather than protecting against a potential cybersecurity loss.

Shortage of qualified talent to address the risk

The cybersecurity skill set is in short supply, and as such, it is difficult to find enough people to do the work.

Rapid growth of the Internet of Things and resultant risks

The IoT is connecting high value assets of significant economic importance to the system that could be targets of attack. For example, power systems are increasingly digital.

Recommendations

Tax Incentives for Cybersecurity Investment

The federal government should consider economic incentives that accelerate company investment in security. This could take the form of tax incentives for such investments or the purchase of cyber insurance.

Government intelligence sharing

Some Information and Security Analysis Centers are more effective than others, and it would be beneficial to enhance all of them to ensure a consistent level of information and engagement across industry sectors. The federal government can incentivize strong participation by using these forums to deliver timely and highly valuable intelligence on emerging cybersecurity threats.

Scenario planning workshops

The insurance industry is prepared to facilitate cross-industry cyber scenario workshops. These would involve federal government agencies, universities, corporations and other participants. The workshops would focus on designing and implementing scenario analysis to better understand the types of attacks that could impact the private and public sector.

Cybersecurity Education

The government's program to certify universities and provide loan forgiveness to students that major in cybersecurity and work for the government is a very good start. We recommend continuing to invest in such programs to ensure that a suitable pool of talent is filled and that companies can draw on this pool. Federal funding for research at non-profits and universities would also dramatically improve the level of knowledge in the field.

Public Service Campaign

We also recommend creating a public campaign similar to the "Say No to Drugs" campaign. This would be highly effective in raising the general level of awareness for cybersecurity and raising the issue to

national attention. Additionally, educational materials should be developed and delivered to mid- and small-businesses through various channels.

Geopolitical Risk Management

DHS, FBI and NSA need to take the lead in protecting the country against such attacks through appropriate offensive and defensive means. Further, intelligence gained from such actions should be shared openly with the private sector to enhance understanding of threats and allow for preparedness.

Clarify the Terrorism Risk Insurance Act

The insurance market needs greater clarity on the applicability of the Terrorism Risk Insurance Act and declarations of war for cyberattacks. Large scale terrorist attacks launched by cyber means should qualify as certified acts of terrorism and trigger TRIA. Additionally, greater clarity on what constitutes an act of cyber war would be helpful.

Legal and Regulatory Immunity

It is essential that legal concerns do not stifle innovation and new technologies that will better protect our society and economy. The federal government should consider including such companies under the auspices of the SAFETY Act given that cyber terrorism and criminal activity is a significant driver of large scale attacks.

Software and Hardware Security Standards

The insurance industry also supports the creation of an independent organization that would be tasked with certifying the security of commonly used software and hardware devices. This initiative would be equivalent to standards developed under the Underwriter Laboratories for the introduction of new electronic devices and components.

Chapter 15: Deploying a Voluntary Cyber-Resilience Program—A Strategic Imperative

Andrea Bonime-Blanc, JD/PhD, CEO, GEC Risk Advisory

A Holistic Approach to Corporate Cyber-Resilience

This chapter makes the case that to be cyber-resilient, businesses of any kind, shape or form should design, develop and implement a voluntary internal cyber-governance, risk and compliance/culture program ("Cyber-GRC Program"). Developing and adopting such a program allows companies to gain better and more sustainable cyber resilience. The cyber-resilient company will have the following three general categories of Cyber-GRC in place: cyber governance, cyber-risk management, and cyber culture.

A Robust Cyber-Resilient Culture Trumps the Law

By building internal resilience into the governance, risk and culture of a company, the need for additional and potentially costly and ineffective laws and regulations will be obviated.

A Paradigm from Another Time: The Defense Industry Initiative and the Rise of the Effective E&C Program

The paradigm is the result of decades of collaboration between companies, professional associations, and research and academic sources, as well as lessons learned from challenging examples, mistakes and scandals. However, cyber risk is different from the average ethics and compliance challenge. Cyber events occur mainly because of the barrage of technological, geopolitical and economic change that have evolved. Companies do not fully control cyber challenges.

The Defense Industry Initiative emerged in the wake of several waves of corruption and fraud involving the defense industry. It calls for five key components of defense contractor self-governance:

1) Creating well-defined risk-based codes of conduct
2) Developing a system that tracks and vets conflicts of interest
3) Developing an employee instructional and communications system
4) A system to monitor compliance and internal controls
5) An independent audit committee

The DII was the principal precursor to a key governmental initiative: Chapter Eight of the United States Sentencing Guidelines. The USSG provides a series of guidelines for prosecutors and judges to help them determine whether a company has an effective E&C Program, which could lead to substantial financial and reputational benefits.

The Emergence of the USSG

Chapter Eight of the sentencing guidelines provided the first cross-industry set of government incentives for corporate wrongdoers to create an internal system of business conduct and compliance. In essence, Chapter Eight mimics many of the tenets of the DII principles.

The Emergence of a Global E&C Paradigm

The most recent salvo of an effective E&C Program was issued in mid-2016 by the Ethics & Compliance Initiative, consisting of a series of principles:

- Principle 1: Ethics and compliance is central to business strategy.

- Principle 2: Ethics and compliance risks are identified, owned, managed and mitigated.
- Principle 3: Leaders at all levels across the organization build and sustain a culture of integrity.
- Principle 4: The organization encourages, protects, and values the reporting of concerns and suspected wrongdoing.
- Principle 5: The organization takes action and holds itself accountable when wrongdoing occurs.

Building and Deploying a Voluntary and Effective Cyber-GRC Program: A Roadmap

There are three basic elements of a strong cyber-resilience or GRC program: governance, risk management and culture.

Governance

This means that the company board, C-suite and top enterprise risk and technology managers are all on the same page about how strategic risk, including cyber risk, is handled at the company. Integrate Cyber-Risk Management into enterprise risk management.

Risk Management

Understand that cyber risk is more often than not a strategic risk: Not every risk is a strategic risk. Many are operational, financial, technological, legal, environmental, etc. Cyber risk can be a strategic risk under two circumstances: instantaneously, when it seriously and deleteriously affects business strategy, or over time, when a situation affecting a company's and its stakeholders' wellbeing has been brewing slowly and eventually surfaces with high impact and strategic consequences.

Understand cyber-reputation risk as it relates to your company: Reputation risk has become one of the top five to ten strategic risks that concern boards and C-suites. Any risk, including cyber risk, qualifies as an underlying risk onto which reputation risk may layer and attach itself.

Know your cyber-stakeholders and their crown jewels: Companies have stakeholders, and each stakeholder has one or more "stakes" in the company. Companies should focus on how to manage their risks in a manner that builds resilience, sustainability and protection of stakeholder interests. Knowledge of stakeholders and their crown jewels goes a long way to understanding what the top cyber risk priorities are.

Culture

Create a robust cyber culture: Integrate cyber risk learning and teachable moments into ethics and compliance or human resources or learning center scheduled and unscheduled training, and take it all the way up to the boardroom on a regular and periodic basis.

Cyber-Resilience Begins at Home

If companies build it, regulators should respect it. The key is to create cyber-resilience through the deployment of an appropriate Cyber-GRC Program that is customized to the needs and profile of a company and that both private and public sectors alike can recognize as such.

Chapter 16: The Digital Equilibrium Project: Balancing Cybersecurity and Privacy

James Kaplan, Partner, McKinsey & Co
Salim Hasham, Partner, McKinsey & Co
Chris Rezek, Senior Expert, McKinsey & Co

Concerned that today's polarized approaches to privacy and security are resulting in the erosion of both, a group of cybersecurity, government and privacy experts banded together as part of the "Digital Equilibrium Project" to foster a new, productive dialogue on balancing security and privacy in the connected world. This memo contains our foundational thoughts on how to advance the discussion past simple binary propositions about security and privacy.

What we propose:

- A new balanced approach, not based on creating detailed polices or legislation, but a framework for creating those instruments. A constitution, not a book of laws.
- A set of structures for continued dialogue and problem-solving, so that continued rapid changes can be understood and incorporated into policy, law and public discourse.
- A framework that builds on successes and finds and leverages analogies to today's world in free trade, diplomacy, law enforcement and social norms, while embracing the unique characteristics of speed, scale and change that mark our new digital age.

Question 1: What privacy management practices should organizations adopt to achieve their goals while protecting their customers?

In an open market, consumers could choose to do business with providers who managed personal information in ways the consumer could accept. However, those market forces can only work when there is transparency, when both sides know what they are trading and open communication can enable the market to settle on its "natural" level.

Starting Hypothesis

While perfect transparency is impossible, organizations could make significant progress by clarifying and simplifying privacy statements. Consumers who understood information collection practices could make informed choices, even automatically if privacy policies are machine-readable, and help establish a more market-based approach to establishing norms. Machine-readable parameters set by consumers, if made practical, could enable a more fluid transaction-based approach to negotiating privacy between these parties.

Question 2: How can organizations continue to improve the protection of their digital infrastructures and adopt privacy management practices that protect their employees?

Employees work for their companies, and companies have a right and obligation to protect their assets and reputations, including gaining information about their employees. As digital infrastructures become more fluid and software-based, organizations will be left with only two constants upon which they can

focus: their users and their users' applications. Those challenges cannot be addressed at a technical level alone. Boards of directors could play a far larger role in developing policies for privacy and security.

Starting Hypothesis

Employees in privacy-oriented nations could recognize that they have more to lose by not empowering their security professionals than they do to gain through inflexible postures on privacy. Enterprises could do a better job of providing transparency so their employees know how their information is being collected and protected in the workplace. Boards of directors could add new members that offer the new skills they need, and can collaborate to create more shared knowledge and perspectives.

Governments could borrow from the nuclear (or other) industry to create and clarify a government role to help corporations protect their critical infrastructure from attack while managing privacy and security interests. We need to find a way to re-work the compliance versus cyber balance so that companies spend more time on value-add cyber security strategy and less on compliance-related work.

Question 3: What practices should governments adopt to maintain civil liberties and expectations of privacy, while ensuring safety and security of its citizens and critical infrastructure?

In terms of our collective physical safety, this question is the most pressing to make progress on, but perhaps the most difficult. As individuals, corporations, nations, criminals and terrorists all increasingly roam the Internet together, enabling governments to protect their citizens without compromising the privacy and trust of those citizens is increasingly difficult.

Starting Hypothesis

Government could play a bigger role in helping define the "how," not just the "why" of protecting critical infrastructure, building on the NIST Cybersecurity Framework. Government could provide proper incentives for corporations to invest in cybersecurity for critical infrastructure. Governments could develop and enforce safety standards for software used in critical infrastructures. Governance and transparency could be strengthened for intelligence agencies, so that citizens can have confidence those agencies are working within the existing laws and guidelines. Government could communicate more clearly both the intentions and realities of intelligence gathering efforts.

Legal limits to domestic military involvement can be re-thought: Digital tools can now create kinetic actions to cause real physical harm to our infrastructure. Governments need to find an approach for attribution and retribution to find and punish culprits of cybercrime, even across national borders. At the same time, private companies may need to be allowed to "hack back" and retrieve their stolen information before it's gone for good.

Question 4: What norms should countries adopt to protect their sovereignty while enabling global commerce and collaboration against criminal and terrorist threats?

Spying on communications has never been easier for governments with the proper skills, and as more information of every form has become digital, more governments have gotten into the business of spying on behalf of their local corporations, in the form of intellectual property theft and communications intercepts.

Starting Hypothesis

Just as nations finally concluded that the long-term benefits of free trade outweighed the short-term benefits of capturing or sinking each other's ships on the high seas, nations will eventually come together to create digital rules of engagement. We need to limit cyber-espionage, the targeting of individual corporations or organizations for economic or political motives. We need to create "arms control" mechanisms to limit the spread of increasingly sophisticated malware tools. Unlike traditional weapons, cyber weapons spread rapidly, are quickly reproduced and modified, and are cheap. We need to address the issues of non-state actors who often have multiple roles, working for their own goals as well as providing services to governments. We need to ensure that digital tools can be created free from nation-state interference either overt or covert so that these tools can be trusted by users globally.

Chapter 17: Best Practices for Cybersecurity Public-Private Partnerships

Larry Clinton, President and CEO, Internet Security Alliance

Introduction

President Barack Obama has said:

> The federal government cannot succeed in securing cyberspace if it works in isolation. The public and private sectors interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government depend. …Only through such partnerships will the United States be able to enhance cybersecurity and reap the full benefits of the digital revolution.

However, despite years of attempting to conduct cybersecurity programs in partnership, it's become apparent that not only were most partnership programs unsatisfying to both parties, but even the definition of partnership is unclear. This confusion and frustration was seen as endangering the partnership model or redefining it in such a way as to rob it of its novel approach to security.

This chapter identifies a set of best practices for operating cybersecurity public private partnerships based on a collaborative research project conducted jointly by the IT Sector Coordinating Council and DHS staff.

Method

The government and industry investigators used a modified critical incident methodology to examine a range of joint programs ostensibly run under the partnership model as identified in the National Infrastructure Protection Plan.

Acting separately, the government and industry groups independently evaluated the various projects on a success scale. Both government and industry evaluators determined that same projects to be successful and less successful.

The groups then undependably identified a set of practices that in their expert opinion as practitioners in the field made the programs successful or not. Consensus was reached as to what practices accounted for the success of the projects.

The case studies that were used for this analysis included:

- The 2006 development of the National Infrastructure Protection Plan;
- the IT Sector Baseline Risk Assessment;
- the construction of the "Cyber Space Policy Review;"
- industry Integration into the National Infrastructure Coordination Center;
- the Information Technology Supply Chain Risk Management Collaboration; and,
- the development of the "Blueprint for a Secure Cyber Future."

Results

Both industry and government evaluators agreed on a dozen best practices that tended to generate successful partnership programs in cybersecurity. These are:

- Senior level commitment to the partnership process communicated to staff and upper echelons.

- Involvement at the priority, goal and objective phases of projects, not just implementation.
- Use of the process identified in the NIPP for involving industry.
- Reaching out to stakeholders early on, ideally at the “blank page” stage.
- Continuous and regular interaction between government and industry stakeholders.
- Providing adequate time for stakeholder review (equivalent to government review).
- Establishing co-leadership of programs
- Consensus partnership decision making.
- Communicating genuine interest in stakeholder input e.g. via co-drafting.
- Adequate engagement from federal agencies beyond DHS.
- Government follow through on partnership related decisions.
- Adequate and competent support services.

Examples of Use of these best Practices

Chapter 17 concludes with two examples of partnership programs, the development of the NIST cybersecurity Framework and the CISRIC Group 4 program conducted by the FCC and the Telecommunications Sector Coordinating Council.

Both programs follow most if not all of the best practices identified in the previous study and were publically judged to be successful by both industry and government.