Government Business Council

Booz | Allen | Hamilton
100 YEARS

WHY PUBLIC-PRIVATE PARTNERSHIPS ARE ESSENTIAL FOR CRITICAL INFRASTRUCTURE CYBERSECURITY

AS CYBER THREATS CONTINUE TO GROW IN NUMBER AND SOPHISTICATION, U.S. CRITICAL INFRASTRUCTURE REMAINS EXTREMELY VULNERABLE

"On a scale of one to ten, with ten being strongly defended, our critical infrastructure's preparedness… is about a three," General Keith Alexander, former head of U.S. Cyber Command and the National Security Agency, recently told the Senate.[1] What makes this cybersecurity challenge particularly difficult is that government owns such a small portion of U.S. critical infrastructure; 85 percent of critical infrastructure is owned or operated by the private sector.[2] Any comprehensive cybersecurity strategy therefore requires extensive coordination and collaboration with private companies.

Recognizing this challenge, the federal government has begun taking important steps. Driven in part by the lack of comprehensive cybersecurity legislation in 2012, President Obama administered Executive Order 13636 and Presidential Policy Directive 21 in February 2013. Twelve months later, the federal government has made progress working with the private sector to develop cybersecurity risk mitigation standards, but information sharing has not yet reached desired levels. By increasing the amount of data available for analysis, partnerships with the private sector would open the door to using big data to detect and prevent cyber attacks directed at our nation's electrical grids, ports, hospitals, nuclear reactors, and more.

Pictured: Bonneville Power Administration's Celilo Converter Station

Vulnerability of Critical Infrastructure

The Department of Homeland Security defines critical infrastructure as the "assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[3]

Because the cyber threat to these systems and assets continues to grow, their security in cyberspace represents one of the most serious national security challenges. In April 2013, two engineers working on their own illustrated the extent of U.S. critical infrastructure vulnerability in cyberspace. Over the course of a single week, they tested open-source software programs integral to the function of 16 utility vendors' SCADA (supervisory control and data acquisition) systems and broke them all.[4] Since then, DHS has posted at least nine advisories addressing the found vulnerabilities.

Quantitative reports also bear out this vulnerability. NSS Labs, a leading information security research firm, estimates that industrial control systems saw a more than 600% increase in vulnerabilities from 2010 to 2012.[5] In 2013, ICS-CERT, the U.S. government's cyber emergency response team for industrial control systems, recorded "an increasing number of incidents targeting our nation's critical infrastructure." It responded to 256 reported incidents, the majority of which "were initially detected in business networks of critical infrastructure organizations that operate industrial control systems."[6] Furthermore, in February 2013, DHS revealed that hackers stole information from 23 gas pipeline companies between December 2011 and June 2012 that could be used for sabotage.[7]

Pictured: The Hoover Dam.

Building Public-Private Partnerships

Recognizing the centrality of the private sector in protecting critical infrastructure in cyberspace, the Obama Administration has adopted a collaborative strategy. Both E.O. 13636 and Presidential Policy Directive 21 underscore the imperative to work with private sector owners and operators of critical infrastructure. E.O. 13636 specifically calls on the U.S. government to "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities" and to develop a voluntary framework that sets industry standards and best practices to aid in managing cyber risks.[8]

In February 2014, one year after the E.O. was issued, the National Institute of Standards and Technology (NIST) published the first edition of that framework. As intended, Version 1.0 of NIST's "Framework for Improving Critical Infrastructure Cybersecurity" marks significant progress standardizing cybersecurity best practices for owners and operators of critical infrastructure. What makes this framework particularly promising is that it was designed to evolve and developed in true partnership with private companies. Speaking at a Brookings Institution event shortly after its release, Dean Garfield, the President and CEO of the Information Technology Industry Council, offered three reasons for why he believes the framework can go the distance. First, it is flexible and based on risk management rather than prescription; second, its standards are digestible because they were developed through consensus-based, multi-stakeholder processes that involved relevant companies; and third, the framework is iterative, but still provides a pathway forward.[9]

Despite the progress made, determining the right level of information sharing with private sector partners remains a significant hurdle. Part of the problem is the lack of congressional action. Cameron Kerry, former General Counsel and Acting Secretary of the Department of Commerce, has said that legislation could facilitate the sharing of information about threats among companies and between government and industry.[10]

In an interview with GBC, Thad Allen, former Commandant of the U.S. Coast Guard and Executive Vice president at Booz Allen Hamilton, identified a more fundamental challenge. "We are still in a period of sorting out definitions of what is an inherently governmental role and what is the responsibility of the private sector."

Private sector concerns do not always align with government concerns. Whereas government is singularly focused on the security of infrastructure

"SHARING CYBER THREAT INFORMATION IN A TIMELY, SPECIFIC, AND ACTIONABLE WAY REMAINS A MAJOR OBSTACLE TO THE EFFECTIVE PARTNERSHIP BETWEEN GOVERNMENT AND INDUSTRY"

systems, the companies that operate them are "driven by market forces and are concerned about the value of their brand, their responsibility to their shareholders, and regulatory compliance." Moreover, the way government works with any given commercial partner differs depending on the sector in which they work. "The relationship between the Department of the Treasury and financial institutions is much different from the relationship between the Department of Energy and oil and natural gas companies," Allen explained.

Further complicating the information sharing relationship is the fact that many private owners and operators of critical infrastructure are not cleared to receive classified information.

For all of these reasons, sharing cyber threat information in a timely, specific, and actionable way remains a major obstacle to the effective partnership between government and industry. Building this partnership may therefore require an intermediary, such as a commercially sourced third-party. This information broker could facilitate the exchange of information along mutually agreed-upon parameters. Reallocating control could be the key to jump-starting an information exchange.

The Role of Big Data

Cybersecurity, at its core, entails an active analysis of data streams. For Allen, "the challenge of cybersecurity is the challenge of increasing the speed of analysis of data in motion, and being able to react to what the analysis reveals." As government and private companies make progress delineating their respective roles, protecting critical infrastructure in cyberspace, and increasing information sharing, agencies will be able to leverage big data to enhance critical infrastructure cybersecurity. With access to greater volumes of data regarding cyber breaches, agencies can use big data analytics to identify threat profiles and build predictive models. Specifically, they will be able to model the progressions of cyberattacks in order to better understand breaches and reduce networks' "attack surface" vulnerabilities. Government will not be the first do so; the private sector is already investing in big data as a cybersecurity solution. By 2016, one quarter of large global companies is expected to have used big data analytics to increase security or detect fraud.[11]

Presidential Policy Directive 21 asserts "a secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of government and critical infrastructure owners and operators." As this public-private partnership develops, the resulting increase in information sharing regarding cyber incidents will permit the use of big data analytics to further improve threat prevention.

About GBC

Government Business Council (GBC), the research arm of Government Executive Media Group, is dedicated to advancing the business of government through analysis and insight. GBC partners with industry to share best practices with top government decision-makers, understanding the deep value inherent in industry's experience engaging and supporting federal agencies. For more information, please visit: www.govexec.com/gbc.

About Booz Allen Hamilton

Booz Allen Hamilton has been at the forefront of strategy and consulting for 100 years. Booz Allen is committed to delivering results that endure. To learn more, visit www.boozallen.com (NYSE:BAH)

Sources

1. Statement by General Keith Alexander to the U. S. Senate Committee on Appropriations, "Hearing on Cybersecurity," June 12, 2013
2. "Critical Infrastructure Sector Partnerships," Department of Homeland Security webpage, <http://www.dhs.gov/critical-infrastructure-sector-partnerships>
3. "What Is Critical Infrastructure?" Department of Homeland Security webpage, <http://www.dhs.gov/what-critical-infrastructure>
4. Perlroth, Nicole, "Electrical Grid is Called Vulnerable to Power Shutdown," *Bits* blog, *The New York Times*, October 18, 2013.
5. Frei, Stefan, Ph.D, "Vulnerability Threat Trends," NSS Labs, February 2013.
6. ICS-CERT Monitor, Department of Homeland Security, October - December 2013.
7. Clayton, Mark, "Exclusive: Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage," *The Christian Science Monitor*, February 27, 2013
8. Executive Order 13636 - Improving Critical Infrastructure Cybersecurity, The White House, February 12, 2013.
9. "Improving Critical Infrastructure Cybersecurity: The Cybersecurity Framework and Beyond," The Brookings Institution, Washington, D.C., February 19, 2014.
10. "Improving Critical Infrastructure Cybersecurity: The Cybersecurity Framework and Beyond," The Brookings Institution, Washington, D.C., February 19, 2014.
11. "By 2015, 25 Percent of Large Global Companies Will Have Adopted Big Data Analytics for At Least One Security or Fraud Detection Use Case," Gartner, February 6, 2014.

First Image: Flickr user – ENERGY.GOV
Second Image: Flick user – dherrera_96