Is America Building a Cyber Security Sand Castle?

William Crowell, former Deputy Director of the National Security Agency, helps explain how private sector efforts coupled with public sector policies can mitigate cyber threats

By Marleah Blades

Security has had more than 20 years to adjust to life in the Information Age. That's the equivalent of two or three lifetimes in high-tech years. But it seems every time we feel closest to truly securing our networks, data and information, cybersecurity once again slithers out of our reach. Why is that?

In part, it's because quickly evolving technology turns threats and mitigation techniques into living, breathing things. It's also because cybersecurity is not just about each of us; it's about all of us. Individual users, businesses and agencies across the globe have excelled at protecting their cyber assets. But individual efforts, while critical, are not enough. Information technology connects us all — sometimes more closely than we would prefer. We all share the risks and the responsibility.

This is one of the messages coming out of this spring's frenzy of media coverage, executive branch shake-ups and legislative action regarding cybersecurity in the United States.

Cross-Sector Failures

Much of the recent attention to cybersecurity has revolved around an April 8 *Wall Street Journal* report that claimed foreign "cyber-spies" had penetrated the U.S. power grid and left behind malicious software. Since these claims surfaced, lawmakers, editorialists and industry experts have repeatedly evoked the alleged infiltration to illustrate both the need to improve national cybersecurity and the potential consequences of inaction.

Here is a prime example of the interconnectedness of our cyber existence: If our power grid were to be compromised and manipulated for malicious purposes, it would pose significant problems for the electric industry in the form of damage, fines, loss of revenue and more. It would pose problems for other privately owned businesses, which could lose significant revenue during prolonged or targeted power outages, and which could stand at greater risk of theft and looting in such circumstances. And it would pose problems for the public sector, which would have to expend extra resources to confront a potential

increase in crime and unrest that extended outages might bring, and which could lose some of its capability to effectively deploy defenses in the event of simultaneous terrorist attack, for instance.

When the *Wall Street Journal* story broke, it should have already been clear that critical infrastructure was not the only sector with a problem. In recent months, we have seen reports of network intruders accessing data from the Pentagon's Joint Strike Fighter project, the FAA's employee information records and the U.S. Air Force's air-traffic-control system. The Cybersecurity Commission of the Center for Strategic and International Studies stated in its Dec. 2008 report, "Securing Cyberspace for the 44th Presidency," that "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration." In its year-long examination of the state of national cybersecurity, the commission found that the Departments of State, Defense, Commerce, Homeland Security and NASA all experienced major intrusions by foreign entities in 2007 alone, and one department official reported that terabytes of information had been lost. It does not take much imagination to see how breaches of sensitive government and military information could negatively impact businesses and organizations across the private sector.

The Cybersecurity Commission of the Center for Strategic and International Studies stated that "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."

While private business outside of critical infrastructure seems to be largely off the hook this year with few high-profile data breaches in the news, their place in the chain of cybersecurity is particularly important. A data breach can have a major impact on their own bottom line — consider that Heartland Payment Systems has reported that the security breach it disclosed in January had cost the company about $12.6 million by May, and that price tag is likely to increase. But businesses' well-being also strongly impacts the state of the nation. Coordinated, malicious attacks on private businesses could degrade an already struggling economy, and economic instability is historically associated with political turmoil, unrest and increased crime.

Loss of trade secrets to foreign entities — as well as loss of information on sensitive projects by private government contractors — could bolster the economic and military strength of other countries at the same time. "A recent report to Congress from the National Counterintelligence Executive highlighted that over 108 countries, both friend and foe, are actively stealing intellectual property from U.S. busi-

nesses to help bolster the competitive posture of their own economies," says Lynn Mattice, former CSO of Boston Scientific and Chairman of the Board of Advisors of the Security Executive Council.

The public sector and the private sector — both critical infrastructure and other business — are inextricably linked; a cybersecurity failure on the part of one could mean a new threat for all.

Why All the Attention Now?

Of course, the federal government, critical infrastructure and other private companies have all been working for years to shore up cybersecurity gaps, some more wholeheartedly than others. Why suddenly is the spotlight shining so brightly on this issue?

One reason is the election of a new U.S. President who has promised to give it a hard look. "You have an administration coming in that's increased the focus on leveraging social collaboration technologies, and the focus on furthering the agenda of the nation and leveraging technology," says Theresa Payton, former White House CIO under President George W. Bush and a Security Executive Council Emeritus Faculty Content Expert. "With that change in administration, the media has really started to look at and have an enhanced understanding of what's going on with cyber globally and in the United States. So in a sense, it's all about timing."

Another reason is the documented increase in the sophistication and number of cyberattacks. Experts agree that the types of threats we are facing now are dramatically different than they were even 12 months ago. "The nature of the threat has changed from casual attacks to very well-financed, substantial, well-delivered attacks. These advanced threats require equally advanced countermeasures for everybody now." says Tom Patterson, a business advisor on security, commerce, and governance and author of the book "Mapping Security — Corporate Security Sourcebook for Today's Global Economy."

Hord Tipton, former CIO of the U.S. Department of the Interior and current executive director of (ISC)², explains, "We have always played this game with the hacking and attacking community, trying to catch up and get on an even par with them. But the evidence and data collected seems to indicate we're falling behind. Annual reports show as much as a 40-percent increase in exploits in '09 than '08, and we have seen a trillion dollars of fraud and identity loss in '08."

These increases can be chalked up in part to the slump in the world economy, according to Payton. "In desperate times, you see a run-up on traditional crimes, and now that cybercrime is becoming more mainstream, it's following the same pattern. I think this does put us more at risk; obviously the more somebody tries to get into your fortress, the more potential they have to find the weak link in the chain, so to speak. But at the same time, from a leadership perspective, the media attention on this topic is creating the positive impact of a heightened awareness of the threats."

"We have always played this game with the hacking and attacking community, trying to catch up and get on an even par with them," Hord Tipton says. "But the evidence and data collected seems to indicate we're falling behind."

Initiatives Already on the Table

The federal government has a number of executive and legislative initiatives on the table aimed at changing how cybersecurity is handled both in the public and the private sector.

The Comprehensive National Cyber Security Initiative (CNCI) was introduced in early 2008. Its overarching purpose is to better protect the nation's cyber infrastructure, starting with federal computer systems and networks. The initiative intends to reduce external points of access to federal networks, improve situational awareness across agencies, shift the focus from passive to aggressive intrusion detection and prevention, and enhance existing information-sharing efforts between the government and the private sector. The details of how all this will be accomplished remain highly classified.

The Cybersecurity Act of 2009 (S.773), introduced April 1 by Senators John Rockefeller (D-WV), Evan Bayh (D-IN), Bill Nelson (D-FL) and Olympia Snowe (R-ME), calls for the National Institute of Standards and Technology (NIST) to create new, enforceable standards of cybersecurity for the federal government and critical infrastructure. It proposes a national licensing and certification program for cybersecurity professionals, and would make it unlawful for any individual to provide cybersecurity services to government or critical infrastructure without a valid license and certification under the new program. The Act would give the President the authority to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network." It would designate the Department of Commerce as a clearinghouse of public and private-sector cybersecurity threat and vulnerability information, and it calls for the President to appoint an executive-level Cybersecurity Advisory Panel with both public- and private-sector members.

President Obama's long-awaited "60-day" review of cybersecurity policy, the report on which was finally released May 29, also recommended the appointment of a presidential advisor on cybersecurity. The report outlines the severity of the need for better cybersecurity and presents a 10-point near-term action plan that also recommends the preparation of an updated national cybersecurity strategy; establishment of performance metrics; the clarification of roles, responsibilities and authority for cybersecurity-related activities across the federal government; the initiation of a national public awareness and education campaign to promote cybersecurity; development of U.S. government positions for an international cybersecurity policy framework; preparation of a cybersecurity incident response plan; development of R&D strategies that focus on game-changing technologies; and the building of a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties. Upon the release of the report, Obama stated his intention to appoint a Cybersecurity Coordinator with a seat on both the National Security Staff and the National Economic Council, although the individual to fill this role had not yet been chosen as of this writing.

Other bills pertaining to cybersecurity include the Critical Electric Infrastructure Protection Act and a set of bills put forth by Sen. Thomas Carper (D-DE) that intend to unify policies, procedures and guidelines for securing federal information systems

by establishing new standards, creating a National Office for Cyberspace and reforming the federal government's IT procurement processes. And between the writing of this article and its publication, this list of proposals will probably be still longer.

Two elements shared by nearly all of the initiatives now up for consideration are: 1) a call for cybersecurity to take its place as a publicly recognized top priority for government; and 2) a call for greater information sharing and public-private partnership.

Sharing is Key to Success

Louis Magnotti, CIO for the U.S. House of Representatives, is one of many who believe cybersecurity is not complete without coordinated protection across sectors. "An IP address does not care if you're a government agency or a private-industry corporation," he says. "Computers do not recognize those boundaries, so our mitigation strategies need to transcend those boundaries as well. All of the players in the public and the private sectors need to put a protection model into place that can do that."

Without effective information sharing between the public and the private sectors, neither side has all the data it needs to provide the best possible protection, says William Crowell, former Deputy Director of the National Security Agency, current Chairman of the Senior Advisory Board to The Director of National Intelligence, and a member of the Security Executive Council's Board of Advisors. "I think the private sector in general is way ahead of the public sector in understanding how to approach the threats and how to build systems that deal with them. The public-sector intelligence organizations are much more aware of the sophistication of the threats. The public sector is still focused on building its own technology instead of looking at what the private sector could bring to the party if it knew more about the threats. There are thousands of new approaches to security being developed all the time, but I think for the most part the government only knows about a few that are sometimes several years old."

Why Today's Options Do Not Work

There already exist several information-sharing forums that are intended to break down the communication barrier between public and private. This is one of the goals of US-CERT, which aims to facilitate collaboration with state and local government, industry and international partners. There are also other CERTs and multiple ISACs (Information Sharing and Analysis Centers) for individual industries that effectively share industry-specific information, and the National Infrastructure Protection Plan has created an information-sharing environment (ISE) for 18 critical infrastructure and key resources (CIKR) sectors.

But the common call for partnership and sharing makes clear that these forums are not working as well or as broadly as legislators would like. Both public and private entities face major obstacles to sharing.

Public-sector officials cannot share sensitive information because of its sensitivity. "When so much information is treated as classified, we just can't get the collaboration we need," Tipton says. "(Federal officials) may tell you, but only on a need-to-know basis. That means there's not much sharing of technology or ideas and

there's no integration between what goes on in government and private sector."

Many private-sector organizations face legal obstacles to information sharing. "The Sherman Antitrust Act limits how much organizations who compete with each other can share," Crowell says. "That one has been an issue in several of the private sectors, particularly financial. There have also been restraints imposed by the Freedom of Information Act, which says if a private organization gives information to the government, the government gets to decide whether the information gets released to the public. That poses some really difficult problems for much of private industry, because company confidential information and brand-damaging information could be released."

"If you're in business, tech is your business," Theresa Payton says. "Because if you use a PC or keep any electronic records, you need to understand your threats and vulnerabilities."

In addition, many small and medium-sized businesses do not even understand why they should be part of the conversation at all. "Many small and medium businesses I have spoken to do not think they're really at risk," Payton says. "I have to explain that they could be used as part of a botnet, and that if they store credit card information from customers or social security numbers of employees, that's valuable data to attackers."

Symantec released the results of its 2009 Storage and Security in SMBs survey in April, which found that globally, a high number of small and medium businesses have not even taken basic precautions, such as implementing anti-virus software and backing up their data.

"Small and large companies need to recognize that cyber attacks are a constant threat and are many times conducted by foreign government intelligence agencies," says Lynn Mattice. "Unless companies deploy sophisticated detection software, they do not realize they have lost trade secrets as a result of these attacks because they still have their information; it has simply been copied and sent back to be utilized by foreign competitors."

"Another challenge for small businesses is that they can't afford a CIO," says Payton. "They think since they're not in the tech business, it does not need to be a big concern. And I tell them, if you're in business, tech is your business. Because if you use a PC or keep any electronic records, you need to understand your threats and vulnerabilities. If you can't afford your own IT person, you should hire somebody to come in periodically and do a threat and vulnerability assessment. They can create a mitigation plan and train your staff on how to protect your company's information and what needs to be done to protect your infrastructure."

An Uncertain Future

As of this writing, it is unclear what will ultimately be done to improve public-private information sharing. The details of all the proposed plans have yet to be hashed out. Many harbor high hopes that a new advisory panel or cybersecurity czar will provide the focus needed to open up the lines of communication.

Whatever happens, says Payton, we must work to ensure that information is not only shared, but usable. "When we build this bridge of collaboration, we have to figure out how we're going to filter all this shared data into actionable information for the public and private sector," she says. "I believe there should be several avenues of communication and several forums that the private sector can use to network and collaborate with the public sector. There may be some groups or councils that need to be vertically focused for specific industries. In addition, emergency alerts regarding cyber threats need multiple levels of notification based on the level of alert. We need to facilitate bi-directional sharing between the government and private industry of core best practices and emerging threats. A combination of Web conferences, in-person meetings and white papers are different approaches to get that information shared in a way that is meaningful and actionable. It's really about sitting down, negotiating what works by industry verticals and thinking through an appropriate communication plan."

Start By Doing Your Part

In the meantime, there are some steps private businesses can take to enhance their own cybersecurity and information-sharing efforts. "There are plenty of organizations out there that foster networking among CISOs," Magnotti says. "The Security Executive Council, (ISC)², ISSA — those types of organizations allow CISOs to not only get to know each other but to share their mitigation strategies."

There are also private service companies that provide threat intelligence to their clients, most of whom are very large financial and retail organizations. Crowell, who is associated with one such organization, iSight Partners, says that these companies tend to remove all identifying information from the threat information they discover and then share that information with their entire customer base, creating a sort of paid information-sharing network.

Organizations that are not already sharing threat information through CERT and applicable ISACs should consider doing so and should weigh the potential benefits against the perceived risks.

Businesses large and small should be ready, Payton says. "You want to have a plan that encompasses three critical areas — protect, defend and recover. You want to make sure you have excellent defenses; however, you should also accept that, more than likely, somebody's going to get in, so you need to have an offensive strategy and a recovery strategy as well."

And more than anything else, we must not allow the increased media attention on cybersecurity to spur a backlash attitude that says the problem is not really as big as it seems. "This threat is very real," Crowell says. "Right now a lot of the attacks are what I would call reconnaissance. They could easily do significant damage, and at a critical moment, that damage would have serious effects on our national security and economic situation." ▮

Marleah Blades is senior editor for the Security Executive Council (SEC). The SEC is a risk mitigation research and services organization for senior security and risk executives from corporations and government agencies. In partnership with its research arm, the Security Leadership Research Institute, the Council is dedicated to developing tools that help lower the cost of security programs. For more info, visit www.securityexecutivecouncil.com/?sourceCode=std.