Print This Article

<< Return to Top gun: Cybersecurity policy

Top gun: Cybersecurity policy

Illena Armstrong
June 01 2010

Priorities for national cybersecurity are where they need to be, says Howard Schmidt, White House cybersecurity coordinator. Illena Armstrong reports.

This May marked the anniversary of what some information security professionals refer to as an historic, exciting and long-overdue presidential speech. Last spring, President Obama showcased a national, five-part Cyberspace Policy Review for the country based on a fresh, 60-day evaluation. During this presentation before public and private executives, Obama discussed the results of the recent assessment kicked off in February and, perhaps most importantly, announced the beginnings of creating a more secure and reliable digital infrastructure, part of which included the establishment of a cybersecurity coordinator.

For months, there had been plenty of conjecture and debate about the creation of such a role. Consequently, the formal announcement to install someone to develop an action plan involving the public and private sectors that would tackle both cybersecurity and civil liberty protection allayed some information security leaders' fears that another presidential administration may give the issues short shrift.

Fast-forward to the end of the year. As months streamed by after the momentous speech, security pros hotly deliberated who would fill the new coordinator position, how much power the leader would have and why it was taking so long for the president to make a choice. Indeed, at the time some experts – a bit unimpressed with the delayed results of the much-ballyhooed 60-day review – began to wonder if any genuine action would follow the speech at all. Then, finally, last December, Howard Schmidt, a well-known and long-time player in the information security marketplace, was appointed.

Most in the industry applauded the move. But, some of this enthusiasm was tempered with various words of caution: Navigating the bureaucratic mire would be tough, progress would be slowed by rumored power struggles among federal agencies, higher priorities in the White House would sideline cybersecurity concerns, authority needed for the post is wanting, and much more. Now that Schmidt begins this job in earnest, the mix of optimism and pessimism for the future still persists. Though some believe things can only get better given false starts by the government on cybersecurity initiatives in the past, others wonder if the ensuing months will see more of the same lurches and stumbles.

"The most difficult job CSO/CISO-types have is to implement security within

the culture of whatever organization they happen to find themselves," says Ron Baklarz (*left*), CISO of Amtrak. "Having to deal with the orchestration across military, government and private sectors is a huge undertaking in and of itself."

Fortunately, though, Schmidt's experience navigating complex organizational issues that plague both federal government and large companies may serve him well. His comprehensive résumé includes stints as the vice chair of President George W. Bush's critical infrastructure protection board and work as the special adviser for cyberspace security for the White House. He also took leading CISO/CSO roles at both Microsoft and eBay and, most recently, served as president of the London-based Information Security Forum, a nonprofit IT security research organization.

"He has the right background and appears to have the right support at the White House to make things happen," says Jerry Dixon, VP for government affairs at InfraGard and director of analysis at Team Cymru. "There are legal issues and varying authorities that still have to be navigated, including potential legislative action. Howard will need adequate resources and staff to tackle the policy issues and to move things forward across government and...with the industry."

Some first steps

With the president having pledged openness in government, Schmidt, whose start date was Jan. 10, says he is personally dedicated to transparency.

"Transparency provides the American people with the ability to partner with government and to participate meaningfully in the discussion about how we can use the extraordinary resources and expertise of the intelligence community with proper oversight for the protection of privacy and civil liberties," says Schmidt.

Jeff Bardin, former CISO at Investors Bank and Trust (which was acquired by State Street Bank) and current VP and CSO at IT consultancy ITSolutions LLC, says Schmidt's recent release of the unclassified description of the Comprehensive National Cybersecurity Initiative (CNCI) shows the desire for openness and helps start the process of direct discourse with the private sector.

In support of these fresh transparency and partnership goals comes Schmidt's main role of coordinating it all – not only the planning required to initiate better security with private entities for the critical infrastructure, but the shoring up of security across all federal government. "Part of the role I have is sitting down with the broad breadth of government activities to look at securing government systems, securing military systems, [as well as] working with the private sector – finding out what [they are] doing, how they are doing it, making sure there's no duplicity between different efforts that are going on, making sure that we're moving at a pace that's fast enough to really affect some long-term positive changes, but not take long-term to get there," says Schmidt.

Another chunk of this job, he explains, involves sifting through the CNCI, as well as the most recent Cyberspace Policy Review, to ensure all of the specific cybersecurity requirements each federal agency has, along with overall goals for the nation, are met comprehensively.

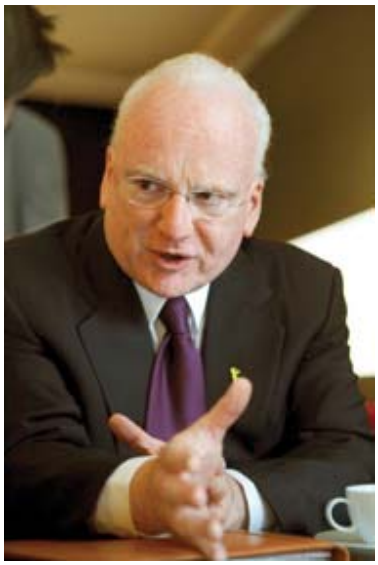
"When you start looking at the key role here, and that's the coordination, a lot of the things that we need to do we know how to do already to make security better," he says. "It's a matter of implementing the processes that we know, making sure people are held accountable for doing those things and moving forward on them."

Looming threats

Moving forward at a fast clip is vital, say many experts, because cyberattackers seem to be charging ahead of most organizations, private or public, at an even faster pace.

Changes have hit both the threat landscape and the planning needed to address it. Digital crimes are worsening, becoming much more sophisticated and frequent, while the economic climate is forcing some organizations to dedicate less than is needed to combat them.

"We have crossed the Rubicon in some way," says Bill Boni, corporate information security officer with T-Mobile, noting that threats are global and often have a macro effect, while information security programs simply are not getting adequately resourced.



As for the types of strikes happening more frequently, there are three major threat areas that should be the focus for Schmidt going forward: cybercrime, cyberespionage and cyberwar, says Richard Clarke (*left*), partner with Good Harbor Consulting and a former White House adviser to the last three presidents.

Cybercrime, he explains, necessitates that a major policy decision be made. "The current approach isn't working because cybercrime pays and we're arresting and prosecuting probably one percent of the people involved in one percent of the incidents that happen," he says. Creating a national cybercrime center is the answer, he says, "rather than continuing the practice that we have now, which essentially devolves the issue to 56 FBI officers and 90 U.S. attorneys, most of [whom] have no skills in this area."

The second big priority would be to undertake a similar national approach with cyberespionage, says Clarke. "China – there are others, but notably China – is engaging in massive, massive cyberespionage that steals all of our data and has a real negative effect on our economic competitiveness."

Nation-state probes, scans, attacks and penetrations of the critical infrastructure and other key resources abound, says ITSolutions' Bardin. "We are under constant attack and have had reams and terabytes of data stolen, but continually crying wolf and driving FUD [fear, uncertainty and doubt] is not necessarily the way to solve the problem," he says, noting that some information security pros continue using this old standby.

The third priority on which Schmidt must focus is that current policy makes the growing problem of cyberwar a major issue, says Clarke.

The government must decide a policy that would state its responsibility to defend all of America's cyberspace in the event of a cyberwar. Such a defense might involve, during a wartime situation, the National Security Agency (NSA) supporting tier-one internet service providers (ISPs), helping them scan for attacks, explains Clarke.

On the flipside, the call on policy would be established during peacetime and be based on federal government taking "some responsibility to defend the private sector against cyberespionage and potential cyberwar," adds Clarke.

Though he's uncertain about the federal role during such a time, Boni says he imagines it'd be the same as one they'd take during a physical incident, which means the government would enlist the authority it needs to do what's necessary to defend the country.

Process changes

New technologies and enhancements to existing processes will help to support initiatives going forward, says Schmidt (*right*). "Many of the things to enhance security do not require huge investment, but require process changes to better protect their systems," he explains. "Over time, investments in technology that is better designed to operate in the threat environment will take us to a new

level."

To shore up security processes and technologies internally, Schmidt says he's working with two key senior pros at the White House: CIO Vivek Kundra, on the IT systems management side of the Office of Management and Budget, and Aneesh Chopra, CTO, to review the future wave of technology and next-generation tools that might be rolled out. Their talks are all about "making sure that security doesn't become an afterthought, that we're doing things specifically…to make sure security and privacy controls are built in right from the outset."

With Chopra, Schmidt is looking at the .gov space as a single enterprise, with hopes of making systems less expensive and more secure. In the process, they're reviewing continuous monitoring and security incident and event management (SIEM) solutions, enterprise management tools that include security and privacy controls, and more – all with the goal of getting visibility into the entire .gov infrastructure, rather than into the discrete organizations that comprise it.

Even with some of the right solutions deployed, incentives for both government entities and private companies are needed to push more secure environments and better safeguards for customers' personally identifiable data, intellectual property and overall operations critical to the running of the country, say security pros.

One source, who wished to remain anonymous because some colleagues vehemently disagree on this point, says something akin to the recent initiative being undertaken by the Federal Communications Commission (FCC) might prove better than any additional regulatory mandates. In April, the FCC announced its move into the cyberspace realm with a proposed Cybersecurity Certification Program. Through this new program – and after input from private industry – the FCC hopes to convince broadband companies to obtain a cybersecurity certification that verifies their compliance with a set of baseline best practices. Certifications would be audited periodically.

With this type of incentive, market choice could drive companies to enlist best practices rather than regulations forcing them to. So, if companies decide to forego the certification process, they would then have to accept the possibility that consumers may choose other organizations that hold the IT security certification.

Market incentives such as this work, say many experts. All one has to do is look to the Payment Card Industry Data Security Standard (PCI DSS).

Others agree that legislation and market-driven incentives do help, although most contend that compliance doesn't equate to security. Because cyberspace moves so quickly, often such mandates and plans are simply a measurement of a certain point.

Yet, laws forcing compliance often prompt senior-level executives to give IT security planning the support, resources and funding it needs, says Bardin. "I hate to see this as a major tool, but how else will we move initiatives to requirements?," he says.

On the federal side, at issue is whether agencies will acquiesce to a more centralized information security practice.

"These organizations will not go quietly into the night with respect to giving up some of their responsibilities and, in turn, power," explains Bardin. "Legislation outlining clearly defined roles and responsibilities across all overlapping agencies needs to be drafted and signed to force consolidation. Howard cannot do this alone. Many commercial organizations that go through mergers and acquisitions have to consolidate resources where it makes sense."

Partnering for security

Still, improvements are being made. For example, the president designated a privacy and civil liberties pro to Schmidt's office. “So not only do I personally look across the privacy and security spectrum, we also have someone dedicated who looks strictly at privacy and how the government is doing things as part of the comprehensive cybersecurity coordination effort,” says Schmidt.

The federal government also is making inroads to re-establish and expand long-discussed public-private partnering, adds Schmidt. Acknowledging that negative perceptions by private sector companies about the federal government's role in such a relationship still exist – such as failing to engage in two-way conversations to share information or attempting to take the lead when many government systems are far from secure themselves – Schmidt says delivering on promises and ensuring transparency and openness on both sides will propel the way forward. Already, progress is happening on this front as the Department of Defense (DoD) works with the DIB (Defense Industrial Base), using a model that might expand to initiatives with other sectors.

Even so, more must be done on the partnership side, say many experts. Better defining the roles and embracing openness are vital to the success of any work to safeguard the critical infrastructure.

“I do not think there are enough resources to do the job the way it's being approached now,” says T-Mobile's Boni. “The boundaries between organizations and between official and private sectors do much more to divide and limit the effectiveness of societal response.”

And while the security community on the private side does have the wherewithal to assess and anticipate many of the emerging threats and vulnerabilities, says Boni, the federal government can play a part here.

“The benefit of the federal role is to help focus and align the various domains – academic, corporate, official – into a more holistic effort that can also increase the range and depth of the analysis of emerging issues,” he says.

Another key undertaking for Schmidt, he adds, would be to create a globally rooted protection framework.

Right now, a major impediment to a more robust public/private partnership is that a lot of the practices around IT “are frozen in a Cold War concept of security that relies too heavily on national defense classification mechanisms and is impeded by security clearances and compartmentalization, which are needed to fight wars, but make unwieldy forming ad hoc communities of economic and technical interest,” explains Boni. “Changing [who we partner with and how] is likely to be very difficult, but necessary to bring a broader range of talent and capability into the effort.”

Getting it done

The impact of cybercrime, whatever form it takes, is being felt by all. The bigger issue now is just what kind of overall economic impact these attacks could have and how all the players will prepare for a more comprehensive onslaught or series of assaults that could affect the country's way of life. What Schmidt must do, says Boni, is “plant seeds of resiliency that will grow outside of the Beltway,” as well as impel all sectors to help reinforce the critical infrastructure against a range of attacks.

It's a tall order, but one that most experts believe Schmidt can achieve. His experience, combined with the attention that the administration, Congress and others are paying to cybersecurity, as well as the maturing of public/private partnering, will facilitate progress, says Dixon.

“I am very positive that the policy issues will be ironed out, there will eventually be a streamlined incident coordination capability in place, and the country will become more prepared for dealing with cyberattacks,” he says. “Having a cyber coordinator at the White House with the right authorities and backing by the president will go a long way in helping to further transparency and cooperation.

Nevertheless, some questions still persist about the creation of a truly actionable plan that evolves the country's security. There are so many priorities that no one person can bear and resolve them all, says Bardin.

But, because Schmidt has a strong sense of mission, he'll be able to lead public and private groups to better organize and establish stronger security plans to not only defend the nation's infrastructure, but its economic viability, say some experts.

“We're here today, this is a permanent office and, basically, we have tremendous focus on behalf of the president across government in this, so things are where they need to be,” says Schmidt. “And that's the bottom line.”

[sidebar 1]

Tech talk: Enlisting technologies

Whatever one calls it – cyberwar, cybercrime, cyberespionage – the government of the United States and enterprises both public and private are clearly in the midst of fighting an onslaught, say many experts.

“The event where Microsoft got a court order to disable enemy machines was the most clear example I saw of us being on the offensive,” says Jennifer Bayuk, principal at consultancy Jennifer L. Bayuk LLC and formerly senior managing director and CISO at Bear Stearns. “The fact that we are not sure if the enemy is a nation state or organized crime does not make much of a difference in cyberspace.”

In February, a U.S. federal judge granted Microsoft a court order in a civil trial to cut off some 277 .com domains tied to the Waledac botnet – a major source of spam and computer infections used by what many believed were Eastern European-based cybercriminals. Cutting off the domains removed command-and-control servers that the spammers enlisted to send orders to the botnet, which reportedly comprised hundreds of thousands of infected machines.

Security, then, is a systemic issue, says Bayuk, so a one-size-fits-all approach must be avoided. Howard Schmidt knows this better than anybody, she says.

“Each system's environment has got to have security designed in such a way that enables resiliency,” she says. “As technology is generally moving in that direction, security should serve to strengthen emerging technologies rather than stifling them.” *– Illena Armstrong*

[sidebar 2]

Transparency: Key to progress

Operation Aurora, the January attack on Google and about 30 other companies and government agencies, such as the Department of Defense (DoD), ended in the theft of intellectual property – likely source code, say many experts. The sophisticated coordinated attack, found to originate from China, also sought out the Gmail accounts of human rights activists. Google, Adobe and other compromised companies have been lauded by information security experts because of their openness about the attack.

“When people who are otherwise well-equipped – think Google, DoD – are successfully attacked, we as a security community have to ask how this can happen and what the national strategy must do differently to enable more effective prevention and response to the next attacks,” says Bill Boni, corporate information security officer with T-Mobile. “We probably need to change our focus from adequate prevention to increased attention [on] effective timely response. Overall, we likely need to put a lot more resources into collection and dissemination of situational intelligence, and sharing this information via communities of shared interests.”

The general industry feeling toward large companies like Google that were victimized by Aurora is that their

embrace of transparency ultimately helps others keep up to date on attack types, their own vulnerabilities and the security mechanisms they must bolster. – *Illena Armstrong*

Photos of Howard Schmidt taken at the White House by Aaron Clamage