CENTER FOR APPLIED CYBERSECURITY RESEARCH

INDIANA UNIVERSITY

COMMENTS TO THE WHITE HOUSE 60-DAY CYBERSECURITY REVIEW

Submitted by

Fred H. Cate
Distinguished Professor,
C. Ben Dutton Professor of Law,
Director, Center for Applied Cybersecurity Research

March 27, 2009

I very much appreciate the opportunity to provide input into the White House 60-day cybersecurity review. You asked for a list of those things that the review team would be remiss if its final report did not take into account. The observations below reflect my own idiosyncratic collection of twelve key points that I believe your report should include, all of which I am confident you are already aware of.

I have surveyed many of my colleagues involved in Indiana University's cybersecurity efforts, and also consulted with professionals in the diverse settings in which I work (including law firms, corporations, government agencies, civil liberties groups, and research universities), but the list is my responsibility alone. I have divided the list into five observations about the current threat picture and seven recommendations about essential steps for combating cybersecurity threats more effectively in the future.

Observations About the Current Threat Horizon

1. Private-Sector Critical Infrastructure

The government has focused significant resources on securing its networks, but very little attention on the private sector, yet it is the private sector that controls the vast majority of critical infrastructure: transportation, utilities, communications, financial services, manufacture and supply of essential commodities, etc. All of this critical infrastructure depends heavily on information and networks. As described in greater detail below, almost all of this information and these networks interconnect with the Internet, which makes them easily accessible and particularly vulnerable. For

example, in January 2008, the CIA reported that attackers have broken into the computer networks of utility companies and then made demands, in at least one case causing a power outage affecting "multiple cities." Moreover, increasingly critical information is both controlled by the private sector and carried via the commodity Internet (e.g., ATM transactions, financial data, health data)

As a result, enhancing the quality of information security in the private sector is critical to protect valuable data and communications systems, to secure systems that control other elements of critical infrastructure (such as the wireless switches that route trains and control pipeline flows), and to secure other (e.g., government) networks that connect with those private-sector systems.

2. The Interconnectedness of Networks, Data, and Threats

"Interconnectivity" seems to be the hallmark of our information networks and the data they carry, as well as, increasingly, of information security threats. So private-sector systems interconnect with each other and with government networks through the Internet. This means that all of those systems are more easily accessible to attacks from foreign countries. This also means that vulnerabilities in one network inevitably weaken information assurance in others.

Interconnectivity also provides valuable tools for wrong-doers, who take advantage of it to organize those attacks, identify targets, expand the attacks surface through botnets and compromised computers, access and sell data stolen via attacks, share attack software and strategies, and evade detection. (Consider that 42 percent of phishing websites observed in the first half of 2007 originated from just three phishing toolkits. Stefanie Hoffman, "Storm Warning," *Varbusiness*, Jan. 28, 2008, at 32.) There is growing evidence of wrongdoers collaborating, and of data stolen in one setting having value in others (for example, account number stolen for financial fraud purposes being used to enhance the apparent authenticity of a phishing message seeking credentials for secure networks).

Interconnectivity also is a hallmark of data. This complicates security because of the ability, already described, to use data from one setting for other purposes (for example, using mother's maiden name or city of birth to answer security questions), the tendency of most people to reuse passwords and security questions (four-fifths of people acknowledge using the same password across sites according to a 2005 Verisign study), and the ability to infiltrate compromised data from one setting into another.

There are two overwhelming lessons that emerge from this interconnectedness. First, to secure data *anywhere* requires raising the quality of information assurance *everywhere*. The communicable disease metaphor is quite apt: you can take all the precautions you want to guard against catching the disease, but to be really safe you have to eradicate it everywhere through vaccinations and other means. Second, information assurance is a global issue, both in the sense of requiring multinational cooperation and in the sense of needing to be addressed on all networks and at every level.

3. The Threat Trajectory

There seems universal agreement that information security threats are getting more malicious and causing or having the potential to cause greater damage than ever before, but it seem equally clear that there are still unexplored possibilities for their potential impact. For example, entire networks

might be crashed, eliminating access to cash or electricity or water. Networks might be compromised in ways that cause significant collateral damage, such as directing airplanes or trains into each other, or causing massive chemical or gas leaks. Command and control systems for the military might be disrupted. False data might be introduced into financial systems causing a further reduction in the reliability and stability of banks, or causing major disruptions in supply lines.

This is no idle parade of horribles. We have enjoyed a relative honeymoon in terms of the severity and impact of malicious code and social engineering, and all signs are that this is changing.

4. Human Vulnerabilities

Threats to data and information networks are many and varied, but increasingly the most successful ones take advantage of human vulnerabilities. These vulnerabilities occur at every level—from not following well establish security procedures to being victimized by phishing or other fraud tools to disclosing access credentials to insiders taking advantage of their privileged access to steal or share sensitive data. Phishing, especially when combined with targeted data ("spear phishing"), and other socially engineered attacks are a particular risk. In one Indiana University study, the percentage of recipients of a phishing message persuaded to provide their account name and password increased from 16 percent to 72 percent when the researchers made it appear that the fraudulent message originated from a Facebook friend. See Markus Jakobsson & Steven Myers, *Phishing and Its Countermeasures* 202-03 (2007).

There is also a tremendous amount of what might be described as bad behavior by users. In 2005 Verisign found that two-thirds of 272 people stopped on the street in San Francisco were willing to trade their network passwords for a $3 Starbucks card. "One executive, too busy to stop, sent his secretary back with his password so he could get the free coffee. She gave up hers, too." Mary Anne Ostrom, "Free Coffee Buys Passwords in San Francisco," *San Jose Mercury News*, May 6, 2005. Social networking is another prime example where even people who claim to be knowledgeable about privacy and security supply sensitive data about themselves and their acquaintances in astonishing numbers.

The weakest link in any system of information assurance is the human user. In the words of Johnny Long (aka JohnnyHax), Jack Wiles, and Kevin Mitnick: "If I was asked to compromise a large organization or government department with a brief to discover or destroy a given piece of data I would rely less on technology and more on human weakness. . . . Despite the best computer software and hardware, there is a human somewhere who holds the keys to the kingdom." *No Tech Hacking* (2008).

5. A Process, Not an End

Information assurance is a process, not an end. Absolute security will never be achieved; the goal is to stay ahead of the bad guys in a perpetual arms race. The impossibility of a clear victory makes obtaining the necessary resources and sustaining the continued investment and scrutiny very difficult, but all the more essential. I always conclude talks about security by saying that it is a fight we are never going to win, but cannot afford to lose.

Recommendations for Moving Forward

6. Create Better Incentives

Cybersecurity is a field in desperate need for better incentives. At present it suffers from a "tragedy of the commons" phenomenon by which many key players assume someone else is providing for security, combined with a sense of despair about the size and complexity of the challenge that often frustrates significant investment. While I would argue it is almost always preferable to allow markets to create appropriate incentives for desired behaviors, there are occasions where government intervention is necessary. Information security is one of those instances. The threats are too broad, the actors too numerous, the knowledge levels too unequal, the risks too easy to avoid internalizing, the free-rider problem too prevalent, and the stakes too great to believe that markets alone will be adequate to create the right incentives or outcomes.

Unsecured computers and networks, as well as unsecured data, threaten us all, yet individuals connect to broadband networks and install home wireless routers with no security and little awareness of how to provide adequate security or the importance of doing so. They visit unsecured websites, download suspect files (even installing peer-to-peer software to facilitate doing so and also providing the world with unhindered access to their machines), share passwords, fail to install or update antivirus software, connect to insecure wireless networks, and install unverified programs and equipment in our homes and offices, often in violation of corporate policies.

Meanwhile, few institutions adequately value the cost of lost or missing data, unless it concerns their own trade secrets or proprietary information. Too many businesses sell digital products and services that are not secure, and use personal information in ways that make it vulnerable to error and abuse. While cyber attacks are growing increasingly sophisticated and malicious, many of the most successful take advantage of our simple failure to do the things that individuals and institutions know they should to protect themselves. Clearly, better incentives are necessary.

Where markets fail to produce appropriate incentives, we usually look to law, yet, as economists Bruce Berkowitz and Robert Hahn observe, the government has largely rejected "regulation, government standards, and use of liability laws to improve cyber security *in toto*. These are all basic building blocks of most public policies designed to shape public behavior, so one must wonder why they are avoided like a deadly virus (so to speak)." Bruce Berkowitz & Robert Hahn, *Cyber Security: Who's Watching the Store?*, AEI-Brookings Joint Center for Regulatory Studies, Regulatory Analysis 03-5, at 6 (2003). Without more appropriate standards and oversight, we will never achieve the broad accountability that effective cybersecurity requires.

7. Provide Clearer Statutory Protection for Privacy and Security

A variety of laws have been enacted and constitutional interpretations adopted to try to both ensure that privacy is protected, even at times of great stress, and to provide government officials and the public with clear guidance as to the contours of privacy and security.

However, advances in technology have resulted in what Professor Daniel Solove has described as the law's "profound complexity." Daniel J. Solove, "Electronic Surveillance Law," 72 *George*

Washington Law Review 1264, 1292 (2004). Courts have "described surveillance law as caught up in a 'fog,' 'convoluted,' 'fraught with trip wires,' and 'confusing and uncertain.'" Id. at 1293. As a result, privacy is often not protected and public and legislative concerns about the proper line between privacy and security have led to political firestorms over proposed security programs and created great uncertainty and even a sense of personal risk among security professionals in the government.

In addition, under the Supreme Court's "third-party doctrine," sensitive personal data held by third parties is denied any protection under the Fourth Amendment. So the government can, and does, avoid the strictures of the Fourth Amendment merely by requiring a third party (such as a bank) to collect certain information from or about individuals and then obtaining that information from the third party. See *United States v. Miller*, 425 U.S. 435 (1976). This creates incredible pressure on third party businesses to supply data to the government without judicial or administrative oversight.

Irrespective of whether the third-party exemption made sense when decided, excluding records held by third parties from the protection of the Fourth Amendment makes less sense today because of the extraordinary increase in both the volume and sensitivity of information about individuals necessarily held by third parties. Professor Kathleen Sullivan has written: "[t]oday, our biographies are etched in the ones and zeros we leave behind in daily digital transactions." Kathleen M. Sullivan, "Under a Watchful Eye: Incursions on Personal Privacy," *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* 128, 131 (2003). The Supreme Court's exemption from the Fourth Amendment for records held by third parties today means that virtually all personal information is removed from the protection of the Fourth Amendment. As a result, individuals feel more exposed than ever to government scrutiny, and thus are less accepting of measures that might implicate personal information in the quest for better information security.

Imposing some order on the law applicable to privacy and security could go a long way towards building public support for important security measures, while also providing everyone with clearer congressional guidance about the proper protection of privacy.

This issue is of more than merely domestic importance. A growing range of foreign governments in Canada and the European Union have cited the U.S. government's broad access to private-sector records as a basis for blocking the export of personal data to the United States. Addressing this issue is critical to building stronger, more cooperative relationships with our allies in the quest for better security.

8. Prioritize Threats, Responses, and Resources

Information security has been dominated in recent years by a sense of unreality or even irrationality. Businesses make unrealistic promises in an effort to attract consumers or sell security solutions. State and federal agencies have been preoccupied with breach notices to the extent that they feel like a solution in search of a problem. Politicians have made bold statements about the importance of data security, while appropriating a pittance to fund a herculean task. Meanwhile data breaches continue apparently out of control, suggesting that even if they are not the direct cause of broad harm to individuals and the economy, they are at least a symptom of a larger scale problem with institutions being stewards of data rather than merely possessors of it. And individuals behave with an almost breathless irresponsibility towards the security of their own and other's data and systems, largely

insulated from the practical effects of their carelessness by laws and competitive businesses practices that shift financial responsibility to banks and retailers.

It is time we develop a more realistic view of information security threats and of the steps and resources necessary to combat them. In particular, we need a better way of prioritizing threats and responses, and then focusing scarce resources where they can do the most good.

9. Anticipate, Not Merely Respond to, Threats and Vulnerabilities

Security often tends to be backwards-looking, responding to the most recently deployed threat. To a certain degree that is inevitable, but to succeed we need to not only reduce the time between attack and response, but where possible anticipate and counter attacks even before they are witnessed. One key step in enhancing collaboration with the research community, which often identifies, or even predicts, threats before they are witnessed in the wild. Another, described in greater detail below, is to enhance data sharing, so that systems can begin actively combating new threats even before they experience them. A more aggressive, anticipatory approach is necessary, to replace our reactive, perimeter-based approach to information security.

10. Enhance Data Sharing

The response to security threats has not kept up with the sophistication and efficient organization of many of those attacks. The United States lacks good data about the frequency and severity of attacks. Organizations that successfully fend off an attack are not required to notify similarly situated entities, even though evidence shows that attacks driven off from one site just move to a less well protected similar site. Customers receive billions of breach notices, but there is neither centralized reporting nationally (much less globally) of attacks and attack strategies, nor is there broad-based collaboration to identify and repel attackers.

The government needs to facilitate the information-sharing and collaboration necessary to enhance security effectively. At minimum this means reducing barriers to collaboration wherever they occur, but it probably also requires mandatory reporting to the government or some other central clearinghouse of threats. The sector-specific Information Sharing and Analysis Centers created, but never funded, by DHS could serve as a useful model, but they need to be expanded and invigorated.

11. Establish Clearly Defined Lead Civilian Authority

The government has had a difficult time imposing even basic security requirements on its own networks. There are many reasons why, but increasingly I believe one critical reason is that lack of central authority. I speak from personal experience. Indiana University suffered from a raft of security incidents as long as security was managed at the department level. The Trustees acted to centralize information security in one office, reporting through the CIO directly to them. It gave the CIO the authority to take whatever measures he believed were necessary to secure the network, including the power to remove any machine or user if they were compromising the network. Today, under that central authority, every machine is registered to our network. Every machine is scanned for patches and antivirus software before a connection is allowed. All incoming email traffic is scanned. Any malicious code, including phishing, that makes it through the firewall is rapidly identified and either removed or

traffic to the suspect sites blocked. Some malicious traffic is also routed into honeynets so that we can learn more about the attack strategy and develop tools for recognizing and countering it in the wild. As a result of these and other steps our incident rate has fallen dramatically.

The point is not the specific measures that we have taken, it is the existence of centralized authority over cybersecurity. Similar authority is needed within the U.S. Government so that at least all .gov connections are subjected to centralized and proactive oversight, within a system such as that maintained by DHS that actively scrutinizes proposed measures for their impact on privacy and other civil liberties.

12. A "Manhattan Project" for Cybersecurity

During this process, many people have used the phrase a "Manhattan Project" for cybersecurity. I think this accurately captures the mindset that is needed if we are to catch up to the threats we face, much less get ahead.

While the term is almost self-describing, I would highlight two particularly important aspects. First, we need to be careful to protect and facilitate research. Information security research is hampered today in many ways, but one of the most important is the growth of laws (for example, state anti-spyware laws) that impede research. Ironically, many privacy laws, while offering scant protection to individuals from deployed cybersecurity tools, do not protect access to data for research on those tools. This is inexplicable, and contributes to the tendency to deploy tools that have been inadequately tested.

As a nation we need to devote more resources to cybersecurity research and deployment. The government has invested very few resources in enhancing information security when compared with the breadth and severity of the threat. Even the increase in funding promised by the Obama Administration still amounts to the same federal investment scheduled for FY2010 that we currently spend in Iraq in a day—a surprising comparison given how greatly national security officials believe cyber attacks threaten our national interests.

We also need to target research funding better. Much of the limited NSF funding has focused on technical solutions, even though most experts agree that the real challenges are behavioral, policy-, and incentive-based. In addition, funding is often targeted at impractical applications, rather than serious, collaborative research designed to advance the level of cybersecurity.

Second, I urge you to rely on much of the good work that has already been done. To offer just one example, in October 2008, the National Academy of Sciences' released its long-awaited report on information-based programs for fighting terrorism. The report was the product of a three-year study funded by DHS and NSF, chaired by former Secretary of Defense William Perry and Academy president and former president of MIT Chuck Vest. The report included a recommended framework for vetting new national security programs to ensure that they were not only legal and consistent with U.S. values, but also effective and efficient. That framework would seem equally applicable for evaluating new cybersecurity tools as well. See
http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=10072008A

I appreciate the difficulty of the challenge facing you, and I thank you again for the opportunity to offer these comments. Should you desire more input on any point, please do not hesitate to let me know. Good luck.

_____

Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, and director of the Center for Applied Cybersecurity Research at Indiana University. He is a member of Microsoft's Trustworthy Computing Academic Advisory Board, the Board of Directors of the Center for Applied Identity Management Research, BNA's *Privacy & Security Law Report* Advisory Board, and the Board of Advisors of Trustee. He serves as co-editor of the Privacy Department for the IEEE (Institute of Electrical and Electronic Engineers) publication, *Security & Privacy*, and a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP. Previously, he served as a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, counsel to the Department of Defense Technology and Privacy Advisory Committee, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. *Computerworld* listed him in its 2007 and 2008 annual lists of "Best Privacy Advisers."

Indiana University is a recognized leader in information assurance, with an unparalleled collection of people and resources devoted to research, teaching, and improving the practice of cybersecurity. The University's approach is highly interdisciplinary and integrates theory and practice, reflecting IU's long leadership in the intersection of technology, policy, organizational behavior, and law. IU is home to the Global Research Network Operations Center for the Internet2/Abilene network, National LambdaRail's FrameNet and PacketNet, and a dozen other of the most advanced domestic and international research networks; the Research and Education Information Sharing and Analysis Center, operated under an agreement with DHS; the Center for Applied Cybersecurity Research, and the Advanced Network Management Laboratory. The National Security Agency has designated IU as both a *National Center of Academic Excellence in Information Assurance Education* and a *National Center of Academic Excellence in Information Assurance Research*.