Leadership and Responsibility for Cybersecurity

Melissa E. Hathaway

Melissa Hathaway is President of Hathaway Global Strategies, LLC and former Acting Senior Director for Cyberspace, U.S. National Security Council. Hathaway served as Cyber Coordination Executive and Director of the Joint Interagency Cyber Task Force in the Office of the Director of National Intelligence. Previously, Hathaway was a Principal with Booz Allen & Hamilton, Inc.

According to Darwin, "it is not the most intellectual of the species that survives; it is not the strongest that survives; but the species that survives is the one that is able best to adapt and adjust to the changing environment in which it finds itself."[1] We have certainly adapted to the Internet and the technology that underpins it. In fact, we have made it an integral part of just about everything in our life; and in many ways we take it for granted that it will always work twenty-four hours a day, seven days a week. There are approximately 2.5 billion Internet users around the world of which nearly half are below the age of twenty-five.[2] Yet, there is another set of actors that have adapted more successfully: criminals, spies, and some clever guys. Media headlines announce daily that our bank accounts are being robbed, our intellectual property is being illegally copied, and our critical infrastructures are penetrated and could stop working at any moment. The very fabric that contributes to nearly 40 percent of the productivity growth of the global economy also facilitates an equally robust underground economy.[3]

These messages appear to fall on deaf ears as our corporate and political leaders continue to talk about the troubled environment, yet too few are adapting to or assuming the

responsibility for resolving it. Instead, our leaders appear to be paralyzed by the prolonged economic recovery and are in denial of the security needs of our infrastructures and enterprises. Why? Because of the difficulty in balancing parallel demands: economic recovery and growth vis-à-vis national security and infrastructure protection. This tension is further exacerbated by the competition for resources, lagging policy implementation, and an ill-defined technology roadmap to address security shortfalls as we adopt and embed the next-generation technology into our infrastructures and enterprises.

Policy makers, legislators, and businessmen should assess the gap between the current defense posture and our needed front line defense in the face of an increasingly sophisticated range of actors. This paper describes a series of case studies that highlight the lack of attention being paid to this serious problem and the subsequent policy and technology solutions that are being brought to bear to close the gap.

Operation Buckshot Yankee.

In the fall of 2010, Deputy Secretary of Defense William Lynn stated that the Department of Defense (DoD) had "suffered a significant compromise of its classified military computer networks."[4] The penetration occurred in 2008 and was delivered via trusted uniformed military personnel who were using USB mass-storage devices to move important operational information between unclassified and classified systems in support of U.S. Central Command's military operations. The devices at issue contained a malicious computer code, which was able to proliferate undetected from network to network. The code was designed to illegally copy information and, when possible, transfer it to servers under foreign control.

The DoD code-named the discovery of, and recovery from, this incident "Operation Buckshot Yankee." Government leaders wanted to learn the extent of the penetration and whether the networks could still be "trusted." Thousands of man-hours were expended to hunt and isolate the infections. The DoD developed and deployed technology to detect and close communication channels, as well as to eradicate the infections. The total operational and capital cost has yet to be publicly disclosed.

From a policy perspective, the Secretary of Defense and the Chairman of the Joint Chiefs of Staff announced a temporary abandonment of the use of portable media/storage devices. This affected department performance, enterprise agility, and for some, the ability to execute their missions. From a technology perspective, it required a change in architecture. Prior to this event, the DoD focused its defensive posture from an outside-in, defense-in-depth strategy. And even though in 2007, the Comprehensive National Cybersecurity Initiative (CNCI) articulated and funded defensive programs along four attack vectors—insider access, proximity access, remote access, and supply chain access—the DoD had not yet implemented technology to detect and deny tainted technology brought into the enterprise by way of trusted insiders.[5] Operation Buckshot Yankee required the DoD to begin to configure its sensors to look for and alert anoma-

lous behavior inside its networks. It also required the DoD to implement a data loss prevention program to block illegal data loss.

The DoD continues to suffer from more than 6 million probes per day with an untold number of successful intrusions against their unclassified networks.[6] Who is being held accountable for the DoD's cyber posture? Is it the DoD Chief Information Officer, the Director of the Defense Information Services Agency, or the Commander of United States Cyber Command? Actually, it is a combination of these individuals and offices and many more. Ultimately, however, the overall defensive posture for the DoD rests in the hands and responsibility of the Secretary of Defense. And while he may have been embarrassed by a foreign country being able to penetrate the armor of the classified networks, neither the DoD nor any of its leaders appear to have suffered any real penalties or repercussions. If we are to adapt and adjust, we must require greater accountability and demand leaders who will take charge rather than sit back and react only when necessary.

Certificate Authorities. In 2011, governments and corporations alike observed a new trend that threatened their ability to trust Internet transactions: the targeting, penetration, and compromise of companies that produce security products. In particular, the weak security postures of certificate authorities, including Commodo, DigiNotar, and RSA, were exploited, causing a wave of other crimes and consequences. Digital certificates represent a second form of identity to help enhance "trust" for financial or other private Internet transactions by confirming that something or someone is genuine.[7] These certificates have become the *de-facto* credential used for secure online communications and sensitive transactions, such as online banking or accessing corporate email from a home computer.

In March 2011, RSA informed its customers of a breach of its corporate network, which could reduce the effectiveness of its SecurID two-factor authentication token.[8] RSA's SecurID two-factor authentication system is a widely used digital certificate system for remote access logins to corporate networks through virtual private networks and by many financial institutions including the United States Federal Reserve Bank. On 21 May 2011, a leading U.S. defense contractor, Lockheed Martin, had its networks penetrated. The perpetrators used duplicates of RSA's SecurID tokens to gain access to Lockheed's internal network.[9] After this breach and several others resulting from the SecurID issue, RSA leadership stated it would replace tokens, upon customer request but not necessarily free of charge.[10]

Another certificate authority provider was penetrated in June 2011. DigiNotar's corporate network servers were successfully penetrated and hackers gained administrative rights to its system. An audit was ordered by its parent company, Vasco, in July 2011 and the auditors discovered that the cryptographic keys had been compromised and rogue certificates had been issued.[11] The Dutch government was among DigiNotar's key customers.

These compromises represent "a

threat to one of the most fundamental technologies used to secure online communications and sensitive transactions."[12] The impact of these events is multifold. First, it calls into question the validity of two-factor authentication. Clearly, the cryptographic keys can be compromised and therefore, whoever has the "keys to the kingdom" can impersonate something or someone and compromise the integrity of that remote transaction. Second, these companies sell security; it is their brand. If a security company is unwilling to invest in its own security, then why should others invest in theirs? Finally, the incidents caused harm. DigiNotar closed its doors after filing bankruptcy, and RSA suffered a loss of nearly $66 million and a diminished reputation.[13] One could even debate whether RSA's lack of full disclosure of the extent of their breach and compromise of their product's integrity could lead to actions being filed against them—either by customers or government investigators. Time will tell what the true cost of these intrusions will be to the certificate authorities and their customers.

From a policy perspective, certificate authorities in particular and security vendors in general need to get back to security basics. The very enterprises that make a profit on their customers' insecurity are insecure themselves. They are failing to lead by example by not making the basic investment required to secure their own infrastructures and enterprises. They are not even implementing the minimal information security procedures and controls outlined in the Consensus Audit Guidelines or the National Institute of Standards and Technology (NIST) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.[14] Security vendors should use these available resources and implement a policy that recognizes that some data should not be accessible via the Internet and publicly acknowledge the need for and implement better information security controls.

From a technology perspective, these companies have discovered that they need to install new technologies and employ more vigilant processes in their enterprises to detect anomalous behavior and continuously monitor their enterprises for good and bad activity. Additionally, given that the key authentication technology used today has been compromised, it is necessary to move toward the research, design, and employment of multiple chains of trust for devices, users, services, and data sources for all transactions.

The lack of corporate leadership and accountability for these events demonstrate that other market levers may be needed.

Furthermore, the lack of corporate leadership and accountability for these events demonstrate that other market levers may be needed to get the attention of the Chief Executive Officers and Boards of Directors. In Octo-

ber 2011, the Securities and Exchange Commission (SEC) issued a notice to industry regarding cybersecurity, confirming that cyber risk and cyber intrusion events must be reported to the SEC and disclosed to the investing public as risks.[15] If the SEC doesn't hold RSA accountable, will its shareholders and customers do so? It is actions like these that will get the attention of corporate leadership and thereby focus their attention on adapting to address cyber risks.

Cloud-based Architectures. According to the NIST, "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources [e.g., networks, servers, storage, applications, and services] that can be rapidly provisioned and released with minimal management effort or service provider interaction."[16] The networked environment is often measured by one of three attributes: its ability to deliver or make information available, its ability to preserve its confidentiality, and its ability to protect its integrity. Cloud computing is attractive to many businesses and governments because it promises to make information available to its customers anywhere and at any time. But the other two cornerstones of information security—integrity and confidentiality—are not readily commanded by the cloud environment. An October 2010 report on cloud security from Forrester Research, a consulting and research firm, states that security is the single biggest barrier to broad cloud adoption.[17]

Citizens around the world are beginning to experience some of the challenges with cloud-based services. In October 2011, Research in Motion's (RIM) Blackberry services suffered a three-day outage due to a core switch error in RIM's infrastructure. As a result, BlackBerry users in Europe, the Middle East, Africa, India, Brazil, Chile, and Argentina had limited or no access to email, web services, and in some cases voice services.[18] The problem cascaded when the backup system, according to RIM's co-CEO Mike Lazaridis, "did not work the way we intended."[19] For a company whose reliability had consistently helped it maintain a strong customer base, RIM's service outage shook customer confidence.[20] RIM didn't deliver on its promise to provide reliable, real-time communications around the world, and customers lost confidence in the product and service. For shareholders, RIM's domination of the corporate and government mobile IT market share was jeopardized. This service outage left room for the iPhone, Android, Galaxy, and others to take market share and capture displeased customers.

From a policy perspective, it highlighted the need to have disaster recovery mechanisms in place. If you were a customer of RIM, it highlighted the gap in continuity of business operations and the fact that RIM could not deliver on its service level agreements. The tangible and intangible costs are immeasurable. From a technology point of view, it demonstrated the fragility of the cloud and the need to test technology prior to embedding it into core operations. It also showed the need for those who promise a 24/7 service to have a graceful degrading architecture so that customers do not suffer from a lack of

quality or continuity of service.

RIM is not the only company to have suffered from cloud computing issues. Recently, LinkedIn, e-Harmony, Yahoo!, and other social networking sites disclosed that their systems had been breached and their customers' passwords and other personal identifiable information had been stolen. Data breaches have serious consequences—according to a recent report, "victims of data breaches are 9.5 times more likely to be a victim of identity fraud than consumers who did not receive such a data breach letter."[21]

In 1994, Citibank suffered from one of the first data breaches that resulted in loss of funds. It also resulted in the creation of a new corporate position, the Chief Information Security Officer (CISO). Many corporations, especially those selling information services, have personnel responsible for the security of their infrastructure and service offering. LinkedIn, whose June 2012 data breach affected nearly 6.5 million customers, had neither a Chief Information Officer nor a CISO. In a focused inquiry of this gap, the company stated that they have a person who is responsible for the functions of a CISO.[22] Yet, LinkedIn apparently was not taking the appropriate measures to secure customer information until after the breach, according to their corporate blog, when they instituted additional or "enhanced" security measures by adding a layer of technical protection.[23] It remains unclear whether they will appoint an executive who is focused on protecting the corporation's infrastructure and customer data.

Furthermore, for LinkedIn and others, an apology may not be sufficient for its customers or the government. The Federal Trade Commission (FTC), which has filed suits in the past for failure to protect consumers' personal information, is exercising its consumer protection and e-commerce authorities to ensure that "companies live up to the promises they make about privacy and data security."[24] Today, LinkedIn faces at least one class action suit for failure to properly safeguard its users' digitally stored information. Again, whether it is government or private actors, we are witnessing reactions to failures in leadership. Ultimately, we need proactive leaders to drive change and address cyber risk early.

Weapons and the Internet.

Critical infrastructures deliver essential services like water, electricity, oil and gas, and sewage, requiring certain components to be able to deliver the product (e.g., electricity) to the customer (e.g., business or household). These infrastructures are comprised of many computer, controller, and network communications components. A supervisory control and data acquisition system (SCADA) or industrial control system (ICS) is at the heart of the functionality of this ecosystem, as it monitors and controls processes and flows of information.

Over the last decade, industry has increased connections between information technology and control system networks to reduce cost and increase efficiency of systems. Executives acknowledge that such connections create security issues because they have chosen to shift their operations from once isolated systems to open protocols where individuals and computers can

gain access to remote sites through the use of modems, wireless, private and public networks, all of which are facilitated by the Internet.

The Stuxnet worm infected more than sixty thousand computers around the world and was "designed to penetrate and establish control over remote systems in a quasi-autonomous fashion."[25] Its use resulted in the degradation and ultimate shut down of Iran's nuclear facility in Natanz. The source code was analyzed around the world, replicated (e.g., Flame and DuQu), proliferated, and has been traded on the black market. In fact, security officials worry that this worm will be used again to attack other critical infrastructures that rely on computers and have the same security flaws.[26]

Finding the ICS vulnerabilities does not require a strong industrial base or well-financed operations—even a kid could do it. As a young explorer of the Internet, a teenage computer programmer named John Matherly developed an Internet mapping tool called Shodan. By combining a search engine, Google Maps, and his understanding of the Internet, he was able to locate thousands of Internet connected devices based on city, country, latitude/longitude, hostname, operating system, and IP.[27] He gave this tool to his friends, and they quickly realized they were able to access uncounted numbers of industrial control computers that were wide open to exploitation and digital sabotage.[28]

From a policy perspective, enterprises that are dependent on control systems are forced to conduct vulnerability assessments and review their risk management controls (e.g., risk register) due to the potential issues related to worms, such as Flame and Stuxnet.[29] The worry is that the malware could deliberately or inadvertently shut down infrastructures and/or operations. These same enterprises also have to review, create, or update their disaster recovery plans. Architecturally, technology needs to be inserted into the enterprise to detect any changes in the "state" of the system. For example, electric utilities and grid operators can use the Cyber Security Self-Evaluation Survey Tool, developed by the United States Department of Energy to "identify opportunities to further develop their own cyber security capabilities," by considering "a series of questions that focus on areas including situational awareness and threat and vulnerability management."[30]

The deployment of Stuxnet raises a new set of questions and…even more concerns about the future of the Internet and Internet-based infrastructures.

The deployment of Stuxnet raises a new set of questions and for many, even more concerns about the future of the Internet and Internet-based infrastructures. Did the decision-makers who decided to use Stuxnet consider the consequences of proliferation of the

capability and potential re-use or retaliatory deployment of a similar weapon? Or were they seduced by the technology and ability to deliver it stealthily over the Internet? Did they review their infrastructure's own vulnerabilities and determine that the offensive use outweighed the risk and consequences of domestic infrastructure outage? Was there even a responsible debate?

Conclusion. Leaders—both in government and business—are expected to be responsible and address key problems. The inescapable conclusion from the examples discussed in this paper, however, is that our leaders are failing in their duties by not acting quickly enough, and are instead being out maneuvered and outwitted by those who intend harm. The examples in this paper show a reactive approach to change, whether in the DoD after Operation Buckshot Yankee, with RSA and other certificate authorities that suffered critical breaches, RIM's crippling service outage, or the Stuxnet worm infecting critical infrastructures around the world. Denials, apologies, or reactive change will not solve the problem, nor will continued study and debate on potential legislative changes or government oversight.

Darwin taught that to survive one must adapt and adjust to a changing environment. As the world continues to progress digitally, real leadership requires adopting and embedding sometimes-costly security solutions into our core infrastructures and enterprises and stop leaving the security of companies, governments, and individuals to chance.[31] Leaders in government and business must work proactively to finally take steps to adapt and adjust to where the cyber environment already has evolved, and if they don't, they must be held accountable.

NOTES

1 Charles Darwin, *On the Origin of Species* (London: John Murray, 1859).

2 International Telecommunications Union, "The World in 2011: ICT Facts and Figures," Internet, http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

3 Jesus Rodriguez and Diego Martinez, "The Role of ICT in the Economic Growth and Productivity of Andalucia," *European Commission, Joint Research Centre, Institute for Prospective Technological Studies* (2007): 11, Internet, http://ftp.jrc.es/EURdoc/eur22781en.pdf.

4 William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstratgy," *Foreign Affairs* (September/October 2010), Internet, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

5 Insider Access: Unauthorized use or access to information, systems, and networks by otherwise trusted agents (employees). The White House, "The Comprehensive National Cybersecurity Initiative," (August 2009), Internet, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative. See also, Melissa E. Hathaway, "Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal," (Statement for the Record House of Representatives Committee on Homeland Security, Sub-Committee on Cybersecurity, Infrastructure Protection and Security Technologies, 24 June 2011).

6 Probe: Any attempt to gather information about an automated information system or its on-line users. Computer intrusion: An incident of unauthorized access to data or an automated information system. Keith Alexander, "Testimony," (Statement for the House of Representatives Committee on Armed Services, Subcommittee on Emerging Threats, 20 March 2012).

7 Certificate Authorities issue secure socket layer (SSL) certificates that help encrypt and authenticate websites and other online services.

8 EMC Corporation, "8K Report for the Securities and Exchange Commission," (filed 17 March 2011).

9 Jeffrey Carr, "An Open Source Analysis Of The Lockheed Martin Network Breach," *Digital Dao Blog*, (31 May 2011), http://jeffreycarr.blogspot.com/2011/05/open-source-analysis-of-lockheed-martin.html.

10 Arthur W. Coviello, Jr., "Open Letter to RSA Customers," (March 2011), Internet, http://www.rsa.com/node.aspx?id=3872. See also, Kim Zetter, "RSA Agrees to Replace Security Tokens After Admitting Compromise," *Wired Magazine*, (7 June 2011), Internet, http://www.wired.com/threatlevel/2011/06/rsa-replaces-securid-tokens/.

11 Fox-IT, "Interim Report: DigiNotar Certificate Authority breach "Operation Black Tulip," (5 September 2011): 5.

12 Symantec Corporation, "Symantec Internet Security Threat Report: 2011 Trends," (April 2012): 13.

13 Arthur W. Coviello, Jr., "Written Testimony," (For the United States House of Representatives, Permanent Select Committee on Intelligence, 4 October 2011).

14 NIST develops and issues standards, guidelines, and other publications to assist public and private institutions with managing cost effective programs to protect their information and information systems. The controls outlined in the 800-53 document include a set of management, operational, and technical safeguards (or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. The CAG outlines best practice guidelines for computer security and recommends twenty security controls that organizations should implement to block or mitigate known attacks. National Institute of Standards and Technology, "Information Security," (August 2009). SANS, "Twenty Critical Security Controls for Effective Cyber Consensus Audit Guidelines," October 2011, Internet, http://www.sans.org/critical-security-controls/cag3_1.pdf.

15 U.S. Securities Exchange Commission, "CF Disclosure Guidance: Topic No. 2, Cybersecurity," (13 October 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Public companies have existing obligations to disclose material risks and events on their public filings. A risk or event is material if it is important for the average investor to know before making an investment decision. Material risks can include cyber risks and material events can include cyber breaches, including the theft of intellectual property/trade secrets, penetrations which compromise operational integrity, etc. See also, Melissa Hathaway, "Creating the Demand Curve for Cybersecurity," *Georgetown Journal of International Affairs. Special Issue: International Engagement on Cyber*, (Winter 2011): 165. While RSA disclosed the incident with the SEC, it claimed that the event was not material in nature.

16 Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing," (Version 15 October 2009), Internet, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

17 Jonathan Penn, "Security and the Cloud: Looking At The Opportunity Beyond The Obstacle," *Forrester Report*, (October 2010).

18 Charles Arthur. "BlackBerry users revolt against RIM as disruption spreads," *The Guardian*, (11 October 2011), Internet, http://www.guardian.co.uk/technology/2011/oct/11/blackberry-users-revolt-against-rim.

19 Julianne Pepitone. "BlackBerry service restored after worst outage ever," *CNN Money Tech*, (13 October 2011), Internet, http://money.cnn.com/2011/10/13/technology/blackberry_outage/index.htm.

20 The fact that it occurred the same week that Apple was launching its iPhone 4S further compli-

cated its situation, as RIM has struggled to keep up in the smartphone and tablet markets.

21 Javelin Strategy & Research, "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier," Internet, https://www.javelinstrategy.com/brochure/239.

22 Eric Chabrow, "LinkedIn Has Neither CIO nor CISO," *Data Breach Today*, (8 June 2012), Internet, http://www.databreachtoday.com/blogs/linkedin-has-neither-cio-nor-ciso-p-1289.

23 Vincente Silveira, "Taking Steps to Protect Our Members," *LinkedIn Blog*, (7 June 2012), Internet, http://blog.linkedin.com/2012/06/07/taking-steps-to-protect-our-members/.

24 Federal Trade Commission, "FTC Files Complaint Against Wyndham Hotels for failure to Protect Consumers' Personal Information," (26 June 2012), Internet, http://www.ftc.gov/opa/2012/06/wyndham.shtm.

25 James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February–March 2011): 24.

26 Stewart Meagher, "Stuxnet worm hits the black market," *THINQ*. (25 November 2010), Internet, http://www.thinq.co.uk/2010/11/25/stuxnet-worm-hits-black-market/.

27 See Shodan software at: http://www.shodanhq.com

28 Robert O'Harrow Jr., "Cyber search engine Shodan exposes industrial control systems to new risks," *The Washington Post*, 3 June 2012, Internet, http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html.

29 A worm is a destructive program that replicates itself throughout a single computer or across a network, both wired and wireless. It can do damage by sheer reproduction, consuming internal disk and memory resources within a single computer or by exhausting network bandwidth. It can also deposit a Trojan that turns a computer into a zombie for spam and other malicious purposes. Very often, the terms "worm" and "virus" are used synonymously; however, worm implies an automatic method for reproducing itself in other computers. "Worm Definition," *PC Magazine*, Internet, http://www.pcmag.com/encyclopedia_term/0,2542,t%3Dworm&i%3D54874,00.asp.

30 AOL Energy, "How Good is Your Security? A New DOE Tool Will Help You Find Out," (10 July 2012), Internet, http://energy.aol.com/2012/07/10/how-good-is-your-security-a-new-doe-tool-will-help-you-find-out/.

31 Jack Goldsmith and Melissa Hathaway, "The Cybersecurity Changes We Need," *The Washington Post,* (29 May 2010), Internet, http://www.washingtonpost.com/wp-dyn/content/article/2010/05/28/AR2010052803698.html.