February 12, 2013

Raising the Bar for Cybersecurity

James A. Lewis

> "What was previously classified as an unlikely but very damaging event affecting one or a few institutions should now probably be thought of as a persistent threat with potential systemic implications."[1]—Dennis Lockhart, President, Atlanta Federal Reserve Bank

Executive Summary

- Analysis of successful attacks has provided good data on both the techniques used in breaching corporate networks and the steps needed to prevent such breaches. However, this information is not reflected in practice.
- Companies underestimate the risk they face of being breached or hacked. Most companies only find out that they have been hacked when told by a third party. This could raise questions of fiduciary responsibility as greater awareness of risk grows in the business community and in government.
- Hacking is incredibly easy; survey data consistently shows that 80 to 90 percent of successful breaches of corporate networks required only the most basic techniques.
- Hacking tools are easily acquired from the Internet, including tools that "crack" passwords in minutes.
- In the last few years, in 2009 and 2010, Australia's Defense Signals Directorate (DSD) and the U.S. National Security Agency (NSA) independently surveyed the techniques hackers used to successfully penetrate networks. NSA (in partnership with private experts) and DSD each came up with a list of measures that stop almost all attacks.
- DSD found that four risk reduction measures block most attacks. Agencies and companies implementing these measures saw risk fall by 85 percent and, in some cases, to zero.
- These measures are "whitelisting," which allows only authorized software to run on a computer or network, very rapid patching both operating systems and programs, and minimizing the number of people on a network who have "administrator" privileges. Implementing these four steps eliminates most of the risk of being breached.
- When the DSD mitigation strategies or their U.S. equivalent are combined with "continuous monitoring" of risk (a term borrowed from the financial risk and audit communities), they provide corporations and agencies the ability to identify and mitigate the risk of cyber attack.
- Companies may need to use other measures and services to secure their intellectual property and networks (from politically motivated denial-of-service attacks, for example), but implementing these mitigation strategies through continuous monitoring for risk is essential for exercising due diligence in protecting shareholder value.
- The White House should direct agencies, in implementing any executive order on cybersecurity and critical infrastructure, to immediately adopt these mitigation strategies as an initial measure while the National Institute of Standards and Technology (NIST) develops its comprehensive set of standards.

[1] Kelly Faircloth, "Cyberattacks on Banks Worry the President of the Atlanta Fed," BetaBeat.com, November 27, 2012, http://betabeat.com/2012/11/atlanta-federal-reserve-president-dennis-lockhart-berlin-cyberattacks-ddos-hactivists/.

Hacking Is Easy

Extracting value from the computers or networks of unsuspecting companies and government agencies has become a big business. No company or agency can ignore network security; it is the source of systemic risk that threatens long-term health and profitability. Companies must secure their networks if they are to exercise fiduciary responsibility and due diligence. Cybersecurity is part of the larger corporate strategy for managing risk and compliance. Cybersecurity risk management is becoming a board-level responsibility. This paper identifies how those responsibilities can be met.

In the past few years, a new approach to cybersecurity has emerged, based on the analysis of data on successful attacks. In this approach, continuous diagnostics and mitigation replace the reactive network security methods used in the past. The approach combines continuous monitoring of network health with relatively straightforward mitigation strategies. The strategies used in this approach reduce the opportunities for attack and force attackers to develop more sophisticated (and expensive) techniques or to give up on the target. In combination, continuous monitoring and mitigation strategies provide the basis for better cybersecurity.

Hacking Is Not that Hard

- More than 90% of successful breaches required only the most basic techniques.
- Only 3% of breaches were unavoidable without difficult or expensive actions.
- Outsiders were responsible for most breaches.
- 85% of breaches took months to be discovered; the average time is five months.
- 96% of successful breaches could have been avoided if the victim had put in place simple or intermediate controls.
- 75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.
- One study found that antivirus software missed as much of 95% of malware in the first few days after its introduction.
- Another study found that 25% of malware is not detected by current techniques.

Cybersecurity is a term that means many different things to many people. It has leapt into prominence as networks moved to the center of business operation, linking companies to what turns out to be a very risky environment. Cyberspace is the Wild West. Governments have not agreed on the "rules" that should apply to cyberspace, or how to apply existing "rules" for espionage, crime, and warfare. Just as Bonnie and Clyde would rob a bank in one state and drive across the border into another state, with the pursing sheriff stopping at the border, smart hackers take advantage of borders and the Internet's ability to cross them with ease and without fear of punishment. They live in countries that tolerate or encourage their activities; they are often outside the grasp of national law enforcement. There are efforts underway to change this, but it will take time to make cyberspace more secure. A good way to think about the cybersecurity challenge is to divide it into three problems:

1. *State versus state conflict.* Cyber war, involving attacks that create physical damage, get the most attention and involve the greatest potential risk to nations and in some instances, such as the recent "Shamoon" attack against Aramco, to companies.[2]
2. *Espionage.* The spread of high-speed global networks makes it easy to extract massive quantities of information. Powerful government agencies target companies, as can competitors and private hackers seeking intellectual property and business confidential information.
3. *Crime.* A cyber-criminal underworld has existed for years, focused on extracting personal information and cash (rather than intellectual property). If a cyber criminal is smart and lives outside the United States, in a country that offers sanctuary, he or she faces almost no risk of prosecution.

When we look at successful attacks, it is embarrassing to note that these are not sophisticated exploits carried out

[2] In August 2012, a group called "Cutting Sword of Justice" linked to Iran claimed it had used the "Shamoon" virus to attack Aramco, a major Saudi oil supplier, deleting data on 30,000 computers and infecting (without causing damage) control systems. The attack also affected the Qatar company RasGas, a major LNG supplier. Other oil companies may have also been infected.

by evil geniuses. Hacking is all too easy. One report estimated that targeted attacks against businesses and governments increased to about 30,000 a year in 2012.[3] The metrics for estimating the damage from a successful hack are not well established. Companies can suffer reduced valuation after they have been hacked, usually in the form of a drop in stock prices. These losses can be significant—ranging from 1 to 5 percent—but the decline is not permanent. Stock prices usually recover by the next quarter. However, it will be interesting to see if this changes as a result of new Securities and Exchange Commission regulations that require companies to report major hacking incidents. In the future, the recovery of stock prices may not be so quick if it is known that there is significant damage to a company's intellectual property portfolio.

It is harder to estimate the damage from the loss of intellectual property (IP). IP now makes up a major part of most companies value, but often the value of this IP is not known until it is put on the market. Counting how much was spent to create the IP is not a good measure of worth. It also takes time for an acquirer to turn stolen IP into a competitive product. In some cases, the damage may not be visible for years. In other cases—such as designs for high-speed trains, automobiles, or wind turbines—the competing product may reach market before the victim company's own design.

The scale of loss and its effect, however, remains a subject of dispute. Anecdotal evidence suggests that cyber crime against banks and other financial institutions probably costs the United States hundreds of millions of dollars every year. Estimates of the dollar value of annual losses to businesses from cyber espionage show a tremendous range, from a few billion dollars to hundreds of billions, but it is safe to say that this is large and growing.

Most people are now aware of the problems with cybersecurity. What many do not know, however, is how simple it is to hack. Currently, the question for hackers, highly skilled or not, is why bother with a high-end attack when something simple will probably work as well. A reasonable goal for policy would be to make hackers work harder for their success. This will reduce both the number of successes and the number of hackers capable of achieving success. Improving the primary level of security will not solve the cybersecurity problem, but it will make it more manageable and, ultimately, easier to "solve."

Numerous studies confirm that hacking is not that hard. Surveys in 2011 and 2012 showed that more than 90 percent of successful penetrations of company networks required only the most basic techniques. Outsiders were responsible for most breaches, and most went undetected for weeks. Usually it was a third party that discovered them. One 2012 survey found that 92 percent of attacks were not highly difficult and that only 3 percent of breaches were unavoidable without difficult or expensive corrective action.[4] "Most victims fell prey because they were found to possess an (often easily) exploitable weakness."[5] Ninety-six percent of successful breaches could have been avoided if the victim had put in place simple or intermediate controls. Eighty-five percent of penetrations took months to be discovered—the average time is five months—and the discovery in most cases was usually made by a third party (such as a credit card company) rather than the victim.[6]

There is a growing cadre of highly skilled hackers, often the proxies of a state that gives them sanctuary. These hackers use programs that continuously scan their target for vulnerable systems, even test systems that are only temporarily online. They have advanced programming skills to identify new vulnerabilities and to create the malicious software (malware) needed to exploit them. With their ability to target specific high-value networks, these high-end hackers can challenge all but the most sophisticated defenders. Equally important, they build and sell the tools and techniques that let less experienced hackers perform successful attacks. Eventually, the work of the advanced hackers in both vulnerability identification and malware writing appears on the cyber black market, becoming globally available.

---

[3] Symantec, *Internet Security Threat Report: 2011 Trends*, vol. 17 (Mountain View, CA: Symantec, April 2012), p. 14, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf.

[4] Verizon, "2012 Data Breach Investigations Report," http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

[5] Ibid., p. 3.

[6] Trustwave, "Global Security Report 2010," https://www.trustwave.com/downloads/whitepapers/Trustwave_WP_Global_Security_Report_2010.pdf.

But successful hacking does not require this level of skill. Relatively simple "hacks" work all too well, and even high-end opponents use them—why use a sophisticated assault when the target can be overcome with a simple one. Most companies that were hacked fell victim because hackers found an easily exploitable weakness. It is so easy that hackers don't have to try very hard because most networks are poorly defended. Eliminating the vulnerabilities exploited by these "easy" hacks will shrink the pool of successful hackers as the less skilled drop out. It will increase the cost for attackers, as they have to put more work into penetrating a target network. Vulnerability mitigation strategies reduce the avenues for potential attack and force attackers to develop more sophisticated (and expensive) techniques or give up on the target. The effect will be to reduce risk and allow companies to focus resources on high-end threats.

The tools for these "easy" hacks are widely available and in some cases freely downloadable from the Internet. A *Washington Post* series explored how hackers can use "Shodan," a downloadable search engine that identifies vulnerable networks and infrastructures, or download programs like "Wireshark," "Aircrack," or "Metasploit,"[7] programs developed as network maintenance and security tools that can be misused for criminal purposes. Hackers have used such tools to create thousands of exploits. Metasploit, for example, is portrayed as a legitimate research tool, but like any tool, it can easily be turned to malicious purposes. It creates programs that can use the Internet to find vulnerable networks and then take control of them. Metasploit has an "open source" version to which anyone can contribute, allowing researchers to share new techniques and hackers to share successful exploits,[8] but it is only one of dozens of downloadable hacking tools.

Cybersecurity Is Feeble

The ability to download hacking tools means that a determined 12-year old with some basic computer skills, if he or she has an Internet connection, can become a successful hacker. For the more advanced, there are cyber-crime black markets that sell personal data, credit card information, tools, passwords, and successful exploits. Criminals can rent "bot-nets" from the cyber-criminal underworld or even purchase complete online stores to collect personal information or to sell bogus products. This is a competitive market, with price wars, guarantees, and special offers. Hacking has become a big business, not only because the Internet is now "where the money is," but because most networks, despite claims to the contrary, are inadequately defended.[9]

Uneven Implementation

- 45% of surveyed companies believed they were doing well; a review showed only 10% were taking adequate steps.
- 70% of surveyed companies use malware detection tools, but only 50% have automated patch management or use intrusion detection tools.
- Only 33% use robust identity and account management systems.

One study found that 75 percent of attacks used publicly known vulnerabilities in commercial software that could be prevented by regular patching—in patching, the software company that made the product sends over the Internet a small fix to an existing program to improve performance or eliminate a vulnerability. A failure to patch leaves the vulnerability unfixed, something hackers are quick to exploit.

While patching is essential, it is not enough. When software vendors announce and ship patches, hackers analyze the patches and can often develop exploits for the problem faster than companies can install the patch. Twenty-five percent of attacks reviewed in this study were new, unknown to defenders, and could not have been stopped. Many security controls—firewalls, intrusion prevention, antivirus—fail to prevent these attacks from succeeding. Often, malware will delete itself after running, and attackers have improved their ability to clean up and hide

[7] SecTools.org, "SecTools.Org: Top 125 Network Security Tools," http://sectools.org/.
[8] Robert O'Harrow Jr., "Hacking tool kits, available free online, fuel growing cyberspace arms race," *Washington Post*, November 13, 2012, http://www.washingtonpost.com/investigations/hacking-tool-kits-available-free-online-fuel-growing-cyberspace-arms-race/2012/11/12/1add77a4-21e6-11e2-ac85-e669876c6a24_story_1.html.
[9] Panda Security, "The Cyber-Crime Black Market: Uncovered," January 2011, http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf.

evidence of what they have done. This complicates the defenders task if their approach is reactive, requiring an analysis of the malware to determine how it functioned and what had been infected.

One way to assess the ease of hacking is to look at the ease of breaking into a network using illicitly obtained passwords. Essentially, the password as we know it is completely useless as a defense. Any password based on a name or word can be rapidly "cracked" with widely available online tools. Passwords based on personal information, such as birthdays, are also easy to guess. Information on social networks can be harvested by hackers to get the personal data that will let them guess passwords. Searching Google on the keywords "password cracker" gets 21 million results, offering free password crackers and advice on how to use them. The hacker's task is made easier by the reuse of passwords, where people use the same password for multiple systems and websites. This reuse is a very common avenue for attack vector, and some data suggests that password reuse is actually a bigger problem than a weak password. Passwords no longer provide any more than the most basic security.[10]

Default settings on computing and network devices are another easy path for attack. Anyone who has bought a computer or other network device knows that the manufacturer sets the password and user name to "admin" and "password." Criminals know this, too. People forget to change these default settings or, for large networks, change most but not all of the settings. A U.S. Air Force study found that in large organizations with thousands of machines, perhaps 5 percent were configured to use the default password and user name. Hacking tools can search automatically for these misconfigured devices.

The most popular technique for hacking currently is phishing, which combines fraud and malicious software to bypass many traditional security measures. Individuals in a company are sent a message that appears to be from a legitimate e-mail address (these addresses are easily spoofed). It has an attachment with a tempting subject, like "Next Year's Bonuses." Sent to a hundred people, hackers can count on a few of them to open the document or click on the link, which immediately installs the malicious software. Advanced hackers may use personal data culled from social network sites to "personalize" the e-mail and make it look more convincing.

How immediate and how visible the damage will be depends on what is taken. Confidential business information, such as sales and marketing plans, plans for new products, or financial data, is immediately profitable for the acquirer. One major oil company lost exploration data that cost it billions of dollars. A major bank saw $10 million extracted in two days; it avoided the damaging publicity by reclassifying the loss as an "operating expense." Companies lose merger and acquisitions strategies and information to hacking, a loss that has an immediate effect—think of the other side of the table having a copy of your briefing book and knowing your bottom line.

The recent attacks on Aramco, where 30,000 company computers had their data erased permanently, along with credible reports of the huge losses of military and commercial technology intellectual property and business confidential information, demonstrate that what governments and companies are doing now in cybersecurity is not working effectively—despite spending as much 7 percent of their information technology (IT) budgets on it. One estimate puts annual spending globally on cybersecurity software at almost $18 billion.[11] However, there is evidence to suggest that the traditional methods are not working. One study found that initial detection rates for antivirus software—there are now almost 50 million different viruses on the Internet—were less than 5 percent when the malware was introduced and that, on average, it took almost a month to update detection mechanisms and spot the new viruses. Another study found that detection rates averaged about 20 percent.[12] Hackers can avoid detection by making minor changes to their malware to evade detection, and some use the updates from security companies to see if their exploits can be detected by the latest updates.

---

[10] Mat Honan, "Kill the Password: Why a String of Characters Can't Protect Us Anymore," *Wired*, November 15, 2012, http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/.

[11] Nicole Perlroth, "Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt," *New York Times*, December 2012, http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?pagewanted=all; Gartner, Inc., "Gartner Says Security Software Market Grew 7.5 Percent in 2011," press release, April 26, 2012, http://www.gartner.com/it/page.jsp?id=1996415.

[12] Imperva, "Assessing the Effectiveness of Antivirus Solutions," *Hacker Intelligence Initiative: Monthly Trend Report* #14, http://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf.

Some business groups argue that companies could improve their network security if there were greater information sharing between themselves and the government. Information sharing is passive and reactive, however, and will always miss a considerable number of attacks (such as the 95 percent of malware missed after its introduction).[13] Someone learns of an attack, analyzes it, and then sends information about it to others. Even if this were done in a matter of hours, it will not work for the 25 percent of attacks that are unknown, nor will it work for rapidly executed attacks, some of which can occur in minutes. Information sharing and reactive approaches to cybersecurity are not effective.

Another traditional approach, the use of "signatures" to identify an attack, is also becoming less effective. A signature is a pattern of code that has been identified as malware. Computers can be programmed to look for that malicious pattern and block it. If the pattern is not known, the attack is not blocked (which is one of the limitations on information sharing). The *New York Times* found that only one of the 45 kinds of malware used in an attack on its networks was detected by its antivirus program.[14] Attackers have also become more sophisticated in evading signature-based controls, often testing their malware on antivirus programs before deployment to see if they can be detected. Advanced attacks can bypass signature-based defenses.

The cybersecurity problem is often presented as the result of a lack of resources. Yet every year, increasing amounts of money are devoted to cybersecurity. The research for this report suggests that the real problem is that cybersecurity resources, adequate or not, are often spent on ineffective activities. Another major problem in cybersecurity is the tendency of corporate leadership to treat it as an "IT problem" best left to chief information officers and technicians. This may have been the right course of action a decade ago, but it is now badly outdated. A better way for a C-suite to think about cybersecurity is that it is the source of a damaging "material effect," hurting a company's profits, value, and financial future, that will be increasingly difficult to ignore.[15]

One survey taken in 2012 found uneven implementation of cyber defense among leading companies. Many companies in the survey believed they were doing well in securing their networks, but a review showed that most were not. While 70 percent used some kind of malware detection tools, only half of the surveyed companies had automated patch management or used intrusion detection tools. Only a third used some form of identity and account management (meaning that an employee's identity must be robustly verified before he can access the network and that, when an employee leaves, the account is automatically closed). Overall, the survey found a "diminution of detection technology arsenals" with declines in the use of malware and intrusion detection tools for, as well as tools for vulnerability scanning, security event correlation, and data loss prevention.[16] A similar survey in Japan found that more than half of the surveyed companies were not even considering cyber countermeasures.[17]

There will always be risk in cyberspace, just as there is risk in driving a car, mailing a letter, or flying in an airplane. The goal is to make online activities no riskier than offline activities—to "normalize" cyberspace. Right now, that is not the case and the risks will grow as we become more dependent on software and computers. But this risk can be reduced and managed and brought to levels where cyberspace is no less secure than any other environment we operate in. We can now describe a minimum standard of due care when it comes to cybersecurity.

Fiduciary responsibility and due diligence on the part of corporate leadership require effective cybersecurity. When people hear that statement, however, it is often the moment when eyes tend to glaze over. Cybersecurity is a business decision about profit and risk. Many companies underestimate the risk and overestimate the cost. Cybersecurity is a decision on business, balancing cost and risk. As with other business decisions, companies with models that generate higher returns or lower costs will outperform their competitors. After a decade or more of

[13] Ibid.
[14] Nicole Perlroth, "Hackers in China Attacked the Times for the Last 4 Months," *New York Times*, January 30, 2013, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?ref=todayspaper.
[15] U.S. Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2: Cybersecurity," October 13, 2011, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[16] Price Waterhouse Coopers, "Global State of Information Security Survey 2013," http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#.
[17] NRI Secure Technologies, "Information Security Survey 2012 Report," http://www.nri-secure.co.jp/whats_new/2013/0109.html.

experience, we can now begin to put together numbers—data collected from actual attacks—to determine what kinds of cybersecurity activities can best reduce risk.

The older compliance and audit-based approach found in legislative mandates like the Health Information Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), and the Financial Services Modernization Act (also known as Graham-Leach-Blilely, GLB) is both resource intensive and ineffective. Compliance is usually a good thing, but in cybersecurity it came to stand for a static, paper-driven method that was expensive without providing equivalent benefits. Now, new approaches are beginning to emerge that offer greater security.

A Proactive Approach to Cybersecurity

This combination of easy hacking and weak defenses has been the situation for many years. The experience of weak cybersecurity has, however, had one advantage—in simple terms, there have been so many attacks that defenders have (if they choose to use it) a very full data set on what kind of attacks have worked. Data, measurement, and analysis of actual events and successful cyber attacks can now guide proactive security strategies. There is still much work to be done in developing consistent techniques and metrics (through work like the NIST S-CAP project),[18] but this approach mirrors, to some extent, both normal approaches to research and the use of "big data" in other business activities. Combine networks and computing power and companies can get a better idea of what is going on and what works. We have, for better or worse, been able over the last five years to amass data on successful cyber attacks and use this data to identify trends and outcomes. The mitigation strategies map defensive actions to data on attacks. They grow out of research by two governments.

Independently, Australia's Defence Signals Directorate (DSD), an intelligence agency responsible for cybersecurity, and the U.S. National Security Agency (NSA), began to count which attacks were most effective and most frequent. They then analyzed why the most frequent attacks succeeded. Like the other surveys, they found that most successful attacks exploited fundamental vulnerabilities. This led them to rank vulnerabilities by frequency and success rate. Both DSD and NSA found that mitigating these vulnerabilities led to dramatic reductions in attacker success.

DSD used the information from its analysis to develop a list of 35 mitigation steps. The first four of these steps provide the greatest defensive benefit. NSA, working with a group of private companies and agencies like the FBI, developed a list of 20 mitigation steps that parallels the DSD list (the U.S. list has fewer steps because its steps have multiple parts). One of the strengths of the DSD and NSA approaches is that they are based on measurements and repeatable data. Another strength is that since most successful attacks consist of several steps that allow the hacker to penetrate the system and exfiltrate data, these measures interfere with one or more of these steps, effectively stopping known or unknown attacks when compared to the reactive approach used in other kinds of defense. A third strength is that the initial data suggest that these measures can actually save money when compared to existing practices.

The data on these two strategies is compelling. We can begin to define the fundamental of cybersecurity in company networks by examining them. One of the best sets of data on effectiveness comes from DSD. Based on the analysis of incidents across the Australian government in the last year, DSD found that more than 85 percent of cyber intrusions can be prevented by following the first four mitigation strategies listed in the "Strategies to Mitigate Targeted Cyber Intrusions":[19]

1. Use application "whitelisting" to help prevent malicious software and other unapproved programs from running—DSD regards this as the most important step companies can take. Rather than trying to identify and block malicious software, which creates the possibility that previously unknown attacks will not be

[18] S-CAP is a set of simple, repeatable protocols allowing security software to send and receive information. S-CAP will enable a real-time response.

[19] Australian Defence Signals Directorate, "Strategies to Mitigate Targeted Cyber Intrusions," October 2012, www.dsd.gov.au/publications/Top_35_Mitigations_2012.pdf.

stopped, using a "whitelist" means that only approved programs can run on a machine. This step eliminates much of the risk from malware.

2. Patch applications such as PDF readers, Microsoft Office, Java, Flash Player, and web browsers. These applications are in daily use in most companies. Patching closes off avenues that hackers will otherwise exploit. Software companies send patches to rectify or eliminate exploitable flaws or weaknesses in a system's design or operation found after it was sold (similar to a recall notice for an automobile). Often, patches are developed in response to the discovery of a flaw by independent researchers or, in some instances, the discovery of a successful hack. A failure to install the patches leaves systems vulnerable. Most companies already have some kind of patching system in place, but research suggests that even with these systems, 5 to 10 percent of computers will "miss" a patch. This means that mitigation works if it is paired with automatic monitoring, which we will discuss later.
3. Patch operating system vulnerabilities, for the same reasons discussed above. All operating systems have potential vulnerabilities; when software companies find and offer a fix, not using that fix leaves the users susceptible to criminals and foreign intelligence agencies, who expend considerable effort to find these "holes" and exploit them.
4. Minimize the number of users with administrative privileges, the highest level of authority to make changes or undertake actions on a network. Easy access to administrative privileges lets criminals who obtain them (and this is a frequent initial goal for most hackers) to install malicious software and change settings to make it easier to exfiltrate data and to hide their criminal activities.

DSD's work parallels an effort in the United States to identify effective cybersecurity measures. Beginning in the early 2000s, NSA developed a list of measures that were effective in stopping or mitigating attacks. The initial list, develop in 2008, was "for official use only," but NSA agreed to share it with the private sector and other agencies to improve cybersecurity on a national basis. This was the basis of the "Twenty Critical Controls" (first published by CSIS), sometimes known as the Consensus Audit Guidelines (CAG).[20]

NSA worked with others who had access to high-value threat information, either because they had large teams that developed and used attack techniques or because they had large teams that performed intensive forensic analysis on a successful attack that identified the tactics, techniques, and methods used by attackers. The consortium included other agencies and companies with access to threat information, either because they had teams that developed and used attack techniques or that performed the after-attack analysis that disclosed techniques used by attackers. This included the Department of Defense, the FBI, the Government Communications Headquarters (GCHQ, the UK counterpart to NSA), several national laboratories from the Department of Energy, and incident response and antivirus companies.

The National Institutes of Standards and Technology (NIST) have excellent security guidelines that provide a very comprehensive set of security controls. The Twenty Critical Controls is a subset of the NIST guidelines that identifies the activities that are priorities for cybersecurity. The group agreed that there were only 20 measures that addressed the most prevalent attacks found in government and industry. This became an initial draft document that was circulated in early 2009 to several hundred IT and security organizations for review and comment. These organizations also participate in an ongoing, periodic review of what is now known as the Consensus Audit Guidelines.[21]

Several different pilot efforts validated the usefulness of the guidelines. The Department of State found in 2009 that the consensus guidelines were effective against the more than 3,000 kinds of attacks made against the department that year. The State Department developed an automated system (which lowered costs) to enforce key guidelines and provide daily mitigation information to managers.

[20] SANS Institute, "CSIS: 20 Critical Security Controls: Version 4.0," http://www.sans.org/critical-security-controls/guidelines.php.
[21] Released in initial form by CSIS as part of its Commission on Cybersecurity for the 44th Presidency.

The UK government's Centre for the Protection of National Infrastructure (CPNI), an agency created by Britain's Domestic Security Service (similar to the FBI) that provides advice on security to businesses in the country, announced that the UK government would adopt the 20 Critical Security Controls as the framework for securing its critical infrastructure. And to help organizations prioritize their cybersecurity efforts against the most common and damaging computer and network attacks, CPNI is now participating in a public-private partnership to promote the guidelines.[22]

New Zealand's National Cyber Security Centre, which provides cybersecurity services to government agencies and critical infrastructure providers, is working with its customers to adopt the top four of the DSD mitigations.[23] In 2012, the Idaho National Laboratory, investigating how to reduce vulnerabilities in the energy industry, validated the utility of the controls for common defenses across IT and control systems in the energy sector.[24]

A project at NASA that continuously monitored agency networks found, when it was first implemented, dozens of vulnerable devices that systems administrators did not know about. Because they were not officially known, they were not patched or updated. This experience of finding things that were not known to be on the network is common in many organizations. Removing these systems that were never patched or missed a patch from the network (and there is some data that suggests this could be true for, on average, 2 to 5 percent of all connected devices), eliminates a significant vulnerability that attackers could exploit.

The DSD controls and the Consensus Audit Guidelines do not meet with universal acclaim. Objections fall into several categories. Some are simply a reflection of "not-invented-here." Many reviewers rightly point out that the controls are nothing new and that they are a subset of the measures already identified by the National Institutes of Standards and Technology and other standards bodies. There are, in fact, a plethora of best practices and standards that have accreted over time. Both of these criticisms are correct as far they go. What is new about these controls is that they correlate the most commonly used attacks with defensive measures identified by NIST and others and prioritizes them by effect. NIST guidance, in contrast, runs to several thousand pages, which poses implementation problems. There are many excellent standards for cybersecurity in the public domain, but these two sets of guidelines bring together a knowledgeable, credible, and diverse community to prioritize cybersecurity activities and spending.

One frequently heard complaint is that cyber threats change too rapidly for the mitigation strategies to have any lasting effect. The evidence, however, completely contradicts this point. While the specific instances of new attacks changes quickly, the mechanisms to manage them have some permanence. DSD found that the effectiveness of its mitigation strategies actually increased in 2011 when compared to 2010. DSD noted that "While no single strategy can prevent this type of malicious activity, the effectiveness of implementing the top four strategies remains unchanged."[25] When the chief information security officer of an agency that had implemented the CAG (in combination with automatic monitoring and mitigation) was asked if the CAG, now several years old, had lost effectiveness, he replied that not only were they still effective but that the first four guidelines remained effective against a majority of attacks. The vulnerabilities that attackers exploit remain unchanged. The key strength of the controls is in measuring outcomes and in correlating defensive measures with effectiveness in reducing attacker success.

Another set of objections involves cost and the possibility that whitelisting would slow operations. The Australian experience showed surprising results for the cost of cybersecurity. Implementation of whitelisting and the other

[22] CPNI, "10 Steps to Cyber Security," http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive; CPNI, "Top 20 critical controls for cyber defence," http://www.cpni.gov.uk/advice/cyber/Critical-controls/; CPNI, "Getting started with the top 20 critical security controls for cyber defence," http://www.cpni.gov.uk/advice/cyber/Critical-controls/getting-started/.

[23] New Zealand National Cyber Security Centre, "Application Whitelisting with Microsoft Applocker," June 2012, http://www.ncsc.govt.nz/sites/default/files/articles/NCSC percent20Applocker-public percent20v1.0.5.pdf.

[24] Idaho National Laboratory, *Vulnerability Analysis of Energy Delivery Control Systems* (Idaho Falls, ID: Idaho National Laboratory, September, 2011), http://energy.gov/sites/prod/files/Vulnerability percent20Analysis percent20of percent20Energy percent20Delivery percent20Control percent20Systems percent202011.pdf.

[25] Australian Defence Signals Directorate, "Strategies to Mitigate Targeted Cyber Intrusions," July 2011, http://www.dsd.gov.au/publications/Top_35_Mitigations.pdf.

four DSD techniques significantly reduced incident response costs. Rough estimates suggest that the savings from reduced incident response tasks and reduced "repair" costs for system and data replacement outweighed the cost of implementing and managing the security controls. Most companies with more than a few hundred employees already have in place the "enterprise technology" needed to implement the four controls—many antivirus programs, for example, come with features that provide for whitelisting. Fears from users that these controls would disrupt operations turned out to be false. Implementing the top four strategies can be achieved gradually, starting with the employees most likely to be targeted by intrusions and eventually extending them to all users. The DSD strategy lays the foundation for security upon which companies can build additional defensive structures tailored to other business needs and the risks to information that they face.[26]

At one Australian agency, the Department of Industry, Innovation, Science, Research, and Tertiary Education, the first four measures on the DSD list together stopped all 327 intrusion attempts made in 2011. In contrast, "traditional" security measures missed 287 of these attempts.[27] Of the four, application whitelisting was the control that proved the most effective. Even if the attackers got malware on the system, it couldn't run, as whitelisting proactively prevented it from running by preventing these files from executing on a system. Another study concluded that "No one can dispute that whitelisting is a better approach in the current environment."[28] While the data on implementation of these measures is limited, what is available suggests that roughly a third of companies currently use these or similar proactive techniques, leaving many others potentially unprotected. These vulnerability mitigation strategies reduce the avenues for potential attack and force attackers either to develop more sophisticated (and expensive) techniques or to give up on the target.

Continuous Monitoring for Risk

Continuous monitoring is a familiar term for the finance and audit communities when it comes to corporate compliance and financial risk issues. It has a similar meaning for cybersecurity. "Big data" can be something of a cliché, but it is an easy way to describe how businesses use dynamic monitoring and analysis of activity to predict trends and to identify effective strategies. A somewhat similar approach works for cybersecurity. Combining the DSD and CAG mitigation strategies with automated, continuous monitoring of networks powerfully increases the effectiveness of company cybersecurity efforts.

Continuous monitoring does not mean a round-the-clock watch of a computer screen by a human being. This approach uses the built-in ability of computers to monitor and log performance. Some continuous monitoring systems generate data by comparing network performance and configuration to specific standards and known vulnerabilities. These fit easily with the DSD mitigation strategies. Continuous monitoring continues the trend of moving toward the measurement of outcomes to improve management. The goal is to move away from approaches that are not dynamic or that are reactive and do not provide managers with adequate information to make decisions on risk mitigation. Continuous monitoring allows companies to observe the behavior of their networks and take rapid action to stop problems and is a critical complement to mitigation. Automating the DSD 35 Strategies or the CAG provides daily, authoritative data on the readiness of computers to withstand attack, as well as prioritized action lists for system administrators to maintain high levels of security.

Continuous monitoring can help to automate cybersecurity functions. It allows companies to automatically collect data on the behavior of their networks and generate quantifiable data that allows them to identify risks. It lets them verify that their security measures are working. In combination, continuous monitoring and mitigation strategies form the basis for the guidance for cyber security. The approach combines constant automated diagnostic monitoring of networks for anomalous behavior with mitigation strategies that address the most

[26] These are: catch malware by application whitelisting; patch software and operating systems; and match administrator rights to staff responsibilities.

[27] Interview with Australian official, January 7, 2013. See also Kelly Jackson Higgins, "Government Agencies Get Creative in APT Battle," *Dark Reading*, October 3, 2012, http://www.darkreading.com/threat-intelligence/167901121/security/news/240008438/government-agencies-get-creative-in-apt-battle.html.

[28] Lumension, "The True Cost of Antivirus," April 8, 2011, http://www.slideshare.net/LumensionSecurity/the-true-cost-of-antivirus-how-to-ensure-more-effective-and-efficient-endpoint-security.

frequently exploited vulnerabilities. In addition to reducing costs associated with manual verification, continuous monitoring will highlight security deficiencies before they can be exploited and more rapidly identify ongoing threats to the environment so they can be stopped before achieving their goals.

Effective security requires continuous automated monitoring of agency networks for security problems, immediate access to the National Vulnerabilities Database and other sources of data to be able to identify problems, immediately mitigate them when they are found, and continuously refine defenses. It does not require periodic written reports on compliance. Automation can provide data on the readiness of computers to withstand attack and prioritized lists for system administrators on the actions needed to maintain security. The combination of automated, continuous monitoring and mitigation strategies can reduce costs.

The technologies needed for mitigation and monitoring are commercially available and already included in many antivirus products. Many mid-sized companies (those with more than 200 employees) already own some variant of them. For example, many of the leading antivirus programs have a built-in whitelisting function that can be used without additional cost if it is turned on. Most big companies also have monitoring software of some kind that can be used to measure mitigation. The result is to increase the return on cybersecurity investments already made. The experience of those who have taken this approach is that it involves a reallocation of resources rather than major new investments.

They key point for continuous monitoring is that it must be linked proactively to mitigation of risk. The UK CPNI puts it as "we recommend that continuous monitoring and mitigation strategies form the basis for the guidance for cyber security." This means not waiting to discover that there has been a breach but identifying vulnerabilities (the "attack surface") and closing them off. The combination of mitigation strategies linked to continuous monitoring free up IT resources and personnel to focus on higher-end challenges.

Due Diligence and Risk Management

Cybersecurity is an issue for corporate governance and a part of adequate risk management. Whether a company board has a Risk Committee, or if they rely on their Audit Committee or other committees, there are two questions to ask to assess cybersecurity preparations: are the four mitigation measures in place; and does the company monitor continuously their performance. This is a minimum standard of due diligence to meet duty to shareholders.

Corporations are used to thinking about risk management and IT risk, which can include damage to data integrity, leakage and Wikileak-style disclosure, loss of intellectual property, and cyber crime. For most companies, an effective strategy to deal with these risks will have three parts:

1. Most hacks are the cyber equivalent of leaving the front door unlocked and unguarded. Fix the most common vulnerabilities, using the DSD or CAG mitigation strategies or something similar.
2. This has to be a dynamic process that tracks flows and trends in malicious activity. Put in place some automated process to monitor risk and compliance (similar to financial) that generates regular reports.
3. Complement the mitigation strategies with a threat-based approach that can provide advance warning of threats from politically motivated groups, denial-of-service attacks, and similar kinds of threat intelligence.

The recent executive order on cybersecurity issued by the Obama administration calls, in Section 10, for NIST to develop standards that regulatory agencies can then apply to critical infrastructure. The NIST process will develop a full range of measures for critical infrastructure, building on its extensive work in this area. The process is expected to take two years. In the interim, the administration could use the DSD/CAG mitigation strategies as an initial set of measures to reduce risk. They are already a subset of NIST's existing guidance (found in documents like NIST 800-53) and could be expanded or modified by the NIST process to implement the executive order. Waiting a year or two to put requirements in place would be a mistake. The DSD/CAG measures, particularly the first four DSD measures, can be implemented immediately at low cost. NIST and the administration should put these in place now as a foundational element for NIST's later work. To not do so would leave the United States unnecessarily vulnerable.

Companies will need to use other products and services to deal with these advanced threats. The DSD/CAG mitigation strategies would not help against the massive denial-of-service attacks recently launched against U.S. banks, but at a minimum, the data on the effectiveness of these risk mitigation strategies suggests a review of current practice to ensure that the first four mitigation strategies are in place and that continuous monitoring for risk has replaced some kind of infrequent audit. Employees will still need to be trained, additional security measures may be needed (depending on the value of the asset), and outside services on advanced threats will be useful. That said, cost and complexity are no longer sufficient explanations for inadequate performance in securing networks.

At the same time, as public awareness grows of the threat and the mitigation strategies, expectations will grow for due diligence at companies and in government agencies. Hacking should not be so easy. We now know how to make it more difficult. Companies and agencies that do not avail themselves of these strategies cannot be said to be exercising due diligence. It will take time for standards of accountability to reflect the results of the DSD and NSA/CAG experience, but the first steps for protecting value are clear. The goal is to combine constant automated diagnostic network monitoring with straightforward mitigation strategies that address the most frequently exploited vulnerabilities.

At a national level, these mitigation strategies provide the foundation for better cybersecurity, but an effective national strategy will need additional elements, of course, that go beyond strengthening the ability of individual companies to defend themselves against hacking. That said, these are proven techniques that can make private networks more secure. We have simply been slow in deploying them. This means that part of the cybersecurity problem becomes one of accelerating change in companies and at a national level. If most companies implemented these measures, advanced opponents would expend more resources and use new techniques to regain access to corporate and agency networks. It is also likely that a significant portion of the cyber-criminal community will be squeezed out as they lack the resources to overcome improved defenses. Cyberspace will never be a risk free environment, but we can raise the bar for success in cyber crime and espionage.

James A. Lewis *is senior fellow and director of the Technology and Public Policy Program at CSIS. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His recent work has focused on cybersecurity, including the groundbreaking report "Cybersecurity for the 44th Presidency," space, and innovation. Lewis received his Ph.D. from the University of Chicago.*