Deloitte Review

Issue 19 | 2016

Complimentary article reprint

Government's cyber challenge

Protecting sensitive data for the public good

By William D. Eggers

Government's cyber challenge

Protecting sensitive data for the public good

By William D. Eggers
Illustration by Dongyun Lee

IN THE DOG DAYS OF AUGUST 2015, one hacking scandal made particularly provocative headlines: 33 million customer records were stolen from AshleyMadison.com, a site designed to facilitate extramarital affairs. Hackers held some 10 gigabytes of member data for nearly a month and then dumped the database onto the Dark Web and various peer-to-peer file-sharing sites. Names, addresses, phone numbers, credit card numbers, transactions, and links to member profiles—everything was revealed.

This hack wasn't just big—it was different. Typically, when hackers breach an organization's servers, most of the ensuing costs are related to identity theft, negative brand impacts, or financial or intellectual property loss. But for Ashley Madison customers, the cost was *much* more personal.[1] It wouldn't be such a big deal if the data were merely leaked onto the black market; the possibility of it coming back to haunt any one individual would be fairly low. But within hours of the release, coders had already built websites on which anyone could type in an email address and see if it was in the database.[2]

How did Ashley Madison find itself in this mess, facing years of lawsuits and a potentially fatal breach of customer trust? And more importantly—other than the 15,000 .gov and .mil addresses found in the company's database—why is this relevant to government?

When it comes to protecting sensitive data, Ashley Madison and government agencies have much in common—even if they're worlds apart on mission. Perhaps the greatest similarity is that both store highly sensitive data that could be lucrative in the hands of criminals.

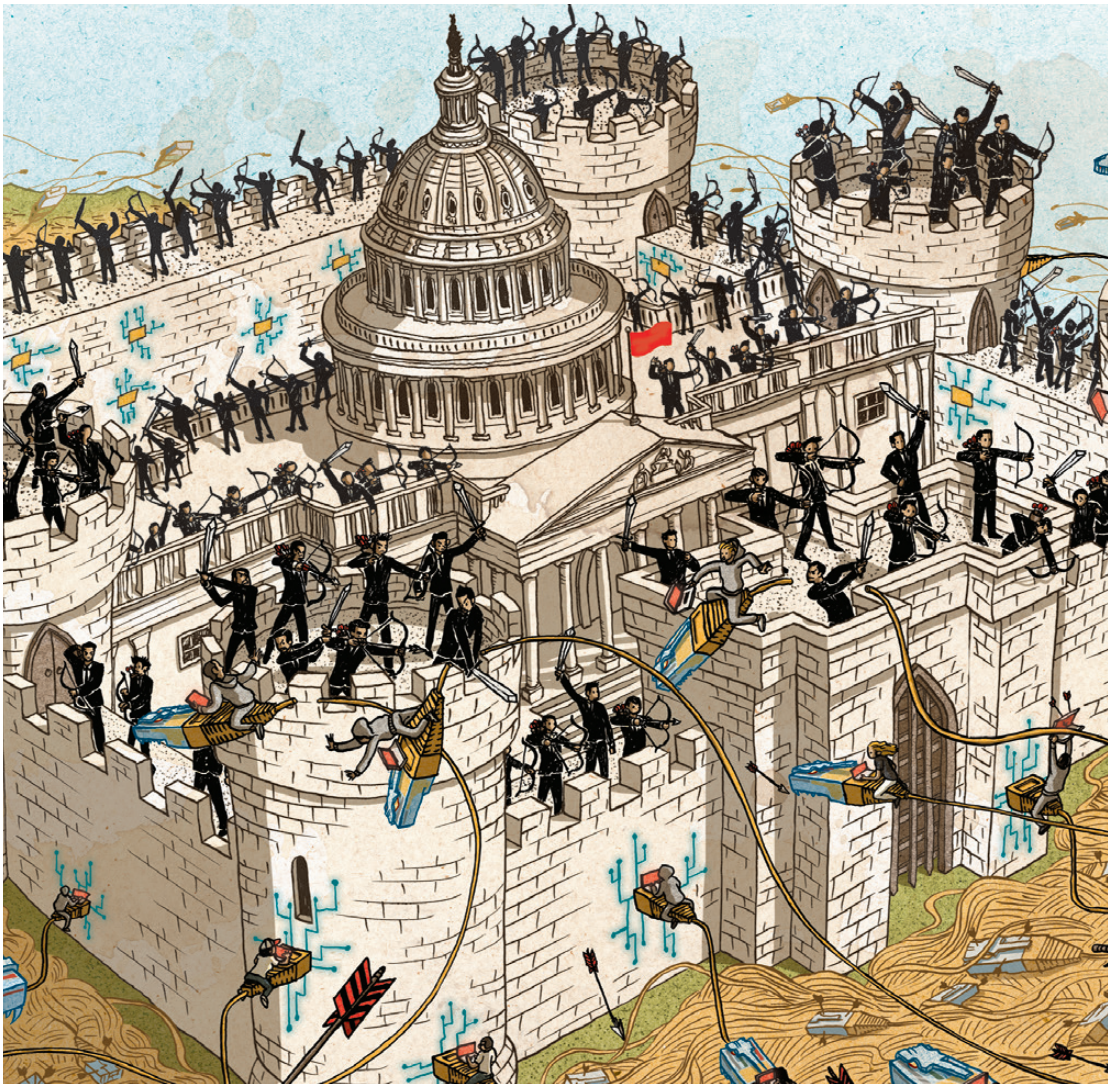
The public-sector challenges, however, run deeper. Government stores far more data than the private sector and often keeps it on older, more vulnerable systems. Agencies are regularly targeted not just by opportunistic hackers but by teams funded and trained by nation-states. And even as governments try to protect themselves against hostile intruders, employees and citizens alike want their data conveniently available anytime, anywhere.

Those with a vision of digital government transformation, then, are finding cybersecurity a major challenge.

GOVERNMENT: THE BIGGEST TARGET

"In the early days of criminal hacking, it was about showing what was possible—breaking into systems for fun and the challenge," explains security expert Marc Goodman and co-author Andrew Hessel. "[But] later, a profit motive emerged, which attracted criminal elements that were serious, organised, and global. As a result, the United States now classifies cyberspace as a new domain of battle—as significant as air, land, or sea."[3]

It's not hard to see why. For every Ashley Madison, we see at least one headline about



In 2013, the energy company BP said it experienced about 50,000 daily attempts at cyber intrusion, but that would represent a holiday at the Pentagon and National Nuclear Security Administration, which each sees *200 times* as many online attacks. States are big targets, too.

hackers breaching a government server. Frankly, it's surprising there aren't more. In 2013, the energy company BP said it experienced about 50,000 daily attempts at cyber intrusion, but that would represent a holiday at the Pentagon and National Nuclear Security Administration, which each sees *200 times* as many online attacks. States are big targets, too.[4] All in all, the public sector faces more security incidents and data breaches than any other sector.[5]

In short, government cybersecurity presents a unique problem simply due to the huge volume of threats that agencies face on a daily basis—and the scale of the potential consequences if the threats aren't foiled.

Consider the 2014 breach at the US Office of Personnel Management (OPM), in which personnel records and security-clearance files for at least 22 million people were compromised.[6] The information was extremely sensitive: Security applications are 127 pages long, containing everything from mental health history to criminal records, financial data, drug and alcohol use, assignment/work history, family member names, personal references, and fingerprints. With this kind of detail, officials have said, it's likely that foreign governments will try to use the data to identify US operatives, particularly those in intelligence roles.[7]

Experts rank this breach as one of the most damaging to date. "It is a very big deal from a national security perspective and from a counterintelligence perspective," says FBI director James B. Comey. "It's a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government."[8] Security veteran John Watters calls it "a huge national loss [that] will have ramifications for years to come."[9]

The OPM hack, and most cyber threats, look a lot like bank robberies: Attackers make a narrow, targeted intrusion to steal lots of data. Yet all-out assaults could be even worse than targeted strikes, and more immediately catastrophic. As security expert Stephen Herzog put it, "Sophisticated and virtually untraceable political 'hacktivists' may now possess the ability to disrupt or destroy government operations, banking transactions, city power grids, and even military weapon systems."[10]

Disruption on this scale has actually already happened. In 2007, Estonia found itself the target of a weeks-long cyberattack by Russian hackers angered by the removal of a famous Soviet statue from the capital. What began with sharp rhetoric and mild protests became a serious economic offensive when Russian Internet forums urged sympathetic hackers to act. Soon, the computer networks of Estonian banks, government agencies, and media outlets began failing. ATMs were knocked offline. It became so serious that the country had to "pull the plug," severing access to all Estonian websites from abroad.

"The episode has since been dubbed the world's first cyber war, or Cyber War I," Kertu

Ruus wrote the following year in the journal *European Affairs*, "because it was the first time that a sustained, wholesale, and politically motivated e-assault was launched to wreak havoc on a country's entire digital infrastructure."[11]

Of course, most government hacks are subtler, targeting state and city agencies, stealing Social Security numbers or tax returns. In South Carolina, for instance, sometime in late summer 2012, Eastern European hackers hit servers at the state's Department of Revenue, sucking up Social Security and credit card numbers in bulk. A state employee had fallen for a "phishing" email, which looks legitimate but harbors computer-breaching malware: The worker clicked on a link in the email that allowed the hackers to steal login and password information, opening the door to the revenue department's servers. By the time the state discovered and closed the breach on October 10, the hackers had vacuumed up 3.6 million Social Security numbers and 400,000 credit card numbers.[12]

In this case, the hacker's motive was clearly financial, since Social Security and credit card numbers can be sold on a network of illegal trading sites. The majority of today's cyberattacks fit this description—indeed, a recent RAND Corp. report found that in many ways, the market built around this type of heist has become more profitable than the illegal drug trade.[13] Increasingly, though, government agencies are also fending off attacks with clearly political aims.

Whatever the motive, it's clear that governments are the highest-value targets for hackers today. Thus, it's critical that agencies invest in strong cyber defenses—stronger, if anything, than those found in the private sector. At the state and local levels in particular, however, most agencies simply are devoting too little manpower and funding to the problem.

More than three-fourths of state chief information security officers say their states aren't spending enough on cybersecurity, and attracting and retaining the right talent continues to be difficult due to low government salaries, a lack of clear career paths, and convoluted hiring processes.[14] But it's also an issue of strategy—and of understanding the adversary.

TOOLS OF THE TRADE

HACKING wasn't always a criminal enterprise. In the early days, it was all about having fun and impressing your peers. Apple co-founders Steve Wozniak and Steve Jobs were early hackers, "phone phreakers" who learned to manipulate telephone systems and trick the phone company into giving out free long-distance calls. For Jobs, hacking was very much about the sense of adventure: "It was the magic of the fact that two teenagers could build this box for $100 worth of parts and control hundreds of billions of dollars of infrastructure in the entire telephone network of the whole world."[15]

Whatever the motive, it's clear that governments are the highest-value targets for hackers today. Thus, it's critical that agencies invest in strong cyber defenses—stronger, if anything, than those found in the private sector.

Today, ego triumphs have largely been replaced by the lure of profit, in the form of stolen data—and the cash you can make with it.

Unsurprisingly, the opportunity attracts organized crime. Marc Goodman, author of *Future Crimes*, one of the most detailed accounts of the massive cybercrime marketplace, writes, "Organized crime groups around the world have created a vast and highly efficient underground economy in which the stolen data is exploited by networks of geographically disparate crime syndicates."[16] And the losses have been catastrophic: Security firm McAfee estimates the global cost to companies and consumers at between $375 billion and $500 billion annually.[17] At the heart of this underground economy are black markets, bazaars where any kind of digital thievery can be commissioned. When a syndicate wants a hack, it can outsource for capabilities it lacks, or simply contract for the whole job.

These markets live on the so-called Dark Web—the Internet's Wild West, which can't be accessed with traditional browsers or search engines. RAND's National Security Research Division recently studied these markets and found exponential growth in the past 10 to 15 years: "Almost any computer-literate person can enter the market. With the increase of as-a-service models and do-it-yourself kits (with easy-to-use administration panels), anyone can deploy variants of malware. One can buy credentials, credit cards, and personally identifiable information (PII) without needing to be highly technical. These technologies have massively lowered the barriers to entry, leading to marketplaces with up to 80,000 members and global revenues in the hundreds of millions of dollars."[18]

Incredibly, Goodman notes, hackers can even learn how to launch phishing and spamming campaigns through massive open online courses specifically tailored to the criminal class. "Hackers are not born," he says. "They are trained, supported, and self-taught by an enormous amount of free educational material in the digital underground."[19]

The boom in hacking has led to skyrocketing sales for hacking tools, like the sales of picks and shovels during a gold rush. And, as in the gold rush, there may be as much money to be made in creating hacking tools as in the actual thefts. In 2006, RAND found only one new "exploit kit"—a toolbox for finding security

flaws and introducing malware—entering the market. By 2013, *33* new tools for distributing and managing attacks had emerged, indicating that companies and agencies face not only a rising number of attacks but an increasing *variety* of them. Goodman says many of the organizations offering these tools have become so sophisticated that they use customer relationship management to track customer requests and build brand loyalty among their criminal clients.[20]

Indeed, he says, the future looks bright for hackers: "Imminent fundamental shifts in computing, including the emergence of ubiquitous computing and the 'Internet of Things,' will yet again exponentially drive growth in big data. As companies gather more and more data from more and more devices . . . criminals will have an ever-expanding pool of targets from which to choose."[21]

This raises key questions about how governments should handle cybersecurity. It's increasingly clear that total cybersecurity is impossible: Every gigabyte you store is a gigabyte at risk. Knowing this, is preserving more and more data really a good idea? Do the potential costs outweigh the benefits?

ADDRESSING THE CYBERSECURITY CHALLENGE

THREATS are growing in volume, intensity, and sophistication, and they aren't going away—ever. And recent failures call into question the effectiveness of the billions already sunk into cybersecurity.

How can government agencies reverse the growing gap between security investment and effectiveness? Traditionally, cybersecurity has focused on preventing intrusions, defending firewalls, monitoring ports, and the like. The evolving threat landscape, however, calls for a more dynamic approach.

New thinking in this arena involves three fundamental capabilities built around being secure, vigilant, and resilient.[22] These three principles reflect the fact that defense mechanisms must evolve. Government agencies can't rely on perimeter security alone—they should also build strong capabilities for detection, response, reconnaissance, and recovery. The SANS Institute, which performs security training and research, codifies this as a guiding principle: "Prevention is ideal, but detection is a must."[23] And given Estonia's experience after removing the Soviet statue, you can see why effective recovery plans are important.

Furthermore, officials must relinquish a zero-tolerance mindset—they should accept risk while trying to minimize it as much as possible, especially for top-priority information. As Ed Powers writes in the *WSJ Risk & Compliance Journal*: "The reality is that cyber risk is not something that can be avoided; instead, it must be managed. By understanding what data is most important, management can then determine what investments in security

controls might be needed to protect those critical assets."[24]

SECURE: LOCKING THE DOORS

GOVERNMENT agencies need to examine and understand all aspects of their operations in cyberspace, and the first step is simple: They need to *lock the doors*. But you can't be sure all your doors are closed if you can't find them. "Most agencies don't even know what IT systems they have," says SANS Institute founder Alan Paller.[25] Similarly, agencies must review their data to determine levels of sensitivity. Public information such as school bus schedules should be stored differently than medical histories. Biometric records, even more sensitive, deserve the highest tier of protection.

Closing doors also means taking simple steps such as two-factor authentication (typically, a card and a password or ID number) and encryption for sensitive data. For extremely sensitive information such as the OPM data, John Watters says, "you have that data decentralized, much of it offline with very tight controls and accesses." Forget convenience and focus on security: "You take those databases offline. Make them hard to access. You place air gaps between them."[26]

One problem is that managers often don't understand how cybersecurity works. A bank's CEO may know how trades and transactions function from the teller's window on up, but few leaders and managers have any background in software code or detailed understanding of cyber issues. The problem is even more acute in the general workforce. Even when an agency's IT staff does an admirable job in closing all the doors, employees may keep opening them back up, inadvertently—or intentionally.

When considering the *insider threat* risk, many may first think of Edward Snowden deliberately leaking classified information from the US National Security Agency. Yet while disgruntled employees are a serious threat to government, so too are those who breach security through ignorance or complacency.[27] The systems administrator who plays Minecraft in a secure environment and clicks on a purported link for the latest update—which is actually malware—has just let the bad guys into the agency's systems. The consequence is equally devastating, whether intentional or not.

Fortunately, the advent of big data and sophisticated analytics gives governments ways to counteract the insider threat. Today's tools can detect anomalous employee actions that deviate from peer-group practices or their own previous behavior. Such behavioral analytics allow agencies to flag suspicious emails and badge check-ins, downloads, and access to unauthorized sites and assets.

Whether it's an inside or external threat, organizations are finding that building firewalls is less effective than anticipating the nature of threats—studying malware in the wild, before it exploits a vulnerability. The evolving

The language of digital crime and espionage is certainly colorful—"phishing," "pharming," "war dialing," "smurf attacks," and "the ping of death"; "zombie systems," "botnets," "rootkits," and "Trojans." But if the language is playful, the consequences of a cyberattack can be devastating.

nature of cyber threats calls for a collaborative, networked defense, which means sharing information about vulnerabilities, threats, and remedies among a community of governments, companies, and security vendors. Promoting this kind of exchange between the public and private sectors was a key aim of the US Cyber Security Act of 2012.[28]

Australia has taken a significant lead in working across government and the private sector to shore up collective defenses. The Australian Cyber Security Centre (ACSC) plays many roles, raising awareness of cybersecurity, reporting on the nature and extent of cyber threats, encouraging reporting of incidents, analyzing and investigating specific threats, coordinating national security operations, and heading up the Australian government's response to hacking incidents. At its core, it's a hub for information exchange: Private companies, state and territorial governments, and international partners all share discoveries at the ACSC.[29]

The Australian approach begins with good network hygiene: blocking unknown executable files, automatically installing software updates and security patches on all computers, and restricting administrative privileges.[30] The program then aims to assess adversaries, combining threat data from multiple entities to strengthen collective intelligence. The system uploads results of intrusion attempts to the cloud, giving analysts from multiple agencies a larger pool of attack data to scan for patterns.

Cybersecurity experts have long valued collective intelligence, perhaps first during the 2001 fight against the Lion worm, which exploited a vulnerability in computer connections.[31] A few analysts noticed a spike in probes to port 53, which supports the Domain Name Service, the system for naming computers and network servers organized around domains. They warned international colleagues, who collaborated on a response. Soon, a system administrator in the Netherlands collected a sample of the worm, which allowed other experts to examine it in a protected testing environment, a "sandbox." A global community of security practitioners then identified the worm's mechanism and built a program to detect infections. Within 14 hours, they had publicized their findings widely enough to defend computers worldwide.

A third core security principle is to rethink network security. All too often, leaders think of it as a wall. But a Great Wall can be scaled—a Maginot Line can be avoided. Fixed obstacles are fixed targets, and that's not optimal cyber defense. Think of cybersecurity like a chess match: Governments need to deploy their advantages and strengths against their opponents' disadvantages and weaknesses.

Perpetual unpredictability is the best defense. Keep moving. Keep changing. No sitting; no stopping. Plant fake information. Deploy "honeypots" (decoy servers or systems). Move data around. If criminals get in, flood them with bad information. The goal is to modify the defenses so fast that hackers waste money and time probing systems that have already changed. Savvy cybersecurity pros understand this: The more you change the game, the more your opponents' costs go up, and the more your costs go down. Maybe they'll move on to an easier target.

"Most people want to build [a defense] and let it sit for two years," says Deloitte colleague Craig Astrich, but that doesn't work: "This is a constant evolution." Agencies need to learn to love continuous change. As Astrich says, "I'm putting myself out of my job as fast as I can every day."[32] New problems will arise. There'll always be work.

VIGILANT: UNDERSTANDING THE THREAT

THE language of digital crime and espionage is certainly colorful—"phishing," "pharming," "war dialing," "smurf attacks," and "the ping of death"; "zombie systems," "botnets," "rootkits," and "Trojans." But if the language is playful, the consequences of a cyberattack can be devastating.

The public sector's difficulties in defending against these attacks are well known. But a new generation of warriors is going on the offense by investigating the tactics and targets of cyber-criminals, infiltrating the Dark Web in an aggressive effort to anticipate, neutralize, and disrupt hackers—or at least offer their targets a warning.

"The fundamental problem is: How do you find signals in the noise, and figure out which one of those alerts created the biggest risk for your enterprise?" John Watters says.[33] The answer, say Watters and other cyber experts, is deep intelligence on hacker networks, from malware vendors to stolen credit card buyers. By understanding their methods, the thinking goes, governments can better anticipate and recognize future risks, thwarting hacks before they start.

This goes well beyond simply probing systems for vulnerabilities. It means understanding which data are the most desirable to the bad guys, which cyber criminals would be most interested in their data, and which hacks they're most likely to use to infiltrate systems.

As with modern-day terrorism, cybersecurity has proven daunting because the nature of the threat is constantly evolving. Each major technological development—mobile, social, cloud computing—brings a host of new risks.

Agencies should make significant efforts to study emerging threats, looking at key risk indicators and understanding the actors—criminals, foreign countries, and hacktivists—who threaten government systems.

As with modern-day terrorism, cybersecurity has proven daunting because the nature of the threat is constantly evolving. Each major technological development—mobile, social, cloud computing—brings a host of new risks. And typically, in the early stages, innovators focus less on security than on creating a minimum viable product. Cybercriminals, on the other hand, aim to exploit new technologies before developers discover their vulnerabilities. Consider Internet of Things technology, whose chief strength—generating fresh data via connected devices—is also its chief vulnerability.[34]

FCC CIO David Bray, drawing on his experience preparing for bioterrorism at the US Centers for Disease Control and Prevention (CDC), suggests that public health can provide a model for cybersecurity. "Consider approaching cybersecurity differently—focusing instead on cyber resiliency and an approach more akin to 'cyber public health' aimed at both preventive measures and rapid detection, containment, and mitigation of cyber threats akin to infectious disease control," he writes in a blog post. Just as anonymized and aggregated health data help public health agencies understand and fight disease outbreaks, Bray believes a "cyber CDC" could "protect privacy

and improve resiliency by anonymously sharing the equivalent of cyber signs, symptoms, and behaviors that different [IoT] devices are experiencing."[35]

RESILIENT: BOUNCING BACK

DOCTORS say, rightly, that prevention is better than cure. But what if, despite vaccines, you get the flu? That's when your body's resilience kicks in, fighting the infection and restoring your health. Bodies generally have a zero-tolerance policy toward pathogens, accelerating blood flow and increasing body temperature to create an inhospitable environment for them. The identity, source, and intent of the threat are irrelevant—the focus is on isolating and attacking it.

Similarly, an organization's resilience to cyberattack—the ability to contain damage and mobilize diverse resources to minimize its impact—can be what saves it when disaster strikes. How and how quickly an organization can detect and then quarantine intrusion can determine the extent to which it can minimize further damage, neutralize threats, and recover.

Organizations shouldn't have to suffer a real crisis to learn they're unequipped to cope with one. That's where cyber wargaming comes in: It immerses participants in simulated cyberattack scenarios, such as a data breach, website defacement, denial-of-service attack, or sophisticated malware on a network. Although infinitely more sophisticated and complex, a war game serves the same purpose as a fire drill, gauging the organization's speed and readiness and giving employees a chance to practice their responses.[36] It also helps earn executive buy-in for cyber risk programs by elevating their importance in the minds of department leaders.

So how does a cyber war game work? It begins with an elaborate scenario. A group of executives is assigned to play the role of a response team for a fictional organization, such as a global pharmaceutical giant or a public agency. The executives are presented with a mock attack on their systems and asked to develop a response-and-recovery plan. To do this, they'll have to answer a variety of questions: How did the intruders get in? What's the extent of damage? How can the breach be contained? How can damage to reputation be minimized?

To complicate matters further, the responders must cope with a continuing flow of new information that may not always be accurate. They need to manage and communicate with stakeholders—clients, a board of directors, business partners, the media, and staff—while racing against the clock.[37] As the war game unfolds, critical insights and lessons come to light.

Overall, such an exercise can help all parties involved appreciate the importance of discipline and agility.[38] Resilience isn't built overnight; it takes practice. Wargaming is a safe way to establish the "muscle memory" and coordination needed to manage a potential crisis.[39]

A resilient organization does a few specific things: It minimizes access rights so that, in

the event of a breach, only a small amount of information can be leaked. It encrypts and anonymizes data to restrict its availability and usefulness. It continually scans for breaches so that it can identify leaks as soon as possible.

But resilience is also about rebuilding trust. Utah Governor Gary Herbert immediately accepted responsibility in 2012 when his state's IT department exposed about 780,000 personal medical records, including some Social Security information. His immediate *mea culpa* overstated the damage but restored citizen confidence.[40]

Rebuilding trust requires concrete steps as well. South Carolina's Department of Revenue hack ultimately led to better security. A few high-profile firings and new standards helped to spark a cultural shift along with dual-protected passwords for all the state's computers; today, a new division of information security helps manage security across all government departments.

CLOSING THE CYBER SKILLS GAP

A CYBERSECURITY strategy means nothing without the skills and talent needed to execute it. Technology companies and banks with world-class cybersecurity capabilities owe much of their success to top-flight technical staff. While the defense and intelligence sectors generally can attract high-caliber talent, other federal, state, and local agencies find it difficult to compete with the private sector. In fact, experts consistently cite a talent shortage as one of the key challenges to better public cybersecurity.[41]

Agencies counting on digital-native Millennials to save the day should think again. A 2014 Raytheon survey found few Americans between ages 18 and 26 inclined toward cybersecurity work.[42] Governments, therefore, must cast a wider net for cybersecurity professionals. One interesting approach is that of the University of South Florida's Florida Center for Cybersecurity, whose 36-week program is designed to train students for lucrative jobs in cybersecurity. With classes slated to begin in spring 2016, the first graduates can't come soon enough; experts say employers offering more than 200,000 cybersecurity jobs nationwide are competing for only 4,000 to 5,000 qualified candidates.[43]

The US Cyber Challenge (USCC) offers another promising model for boosting the supply of cybersecurity professionals. Led by former federal CIO Karen Evans, the organization aims to recruit and place the next generation of cybersecurity professionals.[44]

Experts agree that cybersecurity requires different skill sets than other IT work—in particular, a talent for understanding systems and getting into adversaries' heads. The talent search has been likened to trying to find the rare child who prefers to dismantle toys rather than play with them. It's a different headspace than an engineer's instinct to fix problems. You have to anticipate vulnerabilities: "You have a working system, and you need to figure out how it's

going to be perturbed and broken," Allan Paller says. That's one reason why the Defense Intelligence Agency is recruiting liberal arts students who show aptitude at sleuthing out the motives and means of malicious hackers.[45]

CONCLUSION: MANAGING CYBER RISK

THE Internet is a new environment with its own rules and its own dangers. In the past two decades, we've connected our economy and society via the Internet—a platform designed primarily for sharing information, not protecting it. This connectivity has driven innovation and high performance in the public and private sectors alike.

Yet as connectivity reshapes government in positive ways, it presents business opportunities for criminals with cyber talents. As agencies extend their capabilities through cloud computing, IT outsourcing, and partnerships, they increasingly rely on complex infrastructure not fully within their control. Similarly, government efforts to engage citizens and employees through social media introduce gaps and opportunities attackers will doubtless try to exploit.

In short, digital strategies inevitably introduce new risks. Yet when one considers the inherent link between performance, innovation, and risk, it becomes clear that overly tight controls could impede important strategic initiatives.

The only way forward, then, is to accept that some break-ins will occur. Living with risk is the new normal, and managing it is an essential part of achieving optimal performance in digital government.

This challenge for governments resembles that facing military strategists as their primary roles shift from war against established nations to continual skirmishes against elusive, unpredictable non-state actors. Your government will inevitably lose some cybersecurity skirmishes, but that doesn't mean it's failed. It's a given that not every encounter will end in victory.

The important test lies in how government officials anticipate and counter moves by an ever-shifting cast of criminal adversaries. Digital governments will need speed, dexterity, and adaptability to succeed on this new battlefield. DR

***William D. Eggers**, a director with Deloitte Services LP, leads research and thought leadership for Deloitte's public sector industry practice. He is the author of nine books, including his latest,* Delivering on Digital: The Innovators and Technologies That Are Transforming Government.

Endnotes

1. Brian Krebs, "Was Ashley Madison database leaked?" *Krebs on Security*, August 15, 2015, http://krebsonsecurity.com/2015/08/was-the-ashley-madison-database-leaked/.
2. John Herrman, "Early notes on the Ashley Madison hack," *Awl*, August 18, 2015, www.theawl.com/2015/08/notes-on-the-ashley-madison-hack.
3. Marc Goodman and Andrew Hessel, "The bio-crime prophecy: DNA hacking the biggest opportunity since cyber attacks," *Wired*, May 28, 2013, www.wired.co.uk/magazine/archive/2013/06/feature-bio-crime/the-bio-crime-prophecy.
4. Michigan alone says it averages about 120,000 daily attempts, on par with the entire government of the United Kingdom. See: Brian Fung, "How many cyberattacks hit the United States last year?" *Nextgov*, March 8, 2013, www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.
5. "2015 Data breach investigations report," Verizon, 2015. www.verizonenterprise.com/DBIR/2015/.
6. Sean Lyngaas, "Exclusive: The OPM breach details you haven't seen," *FCW*, August 21, 2015, https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx.
7. Ellen Nakashima and Adam Goldman, "CIA pulled officers from Beijing after breach of federal personnel records," *Washington Post*, September 29, 2015, www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html.
8. Ellen Nakashima, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," *Washington Post*, July 9, 2015, www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
9. Interview with John Watters, October 19, 2015.
10. Stephen Herzog, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security*, 2011, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.
11. Kertu Ruus, "Cyber War I: Estonia attacked from Russia," European Institute, 2008, www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia.
12. David Slade, "South Carolina: 'The mother of all data breaches'," *The Post and Courier*, November 3, 2012, http://www.postandcourier.com/article/20121103/PC16/121109713.
13. Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for cybercrime tools and stolen data: Hackers' Bazaar,* RAND Corporation, 2014, www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
14. Deloitte, *2014 Deloitte-NASCIO cybersecurity study: State governments at risk—time to move forward*, October 27, 2015, p. 18, www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-state-nascio-cybersecuritysurvey_102714.pdf.
15. Geeta Dayal, "Before Steve Jobs and Steve Wozniak invented Apple, they hacked phones," *Slate*, February 1, 2013, www.slate.com/articles/technology/books/2013/02/steve_jobs_and_phone_hacking_exploding_the_phone_by_phil_lapsley_reviewed.2.html.
16. Marc Goodman, "Criminals deftly exploit the data deluge," May 17, 2011, www.marcgoodman.net/2011/09/15/the-economist-online-the-hackers-enterprise/.
17. Tom Risen, "Study: Hackers cost more than $445 billion annually," *US News & World Report*, June 9, 2014, www.usnews.com/news/articles/2014/06/09/study-hackers-cost-more-than-445-billion-annually.
18. Ablon, Libicki, and Golay, *Markets for cybercrime tools and stolen data*, p. 4.
19. Marc Goodman, *Future Crimes: Everything is Connected, Everyone Is Vulnerable, and What Can We Do About It* (New York: Doubleday, 2015), p. 185.
20. Ibid., p. 183.
21. Goodman, "Criminals deftly exploit the data deluge."
22. Deloitte Cyber Risk Services, *Changing the game on cyber risk: The imperative to be secure, vigilant, and resilient*, 2014, www2.deloitte.com/us/en/pages/risk/articles/cyber-risk-services-change-game.html; also see Deloitte Center for Financial Services, *Transforming cybersecurity: New approaches for an evolving threat landscape*, 2014, pp. 6–7, www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/dttl-fsi-TransformingCybersecurity-2014-02.pdf.
23. SANS Institute, "CIS critical security controls: Guidelines," www.sans.org/critical-security-controls/guidelines, accessed December 17, 2015.

24. Ed Powers and Mary Galligan, "The pursuit of cybersecurity," *Risk and Compliance Journal*, July 27, 2015, http://deloitte.wsj.com/riskandcompliance/2015/07/27/the-pursuit-of-cybersecurity/.

25. Interview with Alan Paller, October 6, 2015.

26. Interview with John Watters, October 19, 2015

27. Kristina Torres, "Data breach in Georgia could affect 6 million voters," *Atlanta Journal-Constitution*, November 18, 2015, www.myajc.com/news/news/state-regional-govt-politics/data-breach-in-georgia-could-affect-6-million-vote/npQj8/.

28. Vikram Mahidhar, David Schatsky, and Kelly Bissell, *Cyber crime fighting*, Deloitte University Press, June 27, 2013, http://dupress.com/articles/cyber-crime-fighting/.

29. Australian Signals Directorate, "ACSC—Australian Cyber Security Center," www.asd.gov.au/infosec/acsc.htm, accessed December 17, 2015.

30. Australian Signals Directorate, "Top 4 strategies to mitigate targeted cyber intrusions: Mandatory requirement explained," July 2013, www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm.

31. Internet Storm Center, "ISC history and overview," https://isc.sans.edu/about.html, accessed December 17, 2015.

32. Interview with Craig Astrich, October 9, 2015.

33. Interview with John Watters, October 19, 2015

34. Irfan Saif, Sean Peasley, and Arun Perinkolam, "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age," *Deloitte Review* 17, July 27, 2015, http://dupress.com/articles/internet-of-things-data-security-and-privacy/.

35. David A. Bray, "Democracies and Internet of Everything," *Leadership + Knowledge*, February 26, 2015, http://blog.dbray.org/2015/02/democracies-and-internet-of-everything.html?view=classic.

36. Joab Jackson, "In a mock cyberattack, Deloitte teaches business how to respond," *Computer World*, April 8, 2015, www.computerworld.com/article/2907918/in-a-mock-cyberattack-deloitte-teaches-business-how-to-respond.html.

37. Ibid.

38. Sara Peters, "Cyber war games: Top 3 lessons learned about incident response," *DarkReading*, April 7, 2015, www.darkreading.com/risk/cyber-war-games-top-3-lessons-learned-about-incident-response/d/d-id/1319813.

39. Deloitte, *Prepare for the unexpected: Cyber threat war-gaming can help decrease the business impact of cyber incidents*, 2014, www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-cyber-war-gaming-sales-sheet-07272014.pdf.

40. Brian T. Horowitz, "Utah health care data breach exposed about 780,000 patient files," eWeek, April 13, 2012, www.eweek.com/c/a/Health-Care-IT/Utah-Health-Care-Data-Breach-Exposed-About-780000-Patient-Files-189084.

41. See, for instance, Deloitte, *2014 Deloitte-NASCIO cybersecurity study*, http://www2.deloitte.com/us/en/pages/public-sector/articles/2014-deloitte-nascio-cybersecurity-study.html

42. Raytheon, *Securing our future: Closing the cybersecurity talent gap*, October 2015, p. 2, www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_278208.pdf.

43. Sarah Hegen, "New USF center focuses on cybersecurity," *WTSP 10 News*, February 6, 2015, www.wtsp.com/story/news/local/2015/02/06/sarah-hagen-10-news-cyber-security/22991529/.

44. Interview with Karen Evans, August 20, 2015. USCC's competitions are designed to identify the nation's most promising candidates for a variety of information security disciplines. Its 2015 competition, for example, emphasized secure coding. "By developing and implementing our competitions and programs, USCC is drawing talent out of the shadows and giving them platforms to build upon their skill sets, connect with others in the field, and find careers that put their capabilities to work while defending our nation," Evans says.

45. Mohana Ravindranath, "No STEM training? You can still be a defense cyber intel analyst," *Nextgov*, October 30, 2015, www.nextgov.com/cio-briefing/wired-workplace/2015/10/officer-liberal-arts-majors-can-still-do-cyber-intel-dia/123263/?oref=ng-article-recommended.