ICF QUICK TAKE

Why the Government Keeps Getting Hacked

By Jeffrey Neal, Senior Vice President, ICF International

The Culture of Cyber Insecurity

Data breaches at the U.S. Office of Personnel Management (OPM), Target, and Sony have gotten everyone's attention on cybersecurity and the challenge of securing personally identifiable information. Federal agencies are reviewing systems, and their leaders are making promises about securing employee data. The White House, U.S. Department of Defense, OPM, and Federal Bureau of Investigation are investigating the OPM breach. The U.S. Congress is holding hearings. Requests for money for better technology can be expected. All good, right?

Not necessarily. The OPM breach exemplifies the cultural problem that besets the cybersecurity of both the government and private sectors—the failure to recognize that cybersecurity is a challenge that must be owned by the entire enterprise. Key executives and departments—including CIO, CISO, CFO, COO, communications, and human resources—must be part of the plans and programs necessary for effective cybersecurity.

Today's massive cybersecurity challenge requires the best tools and talent. In a recent white paper called, "Addressing the Whole-of-Enterprise Threat," ICF Senior Vice President Samuel Visner makes this point: Effective cybersecurity requires programs that are end-to-end (from plans through incident response) and involve the entirety of an enterprise. It focuses on the need for a holistic approach.

At the same time we are using the best available security tools, we also must address the issues of culture that contribute to vulnerabilities. Otherwise, the technology cannot protect us. The current culture reduces cybersecurity to "merely" a technical challenge. Let's take a look at a few examples:

Shut it down! Oh…not so fast.

When a system that manages and processes sensitive data has glaring security deficiencies, the first reaction may be to shut it down until the problems can be fixed. OPM's Inspector General made just such a recommendation in his November 2014 Federal Information Security Management Act Audit: "We recommend that the OPM Director consider shutting down information systems that do not have a current and valid authorization."

The threat of shutting down a system is one way to protect vital data and force program managers to address security issues. So what happened when OPM temporarily shut down the e-QIP system because of security flaws? Senators Mark R. Warner (D-VA) and Timothy M. Kaine (D-VA) immediately responded with legitimate concern about the effect of the shutdown on security clearance processing. The Professional Services Council, writing on behalf of the contractor community, asked OPM to clarify how it would mitigate the effects of its decision. Both OPM's decision to temporarily shut down the system and the questions about the impact of that decision were equally sound. OPM would be criticized no matter which decision the agency made. Shutting down critical systems is an extreme risk mitigation action that is not always practical. It can indicate that a flawed tool, sloppy development, or inadequate program management allowed a product to get to the point where it needed to be shut down.

It's mine. Keep your hands off.

Many agencies decentralize control of IT and allow program offices to manage the technology that supports their program, rather than having a team of experts who understand technology and a fully engaged leadership team that knows what information must be protected. They are focused on driving their program rather than what is going on under the hood. The desire to control every aspect of a program is common, based partly upon fear that someone else will not do the work as well and partly on the purely parochial interests of power and control. The harm that parochial culture can cause grows as our systems become more complex and more interconnected. In fact, correcting that cultural flaw is one of the primary objectives of the Federal Information Technology Acquisition Reform Act (FITARA). FITARA will give department chief information officers much greater control over such programs. The result should be a focus on security throughout the acquisition, development, and deployment processes.

Here. You take care of it.

The flip side of the control culture is the "fire and forget" culture that assumes senior leaders do not need to stay engaged in system development, acquisition, deployment, and operations. Agency leaders often identify a need for a new system, pick a program manager, and then disengage. When senior leaders do not remain engaged with big projects, budgets can get out of control, scope expands to undeliverable levels, and the projects can go off the rails and fail. The same applies to the security aspects of systems. Rather than being an integral part of the project, security can be an afterthought that mission-focused program managers do not address throughout the project.

Security is the CIO's job. Or the security officer's.

Anyone but me. The OPM breach may change the culture of "It's not my job" when it comes to security. The lock on the door is irrelevant if users of a system fail to close the door. For example, agencies are mandating use of smart cards and a personal identification number (PIN). But what happens when someone cannot remember the PIN? Too often, the PIN is written on a sticky note or piece of tape on the card. Just one card with a PIN written on the back can give an intruder access to a system. The problem is even worse for agencies that still have user IDs and passwords. How many people have passwords "hidden" under a desk pad, keyboard, or in a drawer where, of course, no one will ever find them? And how many people are disciplined for that offense? I have never seen an employee disciplined for blowing a hole in the agency's security efforts. We have to start holding everyone accountable for behavior that weakens security. Doing so is harder than it might seem, because (a) the offenses are not considered to be serious and (b) the culture of Washington, DC, is to find someone senior to blame and fire that person. Firing someone may make everyone feel better for a few days but does nothing to change the cultural problems that get us into these messes.

> *"What amazes me when I look into a lot of intrusions, including some really big ones by multiple different types of actors, it often starts with the most basic active spear-phishing, where somebody is allowed in the gate and penetrates a network simply because an employee clicked on something he or she shouldn't have."*
>
> *—U.S. Department of Homeland Security Secretary Jeh Johnson*

icfi.com

Any views or opinions expressed in this quick take are solely those of the author(s) and do not necessarily represent those of ICF International. This quick take is provided for informational purposes only and the contents are subject to change without notice. No contractual obligations are formed directly or indirectly by this document. ICF MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

About ICF International

ICF International (NASDAQ:ICFI) provides professional services and technology solutions that deliver beneficial impact in areas critical to the world's future. ICF is fluent in the language of change, whether driven by markets, technology, or policy. Since 1969, we have combined a passion for our work with deep industry expertise to tackle our clients' most important challenges. We partner with clients around the globe—advising, executing, innovating—to help them define and achieve success. Our more than 5,000 employees serve government and commercial clients from more than 70 offices worldwide. ICF's website is www.icfi.com.

No technologist can solve this problem—everyone in an enterprise must own it. Holding employees accountable is much harder when agencies invest so little time in training them. From inadequate annual refresher training to placing people in roles for which they have inadequate training, agencies are not providing their employees with the skills they need to do their parts. Given the potential harm that breaches can cause, more in-depth training, tailored to the employee's role, is critical.

Conclusion

Cybersecurity involves the entire workforce and every aspect of an enterprise's organization. Technologists must install and manage effective cybersecurity technologies—operators just judge the operational risks they can accept. Financial managers must decide what financial consequences they are prepared to accept and make the sustained cybersecurity investment necessary to mitigate those consequences. Human resources and training professionals must help build a workforce (and workforce awareness) to face the cybersecurity challenge head on. This holistic approach to designing, building, implementing, and managing an effective cybersecurity program represents the real shift the public and private sectors must make.

About the Author

Jeffrey Neal is a senior vice president at ICF International. In his career in the Federal Government, he also served as director of human resources for the Defense Logistics Agency. He writes about management and human capital issues in the Federal Government on his blog, ChiefHRO.com.

For more information on cybersecurity contact:
Samuel Visner | samuel.visner@icfi.com | +1.703.225.5860

icfi.com/cyber