In 2013, insider threat was given a face: former National Security Agency (NSA) contractor Edward Snowden, who, before fleeing to Russia, leaked a still unknown number of highly classified documents detailing the U.S. intelligence community’s surveillance tactics. For his actions, he was charged with espionage, accused of severely jeopardizing national security, and named Time magazine’s second most influential person, for good or bad, of 2013—ensuring that 2013 will be remembered as the year of the insider threat.

Organizations no longer wonder if they will experience a breach, but when. Since insider threat can come from anyone inside the organization’s boundaries—including full-time employees, contractors, business partners, and even advanced persistent threats that have infiltrated the network—a comprehensive strategy is needed.

In October 2011, President Obama issued Executive Order 13587, requiring “structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks” as well as the creation of an Insider Threat Task Force led by the Federal Bureau of Investigation and Office of the Director of National Intelligence. Funding for implementing EO 13587 was initially delayed, but data loss prevention is now beginning to pick up—growing from a $300 million industry in 2010 to an estimated $670 million in 2013.

In many ways, the lesson of 2013 is that data loss prevention is something organizations can’t afford not to do—particularly governmental organizations. 2013 saw a 22 percent increase in data breaches over the previous year—exposing 17.3 million documents and costing IT leaders across the country an estimated $585,892. According to the Ponemon Institute, more than one-third (37 percent) of the year’s breaches were the result of malicious attacks, including criminal insiders. While hackers and malevolent outsiders still make up the vast majority of data breaches, insider threats are on the rise. They have grown by more than 10 percent year/year.

In addition to financial costs, the growth of insider threats poses significant reputational risks to government organizations. For example, following the leaks surrounding NSA surveillance tactics, the U.S. government’s global reputation suffered—even among its staunchest allies. In Germany, approval of the U.S. government fell to 35 percent, a 14 percent drop from the previous year when about half of all Germans viewed America as a partner they could trust.
Winning the Battle Against Insider Threats

In the effort to prevent and mitigate data breaches, federal leaders need to leverage a vast tool kit. Doing effective background checks, having clear information handling policies and gaining visibility on the flow of data are all crucial components needed to combat the growth of insider threat.

While insider threats are inherently a people issue, technology plays an increasingly crucial role in identifying risky user behavior. Data loss prevention (DLP) solutions, which Gartner defines as technologies that “perform content inspection of data at rest or in motion, and can execute responses—ranging from simple notification to active blocking,” provide a variety of benefits to institutions looking to secure classified information.9 Leading content-aware DLP tools help IT leaders manage security risks in BYOD environments, gain visibility into encrypted data stored on servers with malicious intent, and identify potential high risk offenders within the organization by tracking abnormal usage and behaviors. In essence, DLP ensures that organizations know where their data is and how to stop it from going where it’s not supposed to go.

Carnegie Mellon’s Computer Emergency Readiness Team’s (CERT) Insider Threat Center, has recommended that agencies “use DLP tools and techniques to detect sensitive data being sent to cloud-based storage” and acknowledged that a “DLP program is needed to filter data and take appropriate actions” to halt data loss via email and USB devices.10

But if agencies know DLP is one of the key tools in mitigating insider threats, why aren’t more federal agencies using such systems? While implementation has been slow in many agencies, some are emerging as clear leaders. For example, the United States Postal Service (USPS) is “outpacing nearly every civilian agency” in leveraging identity systems and is “winning the battle against the insider threat.”11 USPS uses a system called eAccess with 220,000 of its employees, which requires users to request access to particular areas of the network through their managers. Managers then assess the request against Active Directory, a system that keeps actively updated user profiles to ensure proper access. By linking Active Directory to its HR Systems, USPS is able to suspend user access nearly instantaneously upon detection of suspicious activity, employee termination, or organizational changes within the agency.12

Other civilian agencies leveraging DLP tools to combat insider threats include the Department of the Interior, the State Department, and the Federal Aviation Administration.13 The defense and intelligence communities have also launched initiatives to improve identity management and adopt DLP tools, but lag behind many civilian agencies.

Implementing DLP is not something an agency can do overnight—it requires a slow, methodical approach that builds upon incremental successes. In the effort to combat insider threats, there is no magic bullet, but DLP systems will likely be among the first prongs in a multi-pronged approach adopted by agencies in the future.

About GBC
Government Business Council (GBC), the research arm of Government Executive Media Group, is dedicated to advancing the business of government through analysis and insight. GBC partners with industry to share best practices with top government decision-makers, understanding the deep value inherent in industry’s experience engaging and supporting federal agencies. For more information, please visit: www.govexec.com/gbc.

About Symantec
Symantec protects the world’s information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: www.symantec.com/socialmedia.
Sources
1. Time Magazine’s 2013 Person of the Year, Time.com
2. Executive Order 13587, Whitehouse.gov
3. Magic Quadrant for Content-Aware Data Loss Prevention, Gartner, p.1
4. ITRC, 2013 Breach List
5. Study: IT leaders count the cost of breaches, data loss and downtime, SC Magazine
6. 2013 Cost of a Data Breach Study, Ponemon Institute/Symantec
7. 2013 Data Breach Investigations Report, Verizon
8. U.S. popularity in Germany on a steep decline in wake of spy scandal, McClatchy
9. Magic Quadrant for Content-Aware Data Loss Prevention, Gartner, p.1
11. USPS fighting back against the insider threat, Jason Miller, Federalnewsradio.com
12. Ibid.
13. Information Sharing Environment Annual Report to Congress, ISE

Image: Flickr user – StockMonkeys.com