

DEFENDING FROM WITHIN: HOW INSIDERS THREATEN DATA PRIVACY

TO FULLY PROTECT DATA WITHIN THEIR BORDERS, AGENCIES WILL NEED TO SECURE THE DATA ITSELF, NOT JUST THEIR PERIMETERS, NETWORKS, AND APPLICATIONS

In September 2013, the names, Social Security numbers, and business addresses of 2,400 insurance agents were unintentionally made public by MNsure, the Minnesota health insurance exchange set up for the upcoming implementation of the Affordable Care Act,¹ when an employee emailed an unencrypted, unsecured report to the wrong party. Although the information was quickly secured and no damage was done, the lack of technology in place to ensure data privacy and security indicates a larger, more concerning trend.

In the age of increased information collection, analysis and storage, nearly all organizations struggle to respond to and prevent ever-increasing security breaches and cyber threats to their data. Personally identifiable information (PII) like the kind leaked by MNsure is not the only type of information that public sector agencies must safeguard. Protected health information (PHI), financial data, trade secrets, and national security assets must all be protected, but agencies are increasingly finding that firewalls, antivirus software, and other traditional security measures are not enough. To fully protect data within their borders, agencies will need to secure the data itself, not just their perimeters, networks, and applications.



The Real Danger of Insider Threat

Cyber threats originate from various sources, including hackers, terrorists, industrial spies and organized crime groups, foreign governments, hacktivists, and disgruntled or careless employees, among others.² For each of these actors, one or more vulnerabilities in technology, process, or human action create the opportunity for exploitation.³ Insider threat, defined as any action by current or former employees or contractors that exceeds or misuses an authorized level of access to networks, systems or data, is a growing concern that originates from all three of these vulnerabilities.

Though the highest-profile cases of insider threat are likely leaks like those of former CIA and NSA employee Edward Snowden or Private Manning of WikiLeaks infamy, not all insider threats are premeditated. Many cases involve employees who unintentionally disclose sensitive information.

“NOTING THE CONSEQUENCES OF INSIDER THREAT, THE FEDERAL GOVERNMENT IS TAKING ACTION”

Insiders can inadvertently compromise networks in numerous ways. Users may install malware or spyware, allowing intruders to gain access and steal data, or distribute sensitive information to adversaries masquerading as legitimate parties during phishing scams.⁴ In addition, employee error may result in the loss, theft, or sale of agency property containing sensitive information. For example, in January 2013, the city of Macon, Georgia sold old computers without erasing the PII of city police officers from the hard drives.⁵

Finally, agency test and development environments should not be overlooked when assessing insider threat. Analysts, designers, programmers, and testers, whether internal employees or contractors, are all potential threats if given access to information not needed to complete their daily jobs. The insider threat problem is further complicated when agencies allow applications to directly access sensitive data. In a noteworthy case from September 2012, the Cumberland County Sheriff’s Office in Maine used new software to update its Facebook page and media list with arrest reports, but accidentally posted the Social Security numbers for all 180 people arrested. Before the error was caught, as many as 70 people are believed to have had access to the information.⁶

Though possession of one piece of sensitive data may not seem to constitute a significant threat, a substantial privacy risk can ensue when that information is coupled with other freely available data. This “mosaic effect” allows adversaries to create a fuller picture of the victim and more easily commit identity theft or identity fraud. Recently, criminals have used Social Security numbers gleaned from breaches to create new

“synthetic identities.” The creation of alternate identities can be devastating to the original holder of that Social Security number, especially when the victims are children. When the data breach is the fault of a government agency, the effects can be disastrous to an agency’s image and extremely costly to correct. Free credit monitoring services that government must provide for identity theft victims cost agencies millions of dollars, an unaffordable expense in today’s tight fiscal environment.

Noting the consequences of insider threat, the federal government is taking action. With the implementation of Presidential Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” every federal agency and systems integrator is required to implement an insider threat detection and prevention program by the end of 2013.⁷

Privacy Procedures Are Not Followed

Several government-wide policies mandate that agencies protect sensitive data. The Federal Information Security Management Act (FISMA) tasks each agency with developing, documenting, and implementing an information security strategy, while the Open Data Policy requires agencies to “strengthen measures to ensure that privacy and confidentiality are fully protected and that data are properly secure.” It also requires agencies to “incorporate privacy analyses into each stage of the information’s life cycle.”⁸

Other information security requirements apply to specific types of organizations. For example, Health Insurance Portability and Accountability Act (HIPAA) privacy rules dictate the “minimum necessary” use and disclosure of PHI and require that technologies be implemented to hide, protect, or mask individually identifiable health

information. Individual organizations also have their own data security policies. Even MNsure, the health organization responsible for the September 2013 PII data breach, had a privacy policy in place.⁹

Despite the existence of these policies, implementation remains a challenge. One of the largest challenges remains that users and applications are often granted permissions beyond what they need to perform their jobs. The Cumberland County Sheriff's Office software should not have had access to the Social Security numbers of those arrested and city workers in Macon should not have kept unsecured personal data on hard drives sent out for sale. Now, in the midst of implementing the Affordable Care Act, concern about access rights is reaching a new high. Federal and state officials, as well as insurance program "navigators," all have access to private consumer information through the Federal Services Data Hub.

Developing a Strategy to Limit Access Rights

When implementation is less than perfect, agencies should take action to limit inappropriate access to data. Before anything can be done, agencies must first understand where their sensitive data is and who has access to it. This often includes taking a complete inventory. Next, organizations can implement technologies to ensure that data access rights are protected. Firewalls and anti-malware software are necessary, but alone cannot prevent access to

private information by insiders such as database administrators (DBA) and system administrators. Authenticated applications and reporting tools also pose a threat.

Encryption, though useful for rendering sensitive information unreadable for unauthorized users, requires customizations to applications that can impact performance. In the fast-paced environment in which government operates, service delivery cannot be compromised. To adapt, vendors have developed a different technology known as data masking that offers a less obtrusive information security option for agencies.

Data masking solutions, like those offered by Informatica, mask or scramble data to limit access for all but authorized users. This scrambling can be applied to specific parts of databases or data stores, depending on the user's access needs. For example, a DBA would not need to see the Social Security numbers of employees, but a human resources manager would be able to access them freely.

Data masking can also be integrated with other authentication solutions and data protection technologies such as encryption to limit inappropriate access to data, but does not require changes to databases or application source code.

For agencies serious about information security, data masking presents a way for organizations to achieve robust, transparent, and cost-effective data privacy.

-Zoe Grotophorst

About GBC

Government Business Council 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. Contact Dana Grinshpan, Research Manager, Government Business Council, at dgrinshpan@govexec.com.

About Informatica

Informatica provides innovative and robust solutions for addressing the most pressing IT initiatives: data center consolidation; management of big data; application retirement; data integration, quality, privacy; and cyber security. Using our automated solutions, government organizations can focus time and resources on their mission-critical tasks, including defense and intelligence, law enforcement, tax and revenue, education, and the provision of benefits and services to the public.

Sources

¹ Jackie Crosby, "Errant e-mail creates security breach at MNSure," Star Tribune, 13 September 2013, <http://www.startribune.com/business/223564521.html>.

² Government Accountability Office (GAO), "Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity," GAO-05-434, May 2005.

³ World Economic Forum, "Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience," June 2012, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.

⁴ Government Accountability Office, May 2005.

⁵ Andrew Ressler, "Davis: Personal Info Left on City Computer Hard Drives Sold to Computer Repair Shop," 41 NBC/WMTG, 9 January 2013, <http://www.41nbc.com/news/local-news/18526-davis-personal-info-left-on-city-computer-hard-drives-sold-to-computer-repair-shop>.

⁶ "Cumberland County Sheriff's Office Leaks SSN's on Facebook," WCSH6, 6 September 2012, <http://www.wesh6.com/news/article/213809/314/Cumberland-County-Sheriffs-Office-leaks-SSNs-on-Facebook?odyssey=tab%7Ctopnews%7Cbc%7Clarge>.

⁷ Presidential Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," 7 October 2011.

⁸ Open Data Policy – Managing Information as an Asset, M-13-13, 9 May 2013, <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>.

⁹ Crosby, 13 September 2013.

Image: Flickr user JacksonClerk