FEDERAL

It's not them, it's us: The insider threat

By: Kon Leong, ZL Technologies, October 24, 2016 *(Photo Credit: ZL Technologies)*

The recent arrest of National Security Agency contractor Harold Martin for the removal of classified material and theft of government property has reaffirmed the vulnerability of federal organizations to the insider threat. Large enterprises and government agencies increasingly fear security breaches at the hands of cyber activists and state-sponsored entities, yet quite often the more immediate security threat comes from within.

Federal Times
NSA contractor to face espionage charges for 'breathtaking' theft of secrets

As a contractor from the same consulting organization as Edward Snowden, Martin's charges highlight the challenge of vetting and tracking the behavior of third party contractors where sensitive materials are involved. USIS, the company that vetted Snowden, has now reached a

$30 million settlement regarding shortcuts taken in background checks — this case predates the Snowden breach.

But even when soundly performed, a background check is far from conclusive. In retrospect, Snowden was a very clear candidate to commit security transgression, yet it can be deceptively difficult to uncover a disposition to such behavior through a background check, no matter how rigorous. If the NSA cannot preemptively detect an employee's threat to sensitive data before contracting them, normal organizations stand no chance.

It is a given that employees with dangerous data usage — whether malicious or not — will sneak through the cracks of the hiring process. This applies to the NSA just as it applies to any other

transgressions within the NSA and refocus data security efforts internally under the assumption that they have already hired a potential security threat.

Federal Times
Manning/Snowden leaks: The threat from within emerges

Exploring dark data

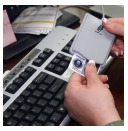
Enterprises and agencies have several incentives to store inordinate amounts of data: utility, e-discovery, compliance and now analytics. There is little disagreement about the value of big data analytics; however, analytics initiatives are impossible without control of data. Even worse, it exposes organizations to increased data vulnerability, from both external and internal sources. It's often the data a company is unaware of that becomes exposed.

The first step to gaining control of data is knowing what you have. File analysis tools should be used to tag and map data across the enterprise, initially through metadata analysis and then through content analysis to illuminate information that metadata alone cannot identify: credit card numbers, personally identifiable information (PII), proprietary content, etc. Once an agency has identified where sensitive information lies, it can take remediation actions — such as deletion, quarantine and relocation — and access privileges can be instated to ensure that files are only accessible to the necessary parties.

Agencies will often find they have sensitive information lying unprotected, in which case simple remediation steps can significantly reduce internal vulnerability. However, data cleanup must be a collaborative process across several departments — IT, records management, legal, as well as end users. Ultimately, the people creating the content have the best idea about who should be touching it, so they must be consulted during this process.

Once information has been tagged and mapped according to sensitivity, snapshots of data can be taken across the enterprise over time, creating a blood flow diagram of where sensitive information lies and where potential vulnerabilities are. From here, analytics tools can set baselines for normal data usage and detect abnormalities that may signify malicious behavior.

with PII, moves a large quantity of classified information or prints confidential documents, an agency will know about it. Once the linear curves of normal data usage are recognized, it's startling how easily deviation can be detected. Using behavioral analytics, an insider threat can be detected before he or she walks out the door.



Federal Times
CDM Phase II centers on monitoring user privileges, activities

Files analysis will help clean up an organization's data, but if nothing is done to preserve its benefits, data will soon return to chaos. It's vital that classification, remediation and retention decisions be used to create ongoing policies. This is only possible with true information governance.

Keeping data initiatives in check

As with any powerful information technology, analytics tools require absolute discretion. Irresponsible surveillance creates a culture of divisiveness and breeds contempt. For example, documents from the Snowden breach reveal that surveillance technology was used by NSA agents to track romantic interests, among other unethical applications. Accountability within the organization is essential, and this starts from the top.

Easier said than done. The only solution to keeping aggressive analytics campaigns in check — limiting unnecessary exposure and ensuring responsible data use among end users and administrators — is information governance. Clear access policies must be created through consultation with the risk guardians — general counsel, risk officers, compliance officers — to balance utility with privacy and define ownership of files. Audit trails can be utilized to create a culture of accountability among employees.

ambiguities can be clarified. For instance, these workshops should cover not only how to responsibly use virtual governance and analytics environments but also real-world protocols, such as inter- and intra-agency interactions.

In the NSA leak, Snowden reportedly obtained passwords from several other employees to access 1.7 million documents and emails. Social engineering — the manipulation of others to gain confidential information, security access or to affect a desired action — has been a key component in many of today's data breaches. To limit its effectiveness, workshops could potentially communicate which types of information can and cannot be disclosed between co-workers. This is typically one of the many gray areas in data security; and in business and government, gray areas can lead to disaster.

When it comes to harnessing powerful information technologies, sometimes the hardest choice is where to draw the line. We can choose to use them or not to use them, but the one thing we can't do is ignore them. As with all disruptive creations, the fabric of reality will inevitably become forever changed. It's up to us to make sure it's the reality we want.

Kon Leong is responsible for managing all aspects of the business, including strategy, finance, sales and marketing for ZL Technologies, including driving the company's partnership with the National Archives and Records Administration. He earned an MBA with Distinction from the Wharton School and received an undergraduate degree in computer science from Loyola College at Concordia

University after completing a year at the Indian Institute of Technology.

Federal Times

When is big data too big?

Long-term CR looms as Pelosi pans Ryan's 'minibus' plan

by Joe Gould

House Minority Leader Nancy Pelosi said Democrats will reject House Speaker Paul Ryan's plans for "m...

FEDERAL

IG: 18F has three months to make $56M

by Aaron Boyd

GSA's inspector general issued a report slamming 18F's funding methods and failure to recoup costs o...

FEDERAL

Next Article