New Insider Threat Emerges in the New Economy

Insider Threat Risks Increase in Face of Economic Woes

To neutralize the threats posed by insiders with ample motivation, IT departments must take away the means and the opportunities to commit crimes. Understand how employees and partners are engaging with your IT assets and intellectual property.

Insider Threat Risks Increase in Face of Economic Woes

They may not make up the majority of security incidents, but insider attacks have the most potential to cause the biggest losses within an enterprise. Think about it: trusted individuals know where the highest value information resides, they've got legitimate access to mission-critical systems and in many cases management has no mechanism in place to track what these individuals are doing with the systems or the data.

Information security experts are bracing for the law of unintended consequences to swing into action in 2009 as layoffs, downsizing and low morale bring the worst out of trusted insiders looking to profit off of proprietary intellectual property, customer contact lists, trade secrets and any other sensitive information. Many employees have admitted as much themselves in recent surveys—last December the majority of participants in a survey reported that if they were fired tomorrow they would definitely take company data with them to their next employer.

Psychology of the downtrodden employee

Even when times are good, there's always the risk of the bad apples giving in to temptation and taking advantage of an organization's trust for the sake of greed, revenge or simple malice. But when the economic climate takes a turn for the worse like it has recently, it isn't just the bad employees that pose a risk.

"In this economy, people are going to be more tempted to steal inside data, to sell it or use it for their own purposes. The insider threat will be more prevalent than in the past there will be more desperate players out there," says Jody Westby, Adjunct Distinguished Fellow at Carnegie Mellon University's CyLab and CEO of Global Cyber Risk, a Washington, DC-based cyber intelligence firm.

Desperation is a powerful emotion and it can make a lot of otherwise good people do things they wouldn't have normally considered in the past. The financial reward of cyber crime may begin to outweigh concern for morality and legal consequences as the economy tightens, the threat of layoffs hover and bills mount. Even those employees not targeted for layoffs at the moment are worried about their job security and the stability of the market at large as they watch co-workers and neighbors lose their positions and read dire news reports. This level of emotional distress is likely to be manipulated by savvy identity thieves, who are offering increasingly easier ways to sell and trade in confidential information through black market online marketplaces and other web channels.

Not only that, there will also be plenty other employees left distracted and overworked due to layoffs and budget cuts. This type can easily make mistakes that could compromise information through ignorance or laziness. For example, a harried employee may more easily give up credential information through social engineering or may not as readily follow company security policies regarding mobile devices.

What are the costs to an organization?

Whether an insider steals information for financial gain or simply leaves the organization open to a breach due to sloppy practices, the risks are costly to an organization. According to analysts with Forrester Research, the typical data breach can cost a company between $90 and $305 per lost record. Organizations stand to lose money in legal fees, the cost to report the breach to customers and fees from compliance organizations. What's more, they will lose even more in reputation damage, brand damage and customer departures. According to Ponemon Research, 20 percent of customers leave immediately upon finding out an organization suffered a breach. Clearly, this is a risk that cannot be ignored.

Who are these people?

In order to mitigate the risk posed by insiders, it helps to understand who these people are. Let's take a look at some typical malicious insiders and their modus operandi. And in case you don't think this type of activity really happens, we'll also look at relevant examples from recent news reports for each type of malicious insider.

Petty Identity Thief

One of the most common malicious insiders is the unsophisticated employee or partner looking to score a few sets of customer data here and there to commit small-scale ID theft on his own. For ex-

ample, it is not unheard of for a phone bank worker to cut and paste customer information into a word-processing document as he is granted access to resolve problems. That information can then later used by the worker to go on a fraudulent shopping spree.

> **Case Study:** Alaska Airlines
> Alaska Airlines informed customers that a former call center employee stole over 1,500 credit card records from the company in order to perpetrate ID theft. The employee diverted payments meant for both Alaska and sister airline Horizon to a personal account over a two year period.[1]

Data Fencer

This type of internal attacker works on a slightly higher level than the Petty Identity Thief. Instead of using the data herself to commit fraud, she'll simply sell it to one of the numerous criminal elements out there in the ID theft underground that buys personally identifiable information in bulk. This type of insider can inflict a lot more damage on the organization as she's usually looking to score a large database or list of names.

> **Case Study:** Countrywide
> In August 2008 news reports surfaced of a Countrywide employee who had been downloading up to 20,000 customer records to a USB device every weekend over the course of two years. The mortgage company had a policy against USB devices and disabled USB ports

---

1. http://www.pressdemocrat.com/article/20080812/NEWS07/808120370/1036/NEWS07&title=Alaska_Air_worker_stole_credit_data

on most endpoints, but this enterprising crook found one overlooked system. He was able to carry on for so long because the company had no method in place to find or monitor system on which it had not disabled USB devices.[2]

Ladder Climber

This particular insider is especially pernicious because he often doesn't believe he's stealing. He'll collect customer lists or intellectual property so that he can take them with him when he gets hired on by a competitor. Many times he'll justify his actions because he helped create the IP or develop some of the relationships with customers on those lists.

Case Study: Lending Tree

Lending Tree sent letters out to customers in 2008 informing them that their information was compromised by a breach caused by unscrupulous former employees. These enterprising souls decided to steal company passwords in order to take them to several lenders with no affiliation to Lending Tree. The resulting access to detailed customer data would allow them to target Lending Tree customers with their own mortgage offers.[3]

Saboteur

Rather than stealing information, this type of malicious insider is slightly more emotional. She's simply looking to hurt the employer rather than to make financial gains. She might want to do so in retribution for a firing or perhaps because she disagrees with some company policy or activity the organiza-

tion is involved in. This insider can be especially dangerous if she's a knowledgeable IT worker with special access privileges.

Case Study: San Francisco

This summer, a single rogue IT administrator for the city of San Francisco held hostage all of the passwords to the city's main WAN in a personal vendetta against the municipality. The employee was responsible for designing the WAN and administering it, and he'd grown disenfranchised with certain city policies and wanted to prove a point. The situation grew out of control as a result of his power as the sole holder of admin rights to the network and the single point of authority to make changes to the network.[4]

Clueless Rube

Much more benign than the typical internal attacker, this type of insider is risky nonetheless. In his mind, his convenience is more important than corporate security and he'll disregard useful company policies established to protect the organization. This type will load unauthorized P2P software on his machine, recklessly transfer sensitive data on unprotected USB devices and click into any old e-mail or website—regardless of how sketchy it looks—for his personal pleasure. This is the most prevalent insider threat and, sadly, outsiders know it. Cybercriminals today are targeting your employees' use of these insecure applications and taking advantage of the threat vectors opened up as a result.

2. http://www.washingtonpost.com/wp-dyn/content/article/2008/08/04/AR2008080401886.html

3. http://redtape.msnbc.com/2008/04/was-your-lendin.html

4. http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11P1M5.DTL

Case Study: U.S. Army

The U.S. Army announced that it would completely ban the use of USB devices as a result of a hapless user's mistake. The branch of the military had been completely ravaged by the spreading of the SillyFDC worm that first infected its internal systems via a USB device.[5]

Why they get away with it

According to the Internet Threat Resource Center, 24 percent of all data breaches that hit financial institutions in 2008 were caused by insider threat. Similarly, 20 percent of government breaches and 16 percent of other business breaches were caused by internal attacks.

The numbers are likely even higher once you consider those insiders who never get caught due to poor monitoring and still more who cause incidents that businesses choose not to disclose.

In taking a closer look at the traditional insider attack where the trusted individual consciously commits an act of fraud or sabotage, two elements are always at play: the motivation to commit the act and the means to do so.

Many insiders are successful because their organizations simply do not have the proper tools in place to enforce policies or even monitor employee and partner activity. Without visibility or automated en-

forcement, employees merely pay lip service to security policies—if the company has even bothered to draft any policies in the first place.

Without a doubt, the most dangerous means to insider attacks in the last couple of years are the ubiquitous USB devices that have proliferated across the enterprise. Removable devices are incredibly prevalent - over 40,000,000 USB Keys sold last year and that does not count the iPods, iPhones and other devices that have USB like capabilities.

Though these devices are useful business tools, if they are allowed on endpoints across the network without any supervision they can also prove to be an invaluable tool to those Ladder Climbers and Data Fencers within the employee pool. They can easily be used to remove large amounts of data or to deliver malware deep inside a network and users usually do not give a second thought to plugging them in to work computers.. And organizations do not have the visibility into how these devices are being used and what data is being moved on and off these devices.

There are other dangers, too. Other threat vectors from the inside also include a lack of configuration controls and monitoring of configurations and lack of visibility into all of the systems connected to the network. Another risk, particularly among the Clueless Rubes, is a lack of control on the endpoints (desktops, laptops, mobile devices, etc.), including the inability to control what software systems run and what updates are installed on those systems.

5.   http://blog.wired.com/defense/2008/11/army-bans-usb-d.html

What you can do

In order to neutralize the threats posed by insiders with ample motivation, IT departments must take away the means and the opportunities to commit crimes. By creating strategic policies and by automating the monitoring, enforcement and reporting of those policies, organizations can understand how employees and partners are engaging with IT assets and intellectual property.

When it comes to USB devices, the best way to protect against abuse is not to ban the devices, per se, but to control how they access data, what data they can access and when they can access it. Lumension Data Protection Solution enables organizations to enforce flexible policies to ensure secure data and device management without impacting productivity. Additionally, robust monitoring and reporting capabilities provide IT with the visibility into user interactions with data so that it can go back to risky employees and inform them of the security implications caused by their actions.

Lumension Vulnerability Management Solution provides organizations with centralized management over their endpoints to ensure proper configuration of machines, control over legitimate software updates and information about every device on the network. Combine this with Lumension Endpoint Protection's application whitelisting approach, which only allows pre-approved applications to run on enterprise systems, and IT staff can drastically reduce the opportunity insiders have to cause harm to an organization.

Of course, technology is never the sole answer to a security problem. IT departments need to develop a comprehensive program that fully utilizes its tools. Acting on the following five steps is a good way to get started in the process:

1. **Discover & Assess Risk** – Know what is in your environment – what assets and what vulnerabilities – and know where your most critical risks lie. Network and agent-based scanning, plus assessment, provide the depth and breadth of info needed to make the right decisions.

2. **Establish & Enforce Policy** – Policies are only as good as the paper they are written on unless there are ways to enforce them. Whitelisting capabilities ensure that only those authorized applications can execute and only those authorized removable devices can be accessed on specific endpoints by specific users. Having the ability to set policies that enable flexibility is key – some policies are only appropriate for some users or departments and not others.

3. **Fix Open Vulnerabilities** – Many research studies and analyst firms have stated that the majority of risk – more than 90 percent - comes from known vulnerabilities. These vulnerabilities are in operating systems, applications, web browsers, and virtualized platforms. If you can stay on top of the vulnerabilities that are critical to your organization then you can mitigate a lot of the risk of outside attackers targeting insiders.

4. **Control and Monitor Devices** – Removable devices are commonplace among individuals. Many folks have multiple devices and they expect to be able to use these devices on business machines. It's what Gartner calls 'the consumerization of IT.' While many of these devices provide benefits that enable a more productive workforce, they also must be managed because of the storage capacity and ease of which data can be moved on and off. Also with the U3 technology and other applications that run on devices, these can introduce malicious code onto your network quite easily. It is imperative to employ systems and practices that enforce what devices are authorized or not, by what users and on what machines. Also necessary is the ability to track what information is being moved on or off these devices.

5. **Audit** – Having visibility into what your users are doing, what data is being moved and what applications and vulnerabilities are in your environment is very important from an audit-readiness perspective. High level and low level auditing capabilities provide necessary levels of insight into the effectiveness of your policies and enforcement capabilities.

Who is Lumension

Lumension™, Inc., a global leader in operational endpoint security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets.

Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at www.lumension.com.

For more detailed recommendations on protecting from risks posed by insiders, please review additional information contained in two other whitepapers or quantify your risk with these free tools:

Whitepapers

» Why End Users are Your Weakest Security Link
» Taking Control of Your Data: Protecting Business Information from Loss or Theft
» Automating the Vulnerability Management Lifecycle
» Whitelisting Technology Improves Security, Reliability and Performance Via Trusted Change

Security Tools

» Device Scanner
» Application Scanner

Lumension™
IT Secured. Success Optimized.

Global Headquarters
15580 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260 USA
phone: +1.888.725.7828
fax: +1.480.970.6323