

Insider Threat: Troubled Economy Puts Organizations at Greater Risk



UES Limited t/a Unity Solutions U.K.
Unit 3
Beswick House
Greenfold Way
Leigh WN7 3XJ
Telephone: +44 1942 267 488
Email: info-uk@unitysolutions.com

Unity Solutions LLC
13575 58th Street North
Suite 136
Clearwater, FL 33760-3746
Telephone: 727 538 4143
Email: info-usa@unitysolutions.com

The reality of insider threat

Insider threat is a reality, and unfortunately, companies are more vulnerable in the down economy. The risk of insider threat greatly increases during times when companies are laying off staff, cutting back on raises and bonuses, deferring promotions, consolidating operations, and outsourcing work to save money.

Massive layoffs have been making headlines for months. In fact, the steep annual drop in jobs marked the highest yearly job-loss total since 1945, the year in which World War II ended. *CNNMoney.com* reported the hemorrhaging of American jobs accelerated at a record pace at the end of 2008, bringing the year's total job losses to 2.6 million or the highest level in more than six decades.

During these turbulent times, security analysts are warning companies to be even more alert to potential insider threat. Not only are angry employees more likely to lash out against their employers, but stressed, worried employees also make easier targets for opportunistic rivals.

Even when employees are fired for legitimate reasons, they might become bitter and launch an internal attack. For example, last year in San Francisco, Terry Childs, a computer network administrator for the Department of Technology, tampered with the network that contains the city's sensitive data and created an administrative password that gave him exclusive administrative access. City prosecutors and San Francisco's mayor sought to resolve the crisis by hiring experts to try to regain control of the city's network. The city is worried that Childs, who worked for the city for five years but faced firing for alleged poor performance, may have installed the means to electronically destroy sensitive documents.

Regardless of the reasons, attacks by company employees are now more common than attacks launched by outsiders and hackers. In fact, the FBI's statistics suggest that 70 percent of attacks in 2007 originated within organizations, and the number keeps growing.

The attacks run the gamut — from fraud to stolen proprietary information to bits of code planted to cause system or network failure, and from financial institutions to retailers to technology companies.

For example, in a 2008 case, the FBI alleges that former Intel employee Biswahoman Pani of Worcester, Mass., copied documents, including 13 top-secret company files containing highly sensitive design plans for future processor chips. In the complaint filed in U.S. District Court in Boston, the FBI stated in an affidavit that more than 100 pages of sensitive Intel documents, as well as 19 computer-aided-design drawings, were found during a search of Pani's house.

Another 2008 case occurred in San Diego when an IT specialist deliberately deleted patient and allied data from his former employer's computer systems.

On the international front in 2008, Jerome Kerviel cost France's second largest bank, Societe Generale, \$7.2 billion when he made unauthorized trades that he hid for months by allegedly hacking into the computers of the bank and creating fraudulent transactions to hide his actions. His combined trading positions totaled €50 billion (\$73 billion). This type and magnitude of attack can only occur when there is a fundamental failure of information security controls.

Lanxoma, the industry's first Restricted Access Permission System (RAPS), recently conducted its own survey of CIOs and IT leaders to determine their take on insider threat. The findings revealed that 43 percent of respondents have experienced some type of fraud, theft or loss as a result of insider attacks, and 12 percent believe they have experienced a substantial amount of malevolent activity.

In fact, 22 percent of Lanxoma survey respondents believe that dissatisfied, under-recognized employees are most at risk to commit some type of fraud or theft. Although nearly one-third of respondents believe that

employees with a technical background are more risky, the truth is, an employee doesn't need to be technologically savvy to launch an insider attack.

For example, in November 2006, a DuPont scientist admitted to stealing corporate-given conditions valued around \$400 million shortly before he left DuPont to work for a rival company.

Here's an example that goes back 13 years and involves multiple employees who worked together to launch an attack. For several months, beginning in the fall of 1996, two credit union employees worked together to alter credit reports in exchange for financial payment. As part of their normal responsibilities, the employees were permitted to alter credit reports based on updated information the company received. However, the employees intentionally misused their authorized access to remove negative credit indicators and add fictitious indicators of positive credit to specific credit histories in exchange for money. The total amount of fraud loss from their activities exceeded \$215,000. The risk exposure to the credit union was incalculable.

Insider attacks occur across all organizational sectors, often causing significant damage to the affected organization. These acts have ranged from low-tech attacks, such as fraud or theft of proprietary information, to technically sophisticated crimes that sabotage the organization's data, systems or network. According to research from the Ponemon Institute, the average cost of a data breach was US\$4.6 million in 2006.

The largest case of identity theft to date was the result of an insider attack and ended in September 2004 when Philip J. Cummings, a former technical support representative at Telecommunications Data Inc., pled guilty to one count of wire fraud, one count of fraud related to ID documents and information, and one count of conspiracy for his involvement in a scheme to steal identities, which defrauded financial institutions of more than \$11 million. Cummings allegedly stole the passwords and access codes of Ford Motor Credit and other financial companies to access credit report records and downloaded credit report information on 30,000 individuals. He allegedly sold the credit reports to a group of co-conspirators.

Organized crime rings are also coordinating attacks. In April 2005 in Hackensack, NJ, Orazio Lembo led an organized insider crime ring that stole more than 675,000 identities and earned Lembo as much as \$4 million. Lembo allegedly set up a bogus collection agency called DRL Associates. He then hired seven bank employees — including branch managers from Wachovia, Bank of America, Commerce Bancorp, PNC Bank NA and a former NJ Dept. of Labor manager — to steal personal account data and social security numbers of bank customers. The group created a manual database of all the identities and sold the data to more than 40 other collection agencies. Lembo paid bank employees \$10 for each record they delivered, and then he charged collection agencies up to \$150 for the data.

The harsh reality is that insider threats exist for all organizations. The threat lies in the potential that a trusted employee may betray his obligation and allegiance to his employer and conduct sabotage or espionage against the company. Betrayals range from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance and sabotage.

Unfortunately, the stigma that an act of insider betrayal carries with it can cause customers, partners, and shareholders to lose trust in an organization. This loss of trust can translate into lost business, revenue, and value. If your organization has not taken a hard look at insider threat controls, then now is the time.

Red Flags: 10 Warning Signs of Employees Who May Pose a Risk

Tough economic times create uncertainty in the workplace, causing employees to become worried about losing jobs and promotions, and concerned about financial liabilities and mortgages.

Stress can come from inside or outside the work environment. An employee, for instance, could be experiencing financial problems or may have lost a home to foreclosure because of an inability to meet the mortgage payments.

This added employee stress makes companies more vulnerable to threats. With this in mind, companies need to keep an eye out for disgruntled employees as they downsize their workforces. Additionally, supervisors need to be trained to spot employees in distress or those who could pose a security problem in the future.

Remember, never rule out anyone, even long time employees. In fact, long time employees may be more aware than anyone of the weaknesses in the computer information system and the ways to get around security.

Here are 10 warning signs an employee may pose a risk:

1. A worker who habitually violates company policy or “breaks the rules” may not be trustworthy enough to handle sensitive computer information.
2. An employee, who suddenly starts working after hours, stays late for no obvious reason or keeps asking for overtime to make ends meet, could pose a risk.
3. Someone trying to gain access to systems and information that they really have no need for could be a sign that something is amiss.
4. An employee who prints out large volumes of data after hours, or e-mails it to himself, could be cause for concern.
5. A worker who displays irrational behavior such as threatening verbal statements toward the company or supervisors should be taken seriously and closely monitored.
6. Recent excessive and unexplained absences from the job, concentration problems, increased signs of poor health or hygiene, and the inability to accept responsibility for errors, are all warning signs of a distressed employee.
7. Extreme mood swings or inappropriate display of emotions on the job such as uncontrolled anger or excessive crying are warning signs of extreme stress.
8. An employee, who is preoccupied with his computer activity, or scheming against a specific supervisor, could be cause for concern.
9. A staff member who is living far beyond his means could be cause for concern. Illegal activities could provide an outside source of income to support a lavish lifestyle.
10. Increased stress in the employee's personal life including financial problems, problems in his or her marriage or other relationships, could cause him to act out of character, making him more prone to questionable activity.

Remember to view these warning signs in context of an employee's typical behavior. These red flags are not meant to cause concern, as employees are people who have stress in their lives, and most people can handle stress well enough to function properly at home and work. However, if you notice a change in employee behavior, use common sense, realize where you are vulnerable, and keep a watchful eye.

Processes, Policies Protect Against Insider Threat

It's essential for organizations to put processes and security measures into place to protect their systems, data and customers against insider threat. Based on an analysis of hundreds of corporate data breaches, including three of the five largest ever reported, Verizon Business found that nine in 10 corporate data breaches could have been prevented had reasonable security measures been in place.

Lanxoma's survey of CIOs and IT leaders revealed that 38 percent of respondents do not have solutions and processes in place. Although 22 percent said they have solutions and processes in place, they are either unreliable or insufficient. A slim 11 percent of respondents feel they have solid solutions and processes to combat insider threat, and consistently adhere to them.

At a minimum, IT organizations need to:

1. Perform a risk assessment and analysis on important customer and employee data and intellectual property.
2. Perform an inventory of data and categorize its sensitivity level based on a risk analysis.
3. Define policy for protecting sensitive data and educate employees on this policy.
4. Create processes for managing data based on data-handling policies – and have policy in place for how sensitive data is backed up and stored.

Although a policy is an important step, IT leaders must ensure that policies are socialized throughout the organization and enforced. The CIO and others within the IT department should have access to a continuous report of the organization's environment, what policies are working and which ones are not, and they should adjust policies accordingly.

IT also needs to consistently monitor privileged access users, and access restrictions must be implemented as people move within the organization. The Lanxoma survey found 20 percent of respondents have strict access restrictions for people who move within the organization. However, 17 percent admitted they do not have access restrictions or that employees know how to override the restrictions.

Companies that lay off large numbers of people or engage in a consolidation or merger need to ensure former employees no longer have access to internal systems and data.

If a person either leaves the company or is fired, make sure that user account is disabled immediately. In addition to terminating accounts, it's important to monitor critical applications and activity logs to make sure those who previously had access to them can't access them through some other entry point.

Once policies are defined and implemented, companies need to focus on awareness and training. Organizations can reduce a significant amount of risk by informing users of their responsibilities to follow policies and to report suspicious activity. Although 20 percent of Lanxoma survey respondents said they have a solid awareness training program in place, 61 percent said they either have no training or infrequent training available.

Developing an adequate security policy is a relatively straightforward process, but is often overlooked or not taken seriously. To be effective, strong security policies must be enforced with strong monitoring technologies. And, once the proper policies are created and implemented, they must be kept current.

Technology to Combat Insider Threat

Imagine a bank robbery. The bank president may not be able to prevent a heist, but he can install security cameras and other technologies that record the crime, creating evidence that can be used in criminal prosecution.

This analogy can be used for corporations. No amount of employee screening will eliminate risk. After all, where there are people, there will be crime. Despite leading edge security technologies, and solid policies and procedures to monitor and report suspicious activity, a company may not be able to prevent employee fraud, eliminate employee data theft, or stop malicious damage to corporate systems and networks.

IT leaders can, however, install software that acts like a security camera, recording employee cyber activities and collecting evidence that can be used to prosecute a worker. Lanxoma, the industry's first Restricted Access Permission System (RAPS), provides a solid, secure way for organizations to combat insider threat, and it's the only product of its kind on the market. Just like a video camera, Lanxoma doesn't prevent the break-in, but it helps the investigation.

Lanxoma enables corporate executives to actually "see" what IT workers with privileged system access have been up to. They can literally watch a video capture of an employee's movements inside the system, and view exactly what the employee did while he was logged in.

With Lanxoma, technicians require management approval to gain access to the system and must state the purpose and estimated time required for their access. While inside the system, each keystroke, mouse movement, screen viewed and audio heard is digitally recorded and available for subsequent playback.

With Lanxoma, technicians are notified that their cyber activity will be recorded. When employees know they are actively being monitored and recorded, they are less likely to commit theft or malicious damage to the system. It's the simple fear of being caught that helps prevent the crime.

In addition to recording cyber activity, management is advised by e-mail, instant message or text message of a system log-in as well as log-out. Unexpected activity can be investigated immediately. In the event of legal proceedings, digitally signed evidence can be provided.

You may have protected your applications, fire-walled your PCs and workstations, secured your network, but until you have deterred the "insider threat" your system is not secure and until you have digitally-signed evidence of system abuse, you don't have much chance of sympathy from your customers, suppliers, staff, media, community... insurers, regulators or the law.

Lanxoma is software for people who know there are "bad guys" out there. It is for CIOs who have to know what's happening at operating system level; it is for CFOs and auditors required to fulfill their compliance responsibilities; it is for CEOs with a need for confidence in the integrity and security of their company and its information.

About Lanxoma

Lanxoma (www.lanxoma.com) is the industry's first Restricted Access Permission System (RAPS), and it is currently installed on more than 2,000 PCs in four countries. Lanxoma restricts access to the root level of computer operating systems, grants limited-time access permission to authorized users and records all activity while the authorized user is logged on.

View an online demo at: <http://www.lanxoma.com/onlinedemo.html>

- Lanxoma ensures 100 percent compliance with regulatory mandates.
- It provides in-depth investigation and forensics for insider threat incidents.
- Lanxoma detects and prevents fraudulent activities, as well as alerts organizations to unauthorized systems access so they can combat insider threat attacks.
- Lanxoma provides staff coaching when mistakes are made.

Special Note: Many of the insider theft crimes noted in this paper we're found in the book "The Insider," by Dan Verton. Thanks, Dan, for your long-time research and reporting on the subject of Insider Threat.