20 Ways To Mitigate The 3 Types Of Insider Threats: Part 1 of 2

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for March 2008 CSI Alert

More reports of insiders doing bad things

It was interesting to read the many different information security threat predictions for 2008 and not find very many that mentioned the significance of the insider threat. Every week more incidents are reported that occur as a result of insiders, yet very few organizations take the initiative to effectively address the insider threat to reduce the risks as much as possible.

The U.S. Secret Service in partnership with the Carnegie Mellon CERT released two new insider threat reports in January 2008 that are worth downloading and putting into your files. They are "Insider Threat Study: Illicit Cyber Activity in the Government Sector" and "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector"; download them from http://www.cert.org/insider_threat/. They contain great information and case studies you can use to create your own insider threat risk reduction policies, procedures, training materials, and awareness communications.

I have two criticisms for the reports, however.

1. I am disappointed that all the data they used comes from incidents that occurred between 1996 and 2002. The types of incidents in the past six years are much more extensive, and it would be worth researching and analyzing how recent insider incidents are occurring.
2. The reports only look at incidents that occurred as a result of malicious intent. There are so many more incidents that have occurred as a result of mistakes and worker unawareness, and it would be valuable to provide information about these.

It is important to recognize that there are three primary types of insider threats so you can work to effectively mitigate them.

1. People Make Mistakes

No matter what type of security technology is used, personnel will make mistakes. If a worker has authorization to access sensitive information and personally identifiable information (PII), a simple mistake can result in a damaging privacy incident. Here are just a few examples:

- An October 11, 2006 news report indicated the Republican National Committee mistakenly emailed a list containing the names, races, and Social Security numbers (SSNs) of dozens of top Republican donors to the reporter who wrote the story about this faux pas.

It is so easy to make this type of mistake! People are too quick to click an email address from their address book and immediately hit send before confirming the address was the one they actually wanted. This tendency adds more reason to require sensitive data that must be sent in emails to be encrypted.

- A January 25, 2007 report indicated the names and SSNs of 3,031 newly licensed nurses were accidentally posted on the Ohio Board of Nursing's website not just once, but twice; once in December 2006 and another time in January 2007. They didn't realize the mistake until a nurse visiting the site saw the information and reported it.

When companies make web site changes in a hurry, without proper quality or change control procedures, these types of incidents will occur. A significantly large number of incidents, of all types, are not discovered internally, but are reported to organizations, much to their chagrin, by people outside, such as customers, the general public, news media, and so on. Organizations must be prepared; they must have controls in place, procedures to consistently apply the controls and to identify incidents, and a documented security incident and privacy breach identification and response plan.

- On November 27, 2006, the Chicago Tribune reported that a printing contractor for the Chicago Public Schools mistakenly mailed a list of names, SSNs and home addresses for 1,740 former school employees as part of a packet of health-insurance information to all the employees.

This is another privacy breach resulting from a combination of human error and actions by an outsourced vendor. If you entrust a contracted vendor to handle PII, you need to make sure that they have controls in place to prevent privacy breaches. In this case, why did the schools give the printing contractor the list of PII for former employees anyway? It was probably a mistake.

- A January 24, 2008 news report indicated a U.K. Dell customer complained to the Information Commissioner's Office (ICO) after his loan agreement documents, which included bank account details, signature and debit card number, were mistakenly mailed to the wrong address; to a man with a completely different surname living in Ireland. Dell reportedly didn't know of the mistake until the recipient in Ireland contacted the man in the U.K., who then contacted the ICO, who then notified Dell.

No one is perfect. You should expect that your personnel will make mistakes. Do what you can to prevent privacy breaches as a result of their inevitable mistakes.

2. People May Be Unaware

Many incidents happen because personnel are not given the training and awareness necessary to effectively safeguard information. You cannot expect for personnel to intuitively know how to protect information; you must provide them with periodic training and ongoing awareness communications to help them obtain the security and privacy understanding necessary to effectively perform their jobs while protecting information. It is your responsibility as an information security and privacy practitioner to make sure your personnel are not security clueless.

I have spoken to business leaders in many organizations who shared their experiences of how bad things happened as a result of personnel not having security knowledge or understanding. I have found some of the most often recurring incidents resulting from unawareness include:

- Loading large amounts, usually entire files, of clear text PII onto mobile computers and storage media and then taking out of the corporate facilities to be lost or stolen because personnel didn't know they weren't supposed to do this.
- Related to the previous bullet, far too many personnel still leave their mobile computers and storage media unsecured, in clear view, in their cars, on coffee shop tables, in airport pubs and other public places, and then have them stolen, often because they say they didn't know of the risks involved. They "didn't think it was likely someone would take their stuff."
- Sending clear-text PII within email messages or email attachments and then having the PII forwarded to someone else, intercepted, mistakenly sent to the wrong folks, and any number of other bad things, because personnel didn't know they weren't supposed to put PII in messages.
- Employees giving their systems and applications passwords to co-workers, most often their managers or people claiming to be technical support, and then having those other folks get to their authorized information and do bad things, because they didn't know they weren't supposed to share their passwords.
- Customer service call center representatives giving PII to callers without first verifying the caller's identity, and then having fraud occur because the social engineering criminal successfully scammed them because they didn't know they were supposed to verify identities of callers.
- Personnel leaving very confidential information out in the open in their work areas, and then having others take, copy or use the information, because they did not know they were supposed to secure PII and other sensitive information when they were away from their desks.
- Marketing and sales folks selling customer PII as a source of revenue generation because they did not know this was against the company's policies, in addition to being a violation of the posted privacy policy promising that no PII will be shared with third parties.

And the list could go on and on. Whenever personnel are unaware of how to secure information, a very wide range of incidents will occur.

Personnel must have training and receive ongoing awareness communications about information security and privacy policies and procedures to make sure they understand how to effectively safeguard information. Too many organizations completely disregard the importance of periodic training and providing ongoing, effective, information security and privacy awareness communications.

3. People Can Be Vengeful

And there will always be a significant percentage of workers who will do bad things if they are motivated. They may think they deserve more money, they may think that their company is too rich, they think that their company has been unfair to them and so on. There are unlimited motivations for workers doing bad things with their authorization.

Here is a perfect example of how quickly an employee will use her authorized access to get even with an employer if she thinks her job is in jeopardy.

- Marie Cooley, a former employee at the Jacksonville, Florida, small business Steven E. Hutchins Architects, read the paper one Sunday morning in January 2008 and saw what she thought was a help wanted ad for her job. So, she went to her office that night and deleted, using her authorized access, 7 years' worth of the architect firm's files. Steven E. Hutchins Architects valued the deleted files at $2.5 million.

Guess what? The business did not have backups! The business was able to get the files back, though, using very costly forensics methods. And then, come to find out, the owner was not planning to fire Cooley; the job she had read about was for Hutchins' wife's business. Cooley could get 5 years in prison for this 2nd degree revenge felony.

The sad fact is that there are so many examples for how malicious insiders do bad things that it was hard to narrow down the examples! But, I want to provide a few more for you to consider using within your training content and awareness communications.

- In 2001 Steven William Sutcliffe posted the PII of over 1000 of his former co-workers, including payroll information, SSNs, birth dates, and residential addresses, with some of this information hyperlinked to an article about identity theft on his personal web site, in addition to posting and making threats to injure or kill others in retaliation for being fired from his job for not providing his SSN to the Human Resources department. The case was still dragging on in the courts in late 2007.

Pretty scary stuff, eh? It really shows how the need for information security and privacy policies goes beyond compliance and truly are necessary for mitigating many types of risks. It also highlights the insider threat.

- On January 9, 2008, the U.S. District Court for the Northern District of Georgia sentenced William Bryant to 5 months of prison, a $15,470 fine, 5 months home confinement, 2 years of supervised release, and 200 hours of community service for hacking into the computer and telecommunications system of his former employer, Cox Communications after he was asked to resign. Bryant "remotely shut down portions of the company's system, resulting in the loss of computer and telecommunications services, including access to 9-1-1 emergency services, for Cox customers in Texas, Las Vegas, New Orleans, and Baton Rouge. Cox technicians restored service within hours."

This shows yet again that revenge is a strong motivator. It also shows how the actions of a malicious insider can have impact beyond just interrupting business. Bryant shut down 911 services for a very large geographic area. This demonstrates how information security goes beyond just protecting networks; in this case the incident had life and death consequences.

- On January 8 a federal court in Newark, New Jersey, sentenced Yung-Hsun "Andy" Lin, a former systems administrator for Medco Health Solutions Inc., to 30 months in prison for planting logic bomb computer code intended to delete data stored on Medco's network in October 2003. Lin must also pay restitution of $81,200 to Medco for costs the company incurred to repair the damage he caused to its computer systems.

Lin also placed the logic bomb on servers containing applications used for Medco clients' clinical analyses, rebates, billing, managed care processing, new prescriptions called in by doctors, coverage determination requests, corporate financials, pharmacy maintenance tracking, pharmacy statistics reporting, and employee payroll input. His changes could have had widespread health impacts to many people; once again showing how computer crime by an insider truly can physically harm people. Lin was afraid he was going to be laid off from his job, and he wanted to logic bomb in place in case he was. Job insecurity fear is a strong motivator for insiders to do bad things.

- In October 2007 Joseph Nathaniel Harris, the former branch manager of the San Jose Medical Group's McKee clinic, was sentenced to 21 months in prison and three years of supervised release, and ordered to pay $145,154 in restitution for stealing computer equipment and a DVD containing patients' names, SSNs, medical diagnoses and other information in 2005. He reportedly also stole money and medications from the clinic, and is suspected of burglarizing the area clinics after he left his job as manager.

Harris was in a position of trusted authoritative access. Reading the full account, it does not appear there was proper separation of duties in place. However, considering this was a small to medium size business (SMB) it is not surprising; SMBs often do not have the personnel or budget to ensure effective separation of duties. This makes it that much more important for SMBs to implement compensating controls to address this weakness.

I could continue writing these short blurbs of insider threat incident examples for hundreds of pages. However, this should give you a good idea of what people are capable of doing with malicious intent.

Coming in Part 2…
So, what can organizations do to combat the insider threat? You cannot prevent all people in positions of trust from purposely abusing their capabilities to do bad things. You cannot prevent all people from making mistakes. You cannot ensure all people have the knowledge necessary to properly safeguard information. However, you can take many actions to significantly reduce these threats. You must implement appropriate due care controls to mitigate the risks of people within your organization doing bad things as much as possible. I will give you 20 effective ways to mitigate the insider threat in Part 2 of this article in the April issue of the Alert.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She just released the quarterly employee awareness tool, “Protecting Information” (Information Shield) and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.