Leap of Faith

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

Final Draft for September, 2005 CSI Alert

Just Shut Your Eyes and Go!

I recently went on my first vacation in over eight years to a tropical island. Among all the other fabulous water activities there were many different fantastic water slides I loved going down, and one of them was called the Leap of Faith, running down the side of a Mayan pyramid replica. It is six stories tall, with the slide going down into a tube running through a large open water shark lagoon. The slide is almost vertical; just enough slant so that you don't fall head over feet at the top and catapult yourself into the pools with the thrashing hungry sharks. The top of the slide has a cover so that no one waiting in line can see down the slide; only the person who is sitting on the slide ready to launch can see when they scoot themselves forward. The man in line in front of my son and me positioned himself to go down, but then he backed up with a look of panic on his face. Then, after looking back at everyone in line, he pushed himself off and disappeared, a faint scream trailing him. My eight-year-old son was next. He sat and hesitated, but then pushed off. As I positioned myself at the top all I could see was the slide disappear like a cliff in front of me; the cover kept me from seeing anything beyond. What did I get myself into? From outside and below I had watched many people plummet down this slide, so I decided my best strategy was to not even look over the edge; isn't ignorance bliss? So, I shut my eyes, crossed my legs and arms, and took the Leap of Faith. My heart pushed into my throat as I felt as though I was freefalling with gravity pulling me at warp speed to the bottom and through the tube to be deposited into the calm destination pool with my legs so shaky that I wobbled up the stairs out of the water. But, I had survived, enjoyed the rush, and my son was ready to go again! Shutting my eyes, following the posted precautions for body positioning, and trusting the slide designers resulted in quite an exciting Leap of Faith experience! Many organizations often seem to take, perhaps by choice perhaps by circumstance, this same blind trust leap of faith when placing personnel into positions with trusted and high impact authority and security capabilities.

Trust Where Trust Makes Sense

When placing personnel into positions of great power and trust capabilities organizations often make a shaky effort at best to ensure they are qualified, or will not be a risk within the position. Employers often have a hard time finding qualified folks to fill these positions. In their desperation to fill these vital roles they tend to not want do anything scare potentially good, scarce, candidates away by digging too deep into their past experiences or capabilities, or examining whether they have been involved in shady, or even criminal, conduct. As an information security or privacy practitioner you are in such a trusted role. What kind of due diligence was performed before you started your position?

Trying to obtain and retain good employees certainly is necessary, but organizations must realize that the trust they impart upon their employees need to have certain limits. Keep the auditor's "trust but verify" mantra in mind. Not only are security measures necessary to help protect against the malicious

activities of those employees who cannot be trusted, such security measures are also necessary to help protect against the mistakes and lack of knowledge of well-meaning employees that could lead to minor at the least to business-closing at the most incidents.

This tribal instinct of trusting everyone who is part of our team or organization must be tempered with good business practice and establishment of due care processes. Trust is certainly good and desirable, but blind trust is not good business practice.

Some of the most trusted positions within an organization are within the IT and information security areas. Systems security administrators hold rein over your network. Making sure these folks are appropriately monitored, have appropriate controls applied, and receive adequate training is a demonstration of due care that your organization needs to take to time to implement. While the vast majority of IT staff will do the right thing, there are still those folks who will be tempted to abuse their powerful capabilities and do wrong.

"I Have Seen The Enemy and He is Me" - Pogo

Consider a few cases in the news recently:

- In August 2005 the Helsinki, Finland branch of global financing company GE Money had police investigate the June theft of about €200,000 ($245,400). The police reported they believe the company's head of data security stole the money using the company's banking software along with passwords for its bank account. Accomplices then accessed the account from a laptop computer using an unprotected Wi-Fi network at a nearby apartment building. Investigation revealed the laptop's MAC address belonged to GE Money, and the bank's security officer was soon implicated.
- In 2003 it was reported an angry system administrator, who alone developed and managed his company's network, centralized the software that supported the company's processes on a single server. He then coerced a coworker to give him the only backup tapes for the software. After the system administrator was fired for inappropriate and abusive treatment of his coworkers, a logic bomb he had planted deleted the only remaining copy of the critical software from the company's server. The company estimated the cost of damage in excess of $10 million and as a result had to layoff 80 employees.
- In 2003 it was reported an application developer who was downsized out of his job launched an attack on his former employer's network three weeks after his termination using one of his former coworker's user ID and password to obtain remote access to the internal network. He modified many of the company's web pages by modifying text and posting pornographic images, in addition to sending each of the company's customers an email message letting them know the web site had been hacked, along with the customer's ID and password for the website. A month and a half later the developer

attacked again through the remote connection, this time resetting all the network passwords and changing 4,000 pricing records. He was sentenced to five months in prison, two years supervised probation, and ordered to pay his former employer $48,600 in restitution.

The National Research Council, Computer Science and Telecommunications Board reports the occurrences of employees with authorized access to critical network resources committing fraud are likely to be increasing even though such crimes are under-reported to law enforcement and prosecutors. The 2004 U.S. Secret Service/CERT® Insider Threat study reports organizations are often reluctant to make such reports because of insufficient level of damage to warrant prosecution, a lack of evidence or insufficient information to prosecute, and concerns about negative publicity.

Preventing Crime by Insiders Is Difficult

It is difficult for companies to guard against crimes when internal staff is involved, which makes it even more important to implement security measures internally. There are comparably few reported incidents of computer crimes committed by insiders, but that definitely does not mean that there are few crimes that are actually committed. It is likely many of these unreported crimes are committed inside the network. It is also likely that many crimes go undetected. In July 2004, Scotland Yard's Computer Crime Unit reported UK businesses typically only report five to seven per cent of all computer-based crimes to the police. "Around 93-95 per cent of all cybercrimes go unreported because companies rate unwanted publicity as potentially more damaging to their business than the incident itself." While this number is basically an educated guess, I anticipate it is reasonable and generally applicable to other countries as well. Also consider all the crime that goes undetected. Crimes committed by those in trusted positions will not necessarily have a clear impact on your company. Think about all the cases of identity theft that may have occurred because people with trusted access to this information sold it to others, or they used the information themselves to commit a crime. If the crime was not linked to your company, how would you ever know?

Here Today, Gone Tomorrow

Several years ago individuals took employment with the hopes of building a future, nice pension, and comfortable retirement from their employer. Employer loyalty was strong. A May 1976 Bureau of Labor Statistics survey showed that only 4.2% of all workers were interested in changing jobs. A 2005 survey conducted by the Society for Human Resource Management and CareerJournal.com reported that 81% of today's employees are looking elsewhere for jobs. This diminished loyalty must be considered when filling positions of trust. Is it as easy to trust someone who's only with you for the short term than someone who wants to be with you for the long haul?

Leap of Faith

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

Final Draft for September, 2005 CSI Alert

Look Before You Leap

Employers have a duty to exercise due care when hiring individuals who may pose a threat your organization or your consumers. If you do not take due care before hiring a new employee and an injurious incident occurs, your company could potentially be subject to charges of negligent hiring or negligent retention.

Federal law prohibits convicted felons from working with financial and security-oriented transactions. And some state laws also regulate restrictions for convicted criminals working with certain types of information. For example, in Oregon, a recent state law prohibits a person from being employed by a mortgage banker or broker as a loan originator if the person has been convicted of any category of crime specified by the Department of Consumer and Business Services. The law requires companies to conduct criminal record checks on job applicants for these positions.

To demonstrate due diligence you must be able to prove you took action to ensure and verify you put trustworthy individuals into trusted positions, and that you took steps to identify the restless stirrings of any current personnel that indicate they may be abusing their positions of trust and engaging in activities that could damage your company or customers. You need to establish practices to show you then subsequently take the appropriate actions.

How do you keep from putting people who shouldn't be trusted into trusted positions? There are many activities you can consider. Some of these may not be allowable by your state or country data protection laws. Some may not be allowable by your union requirements. You need to discuss with Human Resources and your legal counsel to determine what you can and cannot do; these are just some thoughts to get you started. However, doing nothing should not be an option.

- Implement policies and procedures. Establish, formally document and consistently follow policies and procedures for training and monitoring persons in positions of trust, for establishing access controls for these positions, and for performing background, criminal and financial checks on potential employees, contractors and business partners who will have access to sensitive and personally identifiable information. Create a formally documented policy describing how your organization performs and uses criminal background checks and communicate it to all personnel. Periodically run such checks on personnel in trusted positions, such as systems administrators and information security administrators. A July 2005 Employers Mutual Protection Service study reported 3.98% of job applicants screened had a criminal record, 21.57% had a financial record, 4.34% had bogus qualifications and 23.8% of drivers licenses checked did not exist. A 2003 ADP Employer Services review of 3.8 million background checks revealed 10% of employee resumes contain bogus information for significant "facts".

- Check for lawsuits and criminal convictions. Ask individuals you are considering for trusted positions if they have ever been convicted of a crime, as well as ask them to provide their signature to indicate their understanding of the question, and that they will face disciplinary action possibly including termination and legal action if they are found to not be honest with their disclosure. Sure, bad-to-the-bone criminals will probably lie. But if they have signed such an agreement it will help to provide evidence that you were following due care measures not to place, for example, a convicted financial criminal into a position with access to financial records. Then, perform your criminal check.

  Note that some states have industry exceptions regarding arrest information. In at least 12 states the time period for a consumer-reporting agency to report conviction information is limited to seven years, with exceptions, and any earlier criminal record cannot be a factor in a hiring decision. Check with your legal counsel and Human Resources area about these issues before taking actions. Even if the conviction is within the time frame, there may be legal constraints on how you use that information. Generally courts have held that an employer may not lawfully deny employment or discharge an employee because of a criminal conviction unless the conviction is related to the job for which the applicant is applying or which the person already holds. When hiring for a position with access to trade secrets or customer lists, consider checking for lawsuits involving breach of restrictive covenants or non-disclosure agreements. An important note regarding this; performing some of these criminal, background and financial checks may be against data protection laws in some countries. Also, such checks may not be possible in some countries because of the lack of records for such activities.

- Provide training and awareness. A good employee education program is critical and necessary to ensure personnel know and understand what is expected of them while they are performing their job responsibilities, what is considered ethically right and wrong behavior with regard to handling personal and sensitive information and what they should do if they suspect something inappropriate internal activities are taking place. Make sure your personnel, including contracted, temporary and business partner staff, know your policies and procedures. Let your employee candidates know your expectations for security and privacy, and the additional requirements for positions of trust. If you regularly and consistently let people know what they need to do with regard to information security, they will know information security is a concern of your company, and they will be less tempted to make bad decisions or try to get away with fraudulent activity.

- Do not give one person all power. Do not place all security or administrative capabilities for a system, application or process into the hands of one person. Many security incidents were enabled because there was just one person put into a key position of trust. This can create one critical point of failure for your business if that person decides to take advantage of this great empowerment, or if the person just does something incredibly stupid.

- Monitoring. Of course there are many privacy issues and regulations related to the wide range of monitoring possible. Formally document policies that explicitly communicate to your personnel the types of monitoring you do, and whom they can speak with if they have any concerns.

- Statements of understanding. Ask employees to regularly sign statements of understanding that indicate they agree to follow your organization's policies and procedures. There is a great psychological impact when you physically put your signature on the line. Their agreement to follow the rules goes from a conceptual idea to being a concrete binding contract.

- Check driving records. Some employment experts recommend you check driving records when doing background investigations. Even if the job does not require driving, the driving records provide great insight into a person's character. DUIs, drug possession charges, several tickets or accidents, a current warrant, or failure to appear in court could be an indication of potential job performance problems down the road.

- Credit reports. Consider using credit reports when for financial positions. Credit reports can help determine the reliability of any employee who has access to financial information or cash. Note employers cannot discriminate against applicants who have filed for bankruptcy.

- Check third party employees. What would be the potential ramifications of outsourcing a critical business process, perhaps your help desk function, or your operating systems administration, to an organization that employed one of your previously terminated employees? Your company could become a sitting goose waiting for the disgruntled former employee to wreak havoc. What if the third party did no checks on their personnel in trusted positions? Your customer information could be handled and misused by someone working behind bars serving jail time for financial fraud (this has happened).

These will be good conversation starters with your legal counsel and Human Resources representatives. Their expertise insights and expertise will help you to discover more ways to help establish the controls and policies that best fit your organization and your positions of trust. There are definitely EEOC and FCRA issues to consider, along with other state and local regulations and union contracts.

Trust but verify. Apply these practices to your own position; most of you reading this are in positions of significant trust. Demonstrate that these are important measures to take to help incorporate a culture of security within your staff, and to stave off the sharks. You cannot successfully manage a security program by haphazardly and blindly taking leaps of faith when making your security decisions. You must consider the consequences of your decisions, the regulatory requirements governing your decisions, document your decisions, and then act accordingly. This concept also applies to putting personnel into positions of trust without doing adequate due diligence. The possible negative

business consequences of hiring sharks for your trusted positions not only include loss of customers, brand damage and stock devaluation; their inappropriate actions could send you sliding right out of business. When managing information security, don't fling yourself down your six-story security slide with your eyes shut, and find you've bounced and landed in a dangerous pool of hungry sharks!

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.

