
The impact of layoffs on business security

By jgriffin

Published: Apr 20 2009 - 12:04pm

Subtitle: Security experts discuss keeping companies safe during times of financial turmoilByline:

By Joel Griffin, assistant editor

As the economic downturn continues to take its toll on the marketplace, more and more businesses are being forced with the difficult decision of slashing jobs to help keep the company afloat. In fact, since the recession began in December 2007, the economy has shed more than four million jobs, according to the U.S. Bureau of Labor Statistics.

Though most business decision makers' attention is focused on getting through these tough economic times, security experts say that they need to be wary of employees, who fearful that their jobs could be on the cutting block, could take actions that potentially jeopardize the physical and logistical security of the company.

According to a recent joint survey conducted by information management research firm the Ponemon Institute and software security developer Symantec, nearly 60 percent of people, who had recently left or lost their jobs, admitted to taking confidential company information. Of the nearly 950 people surveyed, 53 percent said they downloaded the information, which ranged from client contact lists to employer records, onto a CD or DVD, while 42 percent admitted to transferring the information to a USB drive.

In addition to restricting an employee's means to steal or corrupt company data, security consultant Brian Baker, who has nearly 20 years experience in the private security industry, said that it's also important to impede a worker's access to sensitive files.

"I've learned that there are few secrets in any business and that once rumors begin to circulate regarding a layoff or termination, many of the social controls and company policies are disregarded. While this may involve additional work or temporary expense, passwords and access levels should be modified as soon as the rumor mill provides clue that trouble is coming," he said. Baker added that a business may also want to consider bringing in a third party to help evaluate its IT vulnerabilities.

"The use of an IT security consultant to assist with added security and evaluation is important and by all means, files should be backed up," Baker said. "I knew of a college that was experiencing a turnover event and it was common knowledge that the computer files of instructors were only backed up for 32 hours until the small memory banks were over written. There were no safeguards or warning signs in place to detect any kind of data dump by disgruntled employees. Proprietary educational files were downloaded and then replaced with worthless jpeg files. Nothing suspicious was indicated because the overall instructors' file sizes remained consistent."

Protecting proprietary information

Yet another potential danger that businesses and their security personnel have to be ready for as it pertains to data security are cyber attacks. Often times computer savvy employees can disrupt the operations of an employer by simply downloading files infected with viruses or spyware.

“Let’s say you’re concerned about a virus, you can have your anti-virus software up to date and not just for your employees that are working in the office, but any of your mobile employees who may have laptops or perhaps executives that work at home, because those systems can be compromised if they’re not fully protected,” said Jim Kelton, managing principal of IT security audit firm Altius Information Technologies. “You also want to make sure that those systems have firewalls in place. For a laptop, that’s probably a software firewall, if it’s an organization with servers, you’re more likely to have a hardware firewall that can help reduce your risks.”

Kelton added that checklists need to be made to remove former employee’s usernames and passwords from company networks and to confiscate any handbooks or other materials that may detail how to access company systems.

Felix Nater, president and owner of security management consulting firm Nater Associates, said that companies need to be proactive in protecting their proprietary data by having plans in place that reduce the risk that they could be irreparably harmed by a disgruntled employee. Even something as mundane as an iPod can pose a substantial risk when it’s in the possession of a person with the right know how.

“Do not allow employees, to bring into the workplace, the USB flash drives that have the capability to download significant amounts of data from your systems, whether you’re a small company, a mid-sized company or a large company. Do not allow them to have high capacity iPods. While most employees wouldn’t resort to that type of behavior, when there is impending loss of a job... people are thinking that way. How do I boost my marketability?”

As companies have merged more of their operations into IT departments, the more vulnerable they have become to these sorts of threats, according to Kelton, who says that the most important step in protecting a company’s IT assets is to perform a risk assessment to identify security vulnerabilities. Another issue that must be taken into consideration when talking about IT security is information the company needs to safeguard as it pertains to state and federal laws.

“Everyone is concerned about security and protecting sensitive information right now and a lot of laws have been made and many organizations aren’t even aware. The state of California has 78 privacy laws and most organizations aren’t aware that they’re probably violating a lot of them already,” he said. “So first, take a step back, see what government is saying needs to be done for that specific industry... and then from there start to build in security structures that protect against different threats from bad information.”

Physical Security

Although unlikely, security personnel at companies must also be prepared for a worst case scenario in which an employee turns violent and takes out his or her anger over their job situation on

management or fellow co-workers. As recent events have shown, there are those who will seek vengeance against a company for perceived wrongs perpetrated against them.

“One of the issues that an employer has to take into account is the potential for a disgruntled employee that is being terminated that could turn into a workplace violence situation. The employer has to work out a process with HR and the department heads that they need to involve security in that particular meeting or meetings where security would be in a position to react to any type of violence,” said Gee Cospers, a former Secret Service Agent, who is now president and CEO of security consulting firm Gee Cospers & Associates. “But there’s got to be some sort of a process as to one; locking the person out of any IT or passwords or card access simultaneously; number two, when the employee is being terminated, to have security close by to respond to any type of disgruntled employee’s actions; and then number three, to have a process where the employee is taken back to their desk where they can get their personal items in the presence of security and security can then escort them to their car.”

According to Baker, there may also be reason for many company executives to fear for their safety considering the fervor that has been created in the media about dwindling economic conditions and the perception of the role that management at many organizations have played in it.

“Executives should never dismiss the potential for retaliation, particularly if the wealth gap is great between executive and worker. Criminology teaches about frustration and anger and the lack of control people feel in very strong persistent stress such as a layoff,” he said. “Executive residences and family security should be taken into account because revenge is a possibility.”

Preventing problems before they start

Despite the challenges posed by the aforementioned security issues, there are steps that companies can take to ensure that they don’t become victimized by their employees during these tough times.

Perhaps the most important step, according to security experts, aside from not letting employees know that job cuts are coming, is having a plan in place and conducting risk assessments well in advance of any impending layoffs to safeguard the organization from retribution.

“There has to be a tenaciously coordinated effort (by the company) behind the scenes,” Nater said. “There needs to be a lot of vigilance on the part of the company to make sure that they institute procedures way before they begin to (layoff) employees so they can be adequately prepared in these difficult times.”

Nater also encourages organizations to regularly review and update their security policies collectively across all departments within a company. Experts say a mistake many companies make in regards to security planning is treating the security department as an entity that’s separate from the entire organization.

“There’s got to be a partnership between HR and security as to any termination process, whether it’s for one employee or for many. And security has got to be involved with, one, the planning process, as well as the execution of the plan to facilitate the employees that are being let go,” Cospers said. “That specifically requires HR to provide security with the times and dates that certain employees are being

let go and where that termination is going to take place. You've also got to have a process where security is given a list of people and photographs of people who are no longer employed by the company so there's a check off at the main door or the lobby of the company so security won't admit a familiar face."

Baker echoed Cospers' sentiments and added that non-cooperation between HR and security could lead to even more costly problems in the future.

"Companies need to find a definition of security that fits the nature of their operation. Such definitions can be a feeling of safety, an atmosphere of comfort, freedom from anxiety and fear, or convenience without risk of harm or loss," he said. "The HR staff should be educated in workplace violence topics, just as the security department should be educated in HR law and psychology. If staffers from either department are too narrow minded to cooperate, then the objectives of the corporate mission are in jeopardy and the atmosphere is ripe for a negligent security lawsuit should violence proceed."

In regards to physical security at a company that may be hemorrhaging money, experts say while it's not feasible to implement state of the art security and surveillance systems, organizations should still take adequate steps to secure their facilities.

"A solid kick to a weak door will get most people inside a facility if they are so motivated. Good lighting, observant and professional security personnel, and solid correction to physical vulnerabilities are key," Baker said. "We can't alarm every door inside a bankrupt corporate headquarters and we can't nail the doors shut either. It will be critical to have cooperation of the property manager if it is a leased facility."

Perhaps, the last and most fundamental step an organization can take to secure itself during a period of layoffs is to treat its employees with dignity and respect on their way out the door, according to Baker.

"I recently shopped at a closing Circuit City store. There were numerous employees who stood around and goofed off and acted crudely. Customers would approach them for customer service and they would laugh and reply to the customer, 'Hey open the case and take what you want, they aren't telling us anything cause they think we will steal so just take the product up front and talk to them.' The floor personnel were regular store employees and the personnel along the walls and at the front were temporary staff and corporate management to oversee the operation," he said. "I talked to some of these workers privately and they alluded that while they were paid and employed till the bitter end, and then were not treated respectfully. There is a halfway point demonstrated in this store closing. If you could treat the employee with respect during prosperity, you could treat them respectfully during despair. Controls are important but when a corporation throws the corporate family love out the window during the funeral, it's hard not to empathize with the angry employee."

Source:

SecurityInfoWatch.com

Article Date: Apr 20 2009 Top Story?: Yes Live Date: Apr 20 2009 Expiry Date: Apr 18 2019