The Unchecked Power of the Senior Most IT Professional
February 15, 2012

Summary:
This paper explores the complex issue of terminating the most senior IT professional, such as a CIO, CTO or Director of IT, and what can go wrong and methods can be taken to contain the risk. Most company data is stored electronically, the senior IT professional holds an unmatched amount of power over all of the digital information, including passwords, intellectual property, client information, financial records, and sources of capital.

The Unchecked Power of the Senior IT Professional

The Senior Most IT Professional has an atypical power structure that differs from any other professional in his or her class. The CEO is constantly scrutinized by the shareholders, the CFO is overseen by a 3rd party audit committee, and the COO is under frequent discussions with the CFO and CEO. The cross-skillset within these directors leads to an inherent system of checks and balances. This works well because their responsibilities and actions are generally understood by the other board members; for example, the CEO may have once been a CFO or COO. In contrast to these closely monitored positions, comprehending the technical actions of the CIO requires considerable experience and training in computer systems, which more business-minded executives rarely possess. To address this otherwise unchecked power, financial institutions often enlist an independent party to perform scans and checks on the network. According to the Sarbanes-Oxley Act (SoX) of 2002, publicly traded companies must pass 3rd party IT compliance audits to provide documentation ensuring that their IT systems and the information that they contain are reliable, verifiable, and secure. The private companies that do not and are not required to perform such audits run the risk of misappropriated sensitive information, such as customer data or intellectual property; or worse, having their entire system sabotaged by a hostile employee. Additionally, public companies that do adhere to semi-annual quarterly inspections are still vulnerable to an internal breach by the CIO.

During an IT compliance audit, the firm in charge of assessing the network runs security compliance programs, such as QualysGuard and Nessus Security Scanners, to scan for keyloggers, spyware, and backdoors, which are malware that has become increasingly cheap to install. However, in most scenarios, it is the senior most IT professional who hires these computer forensic technicians, and therefore, he or she can easily conceal any illegal and/or malicious mechanisms and reinstate them after the IT auditors leave. This arrangement places the senior most IT professional in an extremely powerful position where he or she is always in control of the company's information without ever reporting to a higher authority who can properly and frequently evaluate any criminal activity. Even when a the senior most IT professional is being terminated, he or she knows exactly when the IT audits are, how often they occur, and what they comprise, including their limitations and flaws; additionally, the senior most IT professional has access to all electronic information of the company, from hardware to software. Therefore, between the investigation and his or her last day of work, the senior most IT professional can easily divert company information. A process that can take as little as an hour, knowing all the while that the next check would not occur for "X"amount of time. After which he or she may have already sold the intellectual property, stolen the customer data, rerouted company funds (all finances are now IT-centric), wrecked havoc

on the network, or installed silent, remotely activated, destructive software to do any of the above at a later point in time when he or she would be out of suspicion.

A CIO Gone Bad

Mr. Smith, the owner of a rapidly expanding parking garage venture, first noticed that something was amiss when he noticed an unforeseen increase in customer grievances. The complaints ranged from mild concern to open outrage, but all of the callers shared a similar gripe – that the company was charging their credit cards more than they had previously authorized in parking fees. The claims were numerous; however, the excess charge never exceeded more than 1.23% of the owed amount. This strange trend alarmed Mr. Smith and, recognizing his lack of technical tools and know-how to examine the situation further, he hired the computer forensics experts at McCann Investigations to conduct a full-scale inspection of the network. At first glance, the situation seemed obvious – one of the computers that belonged to an IT staff member was hosting a virtual server that was harvesting credit card information off of one of the parking payment machines. However, had the inspectors not conducted a comprehensive scan of the network and forensically imaged all of the computers of the technical personnel, they would not have found the real culprit – the Chief Information Officer (CIO), who had remote access to the liable computer from his computer, was diverting upwards of $300,000 in mini-transactions into his personal bank account. Had these extra measures not been taken, the wrong person would have been fired and likely prosecuted, while the wrongdoer would not only walk free but also keep his position at the company, where, because he was the CIO and thus lacked a technical supervisor, he would have been able to continue to access personal data and steal from unwitting customers.

Profile of a IT Director "Gone Bad"

The IT Director of the Houston-based paper company D.M. knew that his days at the company were limited. He had been reprimanded more than a few times for not completing projects on time or at all, the general state among his subordinates was one of discomfort and turmoil, and he had recently been charged with sexual harassment against multiple other employees. He had always felt underappreciated by the company, and now, he felt, was the perfect time to "get them back". Not only did he set up bugs within the system that could compromise the security of the network and destroy sensitive customer and company information, but he planned it such that the damage would not be immediate; he would be out of suspicion and long gone by the time any misconduct was suspected. D.M., a private company, did not have regular, scheduled IT audits; therefore, the IT Director had thought with relative certainty that the bugs would not be found. However, luckily for D.M., the CEO hired the computer forensic experts at McCann Investigations, who not only found the vulnerabilities but also were able to find enough evidence to link the damage to the IT Director in court.

Compared to a CEO or COO, an IT Director is a typically more introverted and internalized person who is more comfortable with technology than with people.

Therefore, when a IT Director reacts unreasonably after being terminated from a company or when pushed to a crisis point, the response is less likely to be verbal or external, but it instead manifests in destructive schemes against the perpetrating individual or company. For example, some IT Directors may feel a pride of authorship of the company's computer code and, considering it their own, may leave the company only after acquiring a copy of the intellectual property.

The Computer Forensic Investigation

So you want to terminate your senior most IT professional, but you suspect that he or she will respond inappropriately to the decision and lash back against the company? You want to enlist the help of experienced forensic investigators, but what exactly are the responsibilities of such technicians?

For McCann Investigations, the steps of the investigation have been refined through years of experience. First, the forensic experts meet with the CEO and board to discuss the issue and to gain an understanding of the the most senior IT professional personality and t his or her capabilities. The investigators identify the issue and develop a plan quickly, all the while aware that the lines of communication may not be secure (for example, in many cases, the most senior IT professional has access to all company email accounts). The next few steps must be taken swiftly so that the the most senior IT professional does not have time to hide or destroy any incriminating evidence on the networks: first, the investigators lock the the most senior IT professional out of the network by destroying his or her access codes and by changing all of his or her passwords; then, they forensically image the the most senior IT professional computer and all of the computers of the IT staff. Having the tools to perform a proper imaging is crucial in a computer forensics investigation because if the situation escalated to court, the prosecutor would need to be able to prove that, for example, a week before being fired, the most senior IT professional downloaded company information to his personal USB drive, especially if the company wanted to repossess the information. Additional measures taken by the computer forensic technicians include performing internal and external scans, resetting company passwords, and reviewing the security of the network (for instance, if the most senior IT professional had set up a personal VPN for remote access to company data). Also, line-by-line code review is, at times, necessary to completely rule out malicious code in the company's software.

Say that the computer forensics technicians found a keylogger in the system or found evidence of intellectual data theft that puts the most senior IT professional under suspicion; unfortunately, without any direct tie to the theft, the most senior IT professional cannot be prosecuted and forced to return the information. This is where traditional PI work comes into play and why it is necessary for the investigator to possess not only digital forensic experience but also that of an on-the-scene private investigator. In the case of a keylogger, the next step is relatively simple – broadcast false information on the computer to prompt a misstep by the culprit; however,

determining intellectual theft requires greater involvement by the investigator. A possible method of catching the offender is by approaching him or her outside of the company environment and, while wearing an audio device, getting the most senior IT professional with the idea of funding for the technology that "they developed". If the conspiracy is with multiple other employees, it is the job of the investigator to dynamically look at relationships and to follow the path to the perpetrators.

Choosing a Forensic Investigator

The motivation behind enlisting somebody who is both a certified forensic examiner and a licensed private investigator is because if wrongdoing by the CIO is discovered, proper documentation and court testimony is needed to substantiate the findings. In a recent case of intellectual property theft in a company in Houston, the investigators at McCann needed to prove in a black-or-white fashion that the data was downloaded to an external drive and then the drive was removed from the computer. The report must not only show that the investigation was performed in a forensically sound manner, but also that a proper chain of custody of the evidence was maintained; otherwise, the entire investigation would have been for naught.

There are three basic requirements to consider when choosing a firm to investigate your CIO:

1. Scanning – having the technology to run a network scan, perform a Qualys search for security holes, and to perform an IT internal and external vulnerability assessment.
2. Forensic Experience – having skills in imaging, digital forensics, and knowing how to forensically evaluate a network to see if anything is amiss (for example, code review). Even if the scans have a clean result, there may still be digital bugs or backdoors installed.

Traditional PI work – often times, 24-hour surveillance or undercover work is necessary to obtain direct evidence of the CIO's wrongdoings.

Identify, Contain, and Mitigate

While not every senior IT professional termination results in the IT professional reacting in a malicious manner against the company, the unmatched power of the position can potentially lead to the collapse of the company if not checked. A forensic investigation allows the company and its employees to continue to move forward without fear.