McCann
INVESTIGATIONS
Information | Insight | Influence

Case Study: Hiring a licensed Security Provider

Company Profile

McCann Investigations is a full service private investigation firm providing complete case solutions by employing cutting-edge computer forensics and traditional private investigative tools and techniques. For 25 years, McCann's investigators have worked in the public and private sector encompassing law enforcement, physical and electronic security and computer forensics.

McCann works with law firms, financial firms, private and public companies and individuals in cases including contentious divorce, child custody issues, fraud, embezzlement, spyware/malware detection, civil and criminal background investigations, and due diligence.

McCann Investigations tools include:

- Computer Forensics
- Mobile Device Forensics
- Spyware/Malware Detection
- Network Breach Detection
- Digital Debugging
- IT Network Vulnerability Assessments
- Background Investigations
- Under Cover Work
- Surveillance
- Corporate Intelligence
- E-Discovery

Hiring a Licensed IT Security Professional

Licensed security IT professionals don't really exist. There is no licensing or regulatory body for IT security professionals. They can have certifications and security designations such as CISSP or CISP. However, there is no licensing requirement and really no barrier to entry. Regardless of the fact that these individuals can have access to a company's IT network, they are not required by law to have a criminal background check. This becomes problematic when IT security companies begin subcontracting out labor for IT security projects. Often an employee of a company will have a basic background check run at the date of hire. A subcontractor often has no standard background investigations done by whoever has hired them. This can be problematic if the subcontractor has any malicious intent. With access to a company's network, it would be easy to build a backdoor into the network to access sensitive client information such as credit card and banking information as well as social security numbers and home addresses. Intellectual property and other proprietary data could be compromised. A serious data breach not only can affect a company financially, but also can greatly damage a company's reputation. When customers and clients do not feel that their data is safe, they may choose to not do business with that company.

These situations are more likely to arise with the small to medium sized company who simply does not have the budget to hire a national IT security company to work with their IT audit or incident response teams. A national company has employees rather than subcontracting which helps to ensure that backgrounds have been performed. A smaller local IT Security company subcontracting out their IT security personnel may not know who they are really working with. Hackers will often have day jobs as IT security professionals. A company that specializes in computer forensics will also have expertise in IT security. Because computer forensics examiners provide expert witness testimony in court cases, they are required to be licensed by the state. State licensing requires an FBI background check to ensure that those who are licensed do not have criminal backgrounds.

Client Situation

McCann Investigation was contracted by a small ecommerce company. The company discovered anomalies in its network indicating a possible data breach. As a small company, rather than have their own in-house IT personnel, the outsourced their IT support. Because the company wished to have a third party examination of their network, they chose to have an incident response team that was independent of its IT company. McCann Investigators are licensed by the state of Texas as private investigators. All of its computer forensics experts are licensed by the state of Texas which requires finger printing and an FBI background check.

McCann Investigators met with the client at their offices to assess security concerns. Interviews were conducted with several employees in order to:

1. Gain an understanding of the existing network and pc security
2. Gather background information about the suspicious incident
3. Determine who was possibly involved in the incident
4. Prioritize the media to be imaged and analyzed.

McCann Investigators were provided electronic media by the client that was to be imaged and analyzed. The media included:

1. Computer hard drives
2. USB flash drives
3. User directories from 2 server shares (these were documented and copied)
4. Recovered deleted files from the forensic image files
5. Extracted email files in PST and OST formats from the forensic images

Technical Situation

After the initial meetings with the client employees to assess the situation, McCann Investigators formulated a plan to begin the investigation to determine and document the source of the data breach. McCann moved forward with the following:

1. Recovery and extraction of active and deleted internet history
2. Recover, extraction and analysis of Windows Registry Hives and Event Log files
3. Searches for credit card and social security numbers

The computer forensics examiner performed the initial analysis of the files and the Windows registry hive files were examined. Most recently used entries from the registry were noted as suspicious and the user settings were noted. Examination of the windows registry hive files noted anomalous files. The hard drive images were then searched for the notable files that were found. In addition, OST files were converted to PST files for search and analysis.

In addition to analyzing the Window registry hive files, the computer forensics examiner also extracted the internet search history from the file. Notable search phrases included

1. “how do ATM cameras work”
2. “credit card black market”
3. “how do hackers sell credit card numbers”

At first pass, it appeared that the source of the network breach was being orchestrated by a person in the accounting department. However, further investigation revealed that the actual perpetrator was an IT person who was contracted by the company’s outsourced IT support company. A background investigation of the individual revealed a previous record of check and credit card fraud.

Documentation of the incident is key to making a case in court. Throughout the remediation process, McCann carefully documented and recorded everything. McCann Investigations provided the client with detailed reports and analysis of the data breach detailing every step that was taken to determine the source and depth of the intrusion into the company's network, as well as documentation the loss of data. Documentation of the data by a licensed computer forensics examiner assisted the company in making a legal case against the perpetrator.

Solutions

Once McCann completed its initial investigation of the incident, McCann worked with the client's IT personnel to mediate the data breach by identifying any other possible vulnerability. McCann Investigations began an IT security audit in order to put security protocols in place to prevent future network breaches. McCann Investigators collected a list of assets owned by the company that should be included in the IT security audit. This included:

1. Computers and laptops
2. Routers and network equipment
3. Web servers
4. Printers
5. Data such as sales, company and employee information
6. Company smart phones
7. VOIP phones
8. Email accounts
9. Web pages
10. Employee access control

Once all of the company assets were determined, McCann Investigators scanned the company network to determine threats and vulnerability and to ensure that there were no further access points for intrusions. McCann formulated IT security protocol to protect the company's data. This protocol included:

1. Implementing intrusion prevention system
2. Identity and access management systems
3. Implementing network access control
4. Creating on and off-site data back-ups
5. Email encryption protocols
6. Training of employees in IT security protocol

Products and Services Used:

- Computer Forensics Examiner – Licensed Private Investigator in the State of Texas with certification in computer forensics.
- EnCase, a Guidance Software – Leading software application to forensically image computers.

Conclusion:

Because there are no licensing requirements or barrier to entry to becoming an IT Security professional, there is always the threat of allowing personnel who have not have a basic background check into a company's network system. IT security professionals have security designations and certifications, but these designations do not require any background investigations. An IT company that is subcontracting IT professionals may not have run proper background checks. Hackers often have day jobs as IT security personnel. A data breach can cause not only financial loss, but can cause damage to a company's reputation. Customers who do not feel that their data is safe with a company, may take their business elsewhere for fear of their information being compromised. The company must not only formulate a strategy to recover from the intrusion into their system, but also a strategy for recovering customers and mitigating the brand loss. Using a company whose IT professionals have background in computer forensics ensures that the individual has had an FBI background check.