CyberSecurity | Data Breach | Incident Response

The following descriptions highlight a variety of matters for which Vestige has been retained that involve CyberSecurity incidents, breaches and alleged computer hacking. Each of these cases are real matters that we have worked, but for privacy and confidentiality purposes the relevant information has been sanitized. These cases are not the entire population of cases matching such criteria, but instead represent a wide sample of the cases we have worked in this specific area. Should you need additional information, please contact us.

Financial Services Firm | **Data Privacy Breach**

Vestige was engaged by a new client when they were notified by one of their customers that some of the customer's Personally Identifiable Information (PII) was discovered during a routine Google search. The Financial Services firm verified that proprietary, private data appearing to originate from itself was in fact being indexed by Google and still available by following the Google search link. The initial assessment by the Financial Services firm was that 3.5 million records were likely breached, but they did not know how. Vestige's Rapid Response Team swung into motion, forensically preserving the affected infrastructure, forensically analyzing the memory and storage of the organization and successfully identifying the attack vector. Vestige worked with the company's InfoSec individuals to ensure that the attack vector was removed, identified and cleared any additional back-door entry points and then worked hand-in-hand with the Financial Services legal team to turn attention to other major aspects of a Breach Response. At the forefront of this was identifying which records had been (or were likely) compromised to coordinate notification efforts. Through our forensic analysis we were able to prove that a large fraction of the records (all but 60,000 records out of 3,500,000+) were actually compromised and further to show that of the 60,000 records, only 11,000 contained PII necessitating notification. A matter that could have resulted in significant impact – including putting the Financial Services firm out-of-business, while still costly for the organization, ended up being a fraction of the cost because Vestige was able to Forensically prove what data had and had not been compromised.

Manufacturer's Systems Used for **Downstream Attack**

A long-standing client of Vestige's on our Internal Investigations, Employment Relations and Non-Compete/IP Theft matters was notified by the FBI that their environment had been compromised and used in an attack against an unwitting victim. The Manufacturer's large IT Department was able to isolate the potential system to roughly 80 devices, but could not identify any further information about the compromise. Vestige was engaged to analyze the environment, determine what forensic evidence existed to narrow the attack down and to determine the source of the attack. Within a few days, Vestige was able to identify the compromised systems. Upon forensic examination of the infected systems we identified the initial attack vector and provided the Manufacturer with the relevant Indicators of Compromise (IOC) that allowed them to search thousands of their other systems to identify if any other systems were infected with the same malware that lay dormant.

Manufacturer Discovers **All Users Have Administrator Access**

This new client contacted us when it was discovered that their entire user base of 3000+ employees had "Enterprise Administrator" rights to their entire computing environment. Working with Microsoft, the client identified that the Authenticated User group had been added to the Enterprise Administrator group – but it was unclear When, How, Why, Who and for What purpose this may have been done. The client's IT department of some 25 individuals shared varying degrees of Administrator access and it was unclear whether this was an accidental change in permissions or if this was an internal/external attack. To complicate matters, this organization ran a predominantly decentralized IT environment, with over a dozen data centers around the continent. IT provided a number of possible explanations and falsely believed they were following the right trail. Vestige forensically analyzed their environment, identified appropriate source systems that were in the environment at the time that the change had occurred and followed the evidence to identify Ground Zero for the change. By ignoring the IT Department's hunches and following the trail that the evidence laid out, within several days Vestige identified which data center had initiated the change that was rolled out to the entire enterprise. We determined the date for which this occurred (some 90+ days prior to the initial discovery of the issue by the client) and were able to identify the specific manner in which the change had been made. We were further able to narrow it down to a significantly small enough group of people that the organization was able to identify who made the change, confirm that it was accidental and resolve the issue moving forward.

Former Employee | **"Time Bomb" Threat or False Fear**

In this matter an employee was terminated by his employer. This individual worked as a network engineer and had a troubled past. After being terminated, the individual began shopping for a job and used a recruiter to aid in the process. The recruiter successfully landed him a new job. While working for his new employer, the same individual began bragging to some of his fellow co-workers of his mastery of computer hacking. The individual further claimed he had placed multiple "time bombs" on his former employer's computer systems. Word began to spread of these claims in his current department. Upper management decided they no longer wanted the individual and talked to the original recruiter. Upper management also requested that the recruiter notify the former employer of these claims. Ironically, the former employer was having system problems and became suspicious that the "time bomb" claims by the individual were legitimate. Vestige investigated the issues and found out the former employer had not implemented any "time bombs" on their system. The problems experienced by the former employer were actually due to the deterioration of their system infrastructure. Vestige was able to extinguish the former employer's fears and suggested a redesign of their infrastructure, advised on the importance of separation of duties and referred the former employer to a competent networking company to solve their systemic issues.

Former Employee v Manufacturing Company | **Wrongful Termination**

A former employee filed a wrongful termination suit against a manufacturing company seeking $10 million in damages for relief. The former employee was employed by the manufacturer in a sales capacity for only 53 days. The company had terminated the individual for lack of results and inappropriate use of time and resources. In the middle of the case, immediately following the deposition of the former employee, the company's e-mail system became the target of a hack-in. Flagrant, over-the-top, non-believable statements that were harmful to the manufacturer were fabricated by the attacker. Vestige was engaged to determine the identity of the hacker. The source of the attack was traced back to an individual retail center of Kinko's whereby the surveillance video exposed the identity of the hacker as the Plaintiff in the current lawsuit. Upon presentation of this information, the wrongful-termination suit was dismissed with prejudice and the present Plaintiff was sanctioned with the defense's expert fees and attorney fees for the entire suit.

CEO v Former Employee | **Defamatory E-mail**

The CEO of a business services company, along with approximately thirty other individuals, received an extremely defamatory e-mail about said CEO. The defamatory e-mail was sent to the CEO's management team, family members, board members and trustees of other businesses with whom the CEO was affiliated. At the time of the incident, there were no suspects or any good leads about the identity of the perpetrator. Vestige was engaged to identify the individual. After working with several ISP's to identify the subscriber, it was revealed that the individual in question was a former employee that had left on bad terms approximately five years prior. Upon filing suit, the Defendant (the former employee) denied all allegations. The court appointed Vestige as special master to conduct a forensic examination of the Defendant's home computers. The former employee happened to be a seasoned IT professional that ran an internet service company, consisting of four computers and thirty servers, out of his house. Vestige identified the appropriate devices and performed a forensic examination. The examination revealed that not only was the Defendant the author of the defamatory e-mail, but he had taken considerable steps to cover his tracks, including running several pieces of anti-forensic software designed to thwart such investigations. Faced with this evidence, the Defendant quickly settled the libel case. The Defendant was forced to pay attorney fees and expert fees. The former employee was also required to write an apology letter to all the recipients of the defamatory e-mail recanting all the statements.

Mid-size Corporation | **Internal Investigation**

The original owner of the corporation had been reduced to a minority shareholder and was no longer on the Board of Directors; however, the owner continued to have knowledge of what occurred at subsequent Board meetings and would send e-mails with questions related to information exchanged at these meetings. The corporation initiated an internal investigation and hired Vestige after it grew suspicious that information was being leaked out to the original owner by someone on the inside. The corporation suspected that the information was somehow connected to their IT staff member. Vestige performed covert forensic analysis after-hours without IT's knowledge. Vestige not only uncovered that the IT staff member was leaking information, but that this particular IT staff member had a felony record surrounding identity theft. During our investigation, Vestige discovered that this individual's Outlook database had a contact record for everyone in the corporation along with their social security number and other information that would aide in identity theft. Vestige gave a suggestion on how to remove the individual and minimize the IT's access. Vestige used its resources and expertise to stop a small problem from unknowingly becoming a big problem.

Internet Service Provider | **Extortion - Hacker Group**

A high-profiled internet service provider received an anonymous e-mail from an established hacking group. The hacking group attempted to extort money from the ISP by threatening to go public with a successful attack it had performed against the internet service provider. The e-mail contained the identification information of some of the internet service provider's clients as proof of the attack. Vestige was hired to establish the scope of the break-in and assess the damage that was actually suffered. Vestige's analysis revealed that the ISP had an extremely robust perimeter and set of internal security measures with the exception of a lone system that was used for development that had been placed outside the firewall for limited testing purposes. The internet service provider had failed to remove it after the tests were completed. This test machine contained an outdated list of a sampling of the internet service provider's clients' data and was verified as the only source of information that the hacker group had to use for extortion purposes. As a result of Vestige's investigation and ability to show that it was a very limited breach, the internet service provider pre-empted the hacker group from going public by releasing Vestige's report to all of their clients and the press. Vestige's report allowed the ISP to take a potentially damaging situation and reframe it into a positive one.

Subsidiary Infrastructure Intrusion | **Security Analysis**

Vestige was contacted by a subsidiary of a larger organization that did not have its own IT department, but relied on the IT department of the parent company. The subsidiary had been contacted by the FBI to determine its role in a downstream liability matter. The client needed to assess the overall security of its infrastructure and, specifically, two of its web hosting servers. Vestige analyzed the two web servers and log files for the entire infrastructure and pointed out to the client several areas of weakness. Consequently, the client performed a complete overhaul of their system security.

Internet Hosting and Web Development Co | **Financial Data Theft**

An attorney contacted Vestige with a matter regarding a web developing and hosting client. The company was hosting several hundred web sites. They utilized an e-commerce framework for 15 of their customers, one got compromised. The framework was encrypting the data from an encrypted form, passing it from the client to the web server (which was also encrypted), and passing it to the payment gateway provider (in encrypted form as well). They took all the correct steps, however, a hacker got in through a vulnerability and installed his own script between the place where it was received by the e-commerece site and before it was sent to the payment gateway and for a 'fraction of a second' the payment information was decrypted and then re-encrypted for the payment gateway. During that fraction of a second, the hacker's script captured all the information and forwarded it to the hacker in plain text. This data breach went on for 3 months before it was noticed. Luckily it incurred less than 800 transactions and not all of these were compromised. Vestige figured out the vulnerability, discovered the illegally installed script, verified that is was isolated to only the one e-commerce framework customer, determined which transactions were compromised (about 500), and delivered these results to the web company in just 5-7 days.

Customer/Vendor Payment Diversion | **Business Email Compromise (BEC)**

Upon reconciling and closing the books, the financial officer discovered a $107,000 wire transfer that he did not recognize. He contacted the bank almost 35 days after the wire transfer had taken place. The bank provided him the place as to where the money had been wired. A short internal investigation uncovered the fact that an individual in the organization that had access to sending wire transfers had received an email from the CEO with instructions on sending the wire. However, that email did not originate from the CEO, but instead, was from an outside attacker.

Contained within the instructions was enough information that led the financial clerk to believe that it was legitimate. The question became...How did the attacker have legitimate information that appeared they clearly were in on the party's email system? The next question was - which party - the organization or the vendor?

Vestige was engaged to investigate. In reviewing artifacts contained within our clients infrastructure, Vestige hypothesized that the attack was not within our client's infrastructure. That hypothesis, however, needed to be verified.

A comprehensive review of the client's environment confirmed this hypothesis to be true and the client's legal team made contact with the vendor. This triggered a forensic examination of the vendor's systems where it was indeed verified that the outside attacker had infiltrated the organization through the vendor's system.

As a final result, the vendor's cyber liability insurance carrier paid the claim reimbursing our client the full amount.

With Digital Forensics we had the ability to prove where the attack happened and assign accountability.