CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 159 years

THURSDAY, APRIL 24, 2014

Chicago Daily Law Bulletin®

Volume 160, No. 81

Target lessons: Network security, human element are factors in protecting data

Caught off guard by the very public outing in December 2013 of a data breach compromising the credit and debit card numbers of 40 million of its customers and affecting the personal information of 70 million more, Target scrambled to control the situation on multiple fronts, investigating the breach, dealing with panicked customers and managing the mounting public relations crisis.

This is the second of two columns analyzing the Target data breach. The first article first, ("Many lessons for companies to learn after the Target data breach," March 27) looked at Target's missteps in handling the breach. This piece analyzes how and why the breach happened and how Target potentially could have prevented the breach.

The breach took place from Nov. 27 to Dec. 15, 2013. The company later discovered — and was forced to admit — that its security team saw signs of suspicious activity after the hackers entered its network, but the company failed to appreciate the implications of the evidence after investigating it.

Target recently revealed that a "small amount" of the hacker's activity "was logged," but after evaluation, the security team "determined that it did not warrant immediate follow up." That team's judgment gives new meaning to the adage that hindsight is 20-20.

Scamming the system

While the cyber thieves responsible for the Target data breach have yet to be identified, government investigators have been relatively tight-lipped about possible suspects. Commentators have suggested that either Eastern European traffickers in stolen credit card numbers or organized crime groups operating out of the former Soviet Union were responsible for the breach, on the theory that these groups are looking to target companies that maintain large amounts of customer data.

The cyber thieves apparently sell the stolen information in private forums or "carder sites" on the Internet, and such sites are reportedly "incredibly user-friendly," enabling fraudulent use of the stolen credit and debit card numbers.

While the "who" is still unclear, more information has emerged about the "how."

Investigators reportedly have determined that the hackers used a RAM scraper, or "memory parsing software," installed at point-of-sale registers to grab encrypted data by capturing it at the moment when it appeared in readable form. The stolen data was then stored on a Target server commandeered by the hackers until it could be moved to various U.S. staging points, then onto a Moscow-based hosting service.

The hackers gained access to Target's network using credentials stolen from a third-party vendor — not a technology, outsourcing or cloud computing vendor but, rather, a refrigeration and HVAC systems company, Fazio Mechanical Services, based in Sharpsburg, Penn. The HVAC company used the system credentials to manage remotely a number of processes, including electronic billing, contract submission and project management.

While Fazio has denied that its company had remote access to Target's system for monitoring or control of Target's heating, cooling and refrigeration systems, it is a fairly common practice for HVAC companies to be granted network access to clients so they can monitor retail stores and diagnose problems remotely.

The hackers apparently gained the credentials through an elaborate phishing campaign that ensnared Fazio, and probably others, through the use of what has been described as "ubiquitous" malware that hackers employ on a volume basis.

Once the hackers discovered information they had harvested somewhat randomly contained a link to one of the biggest retailers in the country, they had a real and lucrative target in Target.

How the attackers might have parlayed the HVAC company's access credentials for Target's electronic billing, contracts or project-management system into full-blown access to the retailer's IT network and payment processing systems remains the subject of a number of theories — including that Target failed to comply with various security standards, including payment card industry security standards that require retailers to incorporate two-factor authentication for remote network access originating from outside the network by personnel and all third parties.

While security experts who have weighed in on the issue do agree that it is difficult to protect a "vast network" like Target's from this kind of malware because hackers are increasingly sophisticated adversaries who have learned to exploit the less-than-secure American card payment systems, Target reportedly may actually have been better prepared than most retailers for such an attack, yet still failed to detect or prevent it.

Six months before the hackers entered Target's system, the company installed a $1.6 million malware detection tool offered by the computer security firm FireEye. This reportedly "very sophisticated" tool is also used by the CIA, the Pentagon and intelligence agencies around the world to detect security breaches in real time, not after they occur. Target employed a team of security specialists in India to monitor the system 24-7 and report any suspicious activity or FireEye alerts to the company's security operations center in Minneapolis.

On Nov. 30 — just days after the hackers had laid their traps and before any stolen data had been moved from Target's servers to the U.S. staging points — the FireEye system sent the most urgent warning on its graded scale, and the Indian

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a partner in Loeb & Loeb's Chicago office. She focuses on matters involving the convergence of advertising and promotions, emerging media, technology and privacy law as well as intellectual property law. She can be reached on nmcginn@loeb.com.

Even when the best security systems are in place, the people behind those systems can take missteps, exposing the company to PR troubles, financial damages and potential lawsuits.

team escalated the alert to Minneapolis. The security operations center did nothing.

More FireEye warnings came on Dec. 2, and Target missed them, too. Worse yet, the FireEye system has an option to automatically delete malware as it's detected, but for some reason, Target's security team had turned off that function. The security system designed to work seamlessly suffered a breakdown due to human error, and the retailer allowed personally identifiable information from 110 million customers — and sensitive financial information from 40 million customers — to gush out of its mainframes.

It was only after the Department of Justice stepped in that Target took action to find and delete the malware and to launch an internal forensic investigation into the hacking. This new information is bad news for Target, which now is defending as many as 90 class-action lawsuits concerning the breach brought by consumers and financial institutions.

The Senate Commerce Committee, which also is investigating the breach, recently released a report taking the company to task for its many missteps. The committee, chaired by Sen. Jay Rockefeller, D-W.Va., cited a number of critical errors on Target's part that led to the massive data breach, including:

• Giving network access to a third-party vendor that appeared not to be following broadly accepted information security practices, which allowed the cyber-criminals to gain a foothold in Target's network.

• Failing to respond to multiple warnings from the FireEye system that the attackers were installing malware on Target's system.

• Neglecting to properly segregate the company's more sensitive areas of its network, those containing consumer data, allowing the hackers to move easily from the less sensitive areas to which they had access.

Lessons learned

The Target data breach offers several important lessons about protecting your business in light of the real risk of a data security problem. Even when the best security systems are in place, the people behind those systems can take missteps, exposing the company to PR troubles, financial damages and potential lawsuits. To guard against these evils, companies might consider:

• Requiring all third-party vendors to comply with rigorous security measure — both within their own systems and when accessing remotely the companies Internet-connected systems.

• Building a security operations center to monitor IT infrastructure, especially when it stockpiles high-value information.

• Practicing for a "digital disaster" — just like running a fire drill — so that when a security alarm goes off, company personnel follow set process and procedures.

• Developing policies and procedures that provide effective oversight of the security monitoring team.

• Investing in security protections from firms like FireEye, and enabling the automatic malware deletion feature offered by those companies.

• Installing chip-and-pin technology to make point-of-sale transactions more secure.

Even when the best security systems are in place, the people behind those systems can take missteps, exposing the company to PR troubles, financial damages and potential lawsuits.