SERVICING MANAGEMENT®
THE MAGAZINE FOR LOAN SERVICING PROFESSIONALS

*Reprinted with permission from the June 2014 issue*

# No Laughing Matter

## Field services companies take steps to ensure confidential information is secure.

**by Darren Kruk**

The fictional story of Sandy Patterson in the popular 2013 comedy "Identity Thief" poked fun at the trials and tribulations of identity theft - making audiences chuckle and raking in more than $173 million worldwide. The film is about a woman named Diana (played by Melissa McCarthy) who lives in Florida and steals the identity of Sandy (played by Jason Bateman) from Denver.

Diana racks up large credit card bills, gets arrested for an assault in Sandy's name (causing him to be questioned by police) and comes close to destroying Sandy's life. After not getting the results he seeks from law enforcement, Sandy decides to take matters into his own hands and tracks down Diana to turn her into the police. They end up having a hilarious adventure, and everyone lives happily ever after, but in the real world, identity theft and information security breaches are no laughing matter.

According to the U.S. Office of Justice Programs, about 7% of people age 16 or older were victims of identity theft in 2012. Direct and indirect losses from identity theft totaled $24.7 billion that year. Approximately 36% of the victims reported moderate or severe emotional distress as a result. Now imagine the magnitude of a massive security breach at a company and the responsibilities it bears in keeping secure the data entrusted to it by millions of people and consumers.

Everyone can recall the recent data breach Target experienced around the holidays last year. That breach affected the credit card and personal information of 110 million Target shoppers. Since that time, it also has spawned dozens of legal actions and the resignations of Target's top executives, including its chief information officer and CEO.

According to a Feb. 12 post on KrebsOnSecurity, a blog written by Brian Krebs, a former Washington Post reporter who first alerted the public to the initial Target data breach, the breach "began with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer."

It was a malicious email at a vendor's business that caused one of the largest data security breaches in the country's history. It potentially could have been avoided if Target had ensured that information security was a priority, not only internally, but for its vendors as well.

In the mortgage servicing industry, it falls onto field services companies to ensure the security of millions of points of sensitive property data by promoting secure behavior internally and through their vendor networks.

### Promoting secure behavior

Promoting the secure behavior of employees and vendors, rather than relying on awareness alone, is the most important aspect of information security for any business. In the past, businesses have spent millions of dollars on security awareness. But for those programs to be effective, they need to address the behaviors of their biggest asset - their employees and vendors.

While security experts do not like to admit it, they know that a company's biggest asset can also be its weakest point. The old standards are standards only because they are so successful. Why would cybercriminals traverse a maze of elaborate systems and firewalls when all they need to do is send a targeted phishing email to employees or vendors that would trick them into launching a backdoor exploit? Nothing could be easier, and that is why this is still the most prevalent means of attack.

The Information Security Forum released a report in May called "From Promoting Awareness to Embedding Behaviors." The report states that instead of just making people aware of their information security responsibilities and how they need to respond, businesses need to embed positive information security behaviors that become habits and part of the corporate culture.

Field services companies can embrace the message in this report by offering ongoing information security training in topics including fraud prevention, secure coding for developers, phishing and social engineering.

While the security department professionals take advanced training annually and concentrate on security daily,

most employees have other daily duties, and without frequent reinforcement, they are prone to being exploited.

This is why it is necessary to focus on this group and move beyond annual training. Suggestions include monthly newsletters, bulletins, security games and positive reinforcement for following security rules.

There needs to be a belief that information security is a necessity and not just an add-on. It needs to be baked into an organization and its system, not be just a module that is added on afterwards.

Often, security department professionals hear, "What regulations are requiring us to do this?" or "Which client is asking this of us?" The answer is that it doesn't matter. Field services companies must implement security controls because it is the right thing to do, not because a client or regulation is demanding it of them.

### Communication is key

In the information security world, communication trumps all. Hackers communicate and help each other develop better and more efficient techniques of cracking into business systems. That same degree of communication at all levels of the mortgage servicing industry will help to minimize information security risks and prevent data breaches.

In any company, there should be clear and frequent communication not only between departments, but also with employees, clients and vendors. This can take the form of business-to-business calls to discuss operational issues and service-level agreements but also should include communications regarding security issues.

Security departments tend to be secretive, not wanting to divulge issues that exist, but that is exactly what hackers count on. Security departments within field services organizations need to balance the need to protect weaknesses with the benefits of communication. By sharing experiences with employees, clients and vendors, all can benefit and collaborate on building security protocols.

Field services companies need to create and maintain a common forum for their security officers to have these discussions on a frequent basis, without judgment. Only then would those officers be able to share new techniques, trends in the industry, and new threats to assess and adapt to them faster and more efficiently.

### Monitoring, logging, alerting

Knowing what to monitor and log when it comes to information security can often be tricky. The best practice for field services companies in keeping private client and consumer information secure is to identify the confidential information and continually monitor and log it. And, just as importantly, these companies must remember to set up alerts that warn of deviations to the norm.

Many security professionals conduct tests to determine the effectiveness of their company's security programs. They look for ways a hacker can gain entrance into the company's environment and realize that they can never have too much information on where weaknesses have been identified. Companies often remember to secure the servers, network gear and desktop systems but also need to remember to include the printers, faxes, phones, remote access and the industrial control systems (ICSs).

The ICSs tend to be the most forgotten. After all, it is easy to forget that your computer room air conditioner units and uninterruptible power supply systems are attached to the same network, usually via simple network management protocols (SNMP), and are often left with their default passwords and settings. Anything that contains embedded operating systems today can be used as an entry point into your environment.

It is important to recognize and track the shape of the company's data traffic because a change from the norm can indicate a problem. Employees embedded and engrained in information security also need to respond to alerts once they are received.

Effective ways to monitor and log confidential information include the following:

• Asset management: The pillar to protecting sensitive information is having a clear understanding of the company's and clients' assets, their classification, and where and how they are stored. Without understanding what needs to be secured and where it is located, it would be very difficult to protect it. There should be clear definitions of the data types that exist within the company and a matrix identifying the location of them. This is important when dealing with change control approvals. Anyone who has spent hours reviewing changes for approval can attest that knowing what data may be affected by the change can be the difference between an approval and a denial - and the difference between secure data and leaving the company or client open to a potential breach. A variety of changes have been known to be denied simply because the authors of a proposal did not do their due diligence and did not understand that they were manipulating confidential data incorrectly.

• Network intrusion and prevention: Limited access and prevention will keep hackers or unauthorized persons from accessing your environment. A layered approach to information security is the most effective and includes systems such as firewalls, network monitors, anti-denial of service and anti-distributed denial of service, access-lists, virtual local area networks, integrated file integrity monitoring, and host-based intrusion detection systems. Each layer makes it more difficult for an attacker to enter and gives a chance for security professionals to stop and prevent unauthorized access.

• Password protection: Everyone knows the reason for passwords and that they need to be complex and changed frequently. But there is one aspect of passwords that tends to be overlooked, and that is changing the default user accounts and passwords from the defaults. This includes the default iLO passwords, the SNMP strings and remote access modems. Security professionals also need to Google the backdoor passwords and accounts that are created by manufacturers to be able to get into their company's systems to repair possible issues.

In "Identity Thief," Diana made a simple phone call and was able to obtain enough information to steal Sandy's

identity and ruin his financial life. More than 110 million people were left vulnerable to cybercriminals in the 2013 Target security breach. Although one is a fictional movie, the message about the importance of protecting sensitive data remains the same in people's personal lives and in all industries.

Field services companies' security professionals need to keep an open mind and never stop exploring new ways to protect their companies' systems. From creating positive security habits in their employees and vendors, to constant communication and monitoring data transfers, information security programs should never remain stagnant. It is important to keep learning and improving.

Field services companies and their vendor networks are tasked with assuming their clients' posture with respect to data and protecting it as if the fate of the company depends on it. Often, it does. SM

---

Darren Kruk is the information security officer for property preservation and field services firm Safeguard Properties. He can be reached at darren.kruk@safeguardproperties.com.