CYBERCRIME AND THE HEALTHCARE INDUSTRY

Executive Summary

Healthcare professionals are in a tight spot. As administrative technologies like Electronic Health Records (EHRs) and patient and provider portals become standard issue in healthcare organizations, the access to data and information so strongly demanded by patients, providers, payers, and employees is also fast becoming a target of scrutiny and risk.

Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) require healthcare organizations to implement administrative, physical and technical safeguards to ensure the integrity and privacy of patient records and other sensitive medical data. Despite increased protection, healthcare organizations are a target for cybercriminals because of the wealth of personal data they collect that can be monetized. The question is whether regulations alone will be enough to halt the hard reality of a successful cybercriminal network turning its attentions to the healthcare industry.

These breaches can have dire implications for those whose records were breached. According to Javelin Strategy and Research, the correlation between receiving a data breach notification and being a victim of fraud is one in four – significantly up from one in nine that Javelin identified in 2010.[1]

So why is the data that is available in healthcare records so valuable to a cybercriminal?

First, the theft of credit card and account data has a limited lifespan; it is useful only until the victim cancels the card numbers and accounts, whereas the information contained in medical records has much broader utility, can be used to commit multiple types of fraud or identity theft, and does not change, even if compromised.

Second, the value of personal data to a cybercriminal is much higher than a credit card or bank account number. For example, the average selling price for a U.S. credit card in the underground is $1 USD. However when that single card is sold as part of a “fullz,” or full identity profile, the cost increases dramatically to around $500, with health insurance credentials adding an additional $20 each. Health insurance credentials are especially valuable in today’s economy, where skyrocketing healthcare costs are driving some to seek free medical care with these credentials.[2]

1 https://www.javelinstrategy.com/blog/2013/04/28 financial-pain-ensues-when-custodians-of-health-fail-to-be-good-stewards-of-privacy/

2 http://www.darkreading.com/attacks-breaches/hackers-hawk-stolen-health-insurance-inf/240158396/?nomobile=1

Healthcare and other organizations are at a disadvantage when it comes to addressing the threat of cyber attacks. For one, financial services and retail organizations have been the traditional targets of criminals and as a result have developed more experience and insight mitigating the risk posed by cyber threats.

Healthcare organizations need to quickly learn the hard lessons that financial services and retail organizations have learned over the last few years. When TJX Cos. experienced its massive data breach in which a hacker stole 45.6 million credit card numbers over a two-year period, the company had to set aside a $178 million cash reserve to compensate victims, and as recently as July 2010, settled an investor lawsuit that cost the company more than half a million dollars.

Are healthcare organizations willing or able to bear the same costs?

The Rise of Underground Cybercrime Networks

For at least eight years, a vast underground network of cybercriminals has been growing in size and sophistication. Employing ingenious strategies and complex technological capabilities, they have been preying on financial services and retail organizations and their customers to steal account numbers, credit card numbers, personally identifiable information (PII), and other data that they can use to commit fraud, identity theft, or sell that data to other criminals in a thriving black market.

The once-popular hacker stereotype of a lone, alienated techno-nerd breaking into an organization's systems for fun has given way to a truly frightening reality of coordinated groups of innovative cybercriminals who collaborate, facilitate and strike aggressively. They rely on a range of advanced cyber-attack methods and social engineering techniques to steal sensitive data and then cash out in the real world, or in the same underground market where demand is well-publicized and fraudsters are well compensated.

While cybercriminals have greatly evolved their methods and grew their networks to attack financial services and retail organizations, working around security measures that have been implemented through the years, no such gradual escalation is required when targeting new industries such as healthcare. The infrastructure exists and the methods are proven – and they are gradually being trained on new targets.

Electronic Healthcare Data Creates New Risks

The emergence of Electronic Health Records (EHR) and healthcare portals for patients and providers has made it easier to access and share medical information. While such access is necessary for improving patient care and safety – not to mention empowering patients and their families to make more informed decisions about care – it also makes it easier for cybercriminals to gain access to healthcare data and other personal information.

EHRs and healthcare portals contain massive amounts of PII, including dates of birth and Social Security numbers, as well as sensitive information about medical diagnoses and treatments that violate patients' privacy. And for those that enable payment of medical bills and other account management services online, there is also the prospect of gaining access to financial data.

3 http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202013.pdf

"Hello, this is the voicemail of Healthcare Company ABC. If you are calling regarding an email you received indicating something about a complaint against you, please be advised that we did not send you that email. It is a fraud, scamming-type of malicious email and the attachment does contain a Trojan virus. Please do not open the attachment and delete the email from your system immediately."

This is an actual message that was left on the voice mail of an employee at a large healthcare association that was targeted by cybercriminals. In the attack, potential victims received a phishing email appearing to be from the healthcare company that cited a complaint had been filed against them and directed the user to open the attachment within the email for more details. Once the user clicked on the attachment, a Trojan virus was installed on their computer.

The double use of phishing and malware within the same cyber attack is not new. However, it is a popular method being used by cybercriminals today to propagate malware, and they are using social engineering scams outside of the traditional phishing email that appears to be from a victim's financial institution. Increasingly, RSA has witnessed brands across industries such as healthcare, government, education and oil and gas being exploited to serve as the face for these types of attacks.

With the pervasiveness of information being made available electronically, healthcare organizations are increasingly attracting cybercriminals. As of June 2013, 45.2% of breaches identified by the Identity Theft Resource Center were in the medical/healthcare industry – in the first half of 2013 over two million records were compromised, representing 31.2% of all breaches. Healthcare was second only to business as far as number of breached identified.[3] Certainly, the number of healthcare breaches is expected to grow.

Why? There are numerous reasons. For one, it pays. The World Privacy Forum has reported that the street cost for stolen medical information is $50, versus $1 for a stolen Social Security number. The average payout for a medical identity theft is $20,000, compared to $2,000 for a regular identity theft.

Second, it is harder to detect. Medical information fraud takes more than twice as long to identify as compared to regular identity theft[4]. Simply put, victims can close a compromised bank account, but they can't delete or change their personal information, medical records or history of prescription use.

Healthcare Data for Sale in the Underground

Cybercrime in the healthcare industry is particularly heinous because the cybercriminals target not just consumer data but also information from healthcare providers, insurers, and pharmaceutical manufacturers and distributors. Using phishing, Trojans, and other malware infections, fraudsters target internal systems as well as connections to the systems from outside the healthcare organization. Once they get in, there are many ways to profit from the stolen information.

Those who have no way or knowledge to use the information for their own illicit purposes, sell it. And when they do, they sell the same database to an average of 8 different criminals.

Figure 1 shows an example of the increasing value of healthcare information in the criminal underground. In this case, a cybercriminal is trying to sell data on individual medical claims. The wealth of information shown for sale here is rather alarming – from personally identifiable information to medical history information including illnesses and diagnoses.

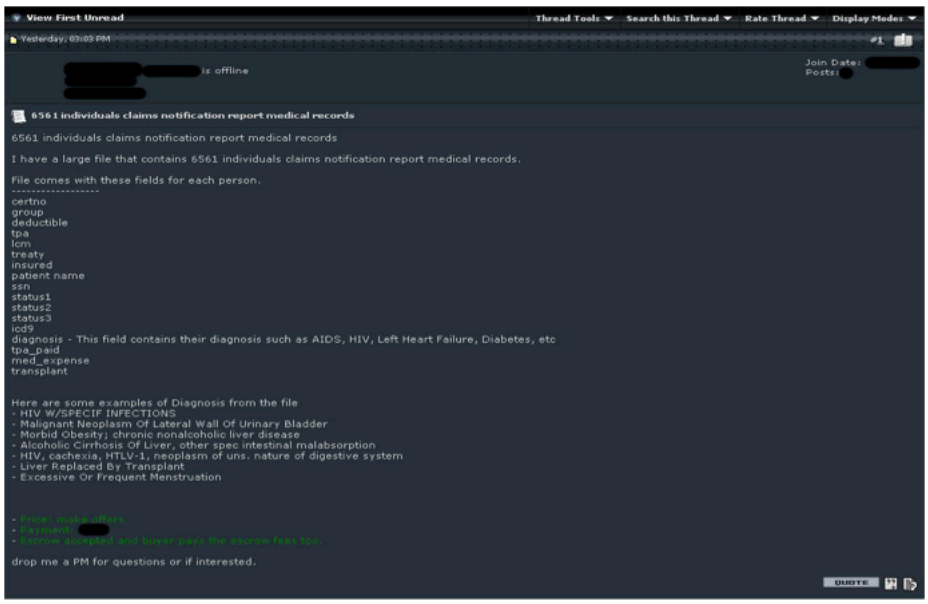

Figure 1: A post in the underground seeking buyers for the medical records of over 6,500 patients

4 Javelin Strategy & Research

Those who do have a crime scene in mind, act on it. For example, one of the ways in which cybercriminals are committing healthcare fraud is by filing false patient claims to insurers and government agencies that provide health services. With access to data contained within EHRs, a fraudster can use that information to bill for services that were never rendered. Figure 2 shows a cybercriminal seeking someone with access to information from healthcare or insurance providers and samples of completed medical claim forms to exploit for this purpose.

Figure 2: A cybercriminal seeking data that will enable him to file false medical claims

There is also a growing demand for pharmaceutical data in the underground. Cybercriminals can use this data to order prescriptions at multiple pharmacies and then attempt to resell the medicine online. Criminals can also buy prescriptions with another person's account and reroute it to be delivered to the wrong place. Physicians' information is also valuable to cybercriminals because they can use it to write fake prescriptions to facilitate schemes involving the purchase and resale of prescription drugs.

Consumers of healthcare services are also affected in many ways by having their medical records exposed or breached. Some of the risks they face include:

- Personal data being used by criminals to open new credit accounts in their name
- Being wrongly accused of abusing medical services due to criminals filing false medical claims using their information
- Threatened with blackmail or extortion from criminals threatening to expose sensitive medical or health details (while no cases of blackmail have yet been reported with consumers of healthcare services, cybercriminals who had stolen 8.3 million patient records from the Virginia Prescription Monitoring Program demanded a $10 million ransom – this could certainly happen with the medical information of high-earning individuals)

The Threats and Challenges Healthcare Organizations Face

The harvesting of healthcare data by cybercriminals is both intentional and inadvertent. Intentional incidents are evident by the sheer number of data breaches targeting healthcare organizations as well as the estimated 250,000 to 500,000 medical identity thefts that take place each year[5]. Inadvertent losses are a result of the rapid proliferation of Trojans and malware that seek to steal financial data yet unintentionally collect other information such as login credentials to online healthcare portals.

Essentially, the push to share and exchange medical information electronically is opening the door for healthcare organizations to become a target of cybercrime. The same cyber threats that have been used by criminals to attack financial institutions for years – including phishing, Trojans, malware, drive-by downloads, and other schemes – are now being leveraged to target users of healthcare portals. The types of healthcare data being collected and the ways criminals are attempting to monetize it are still evolving. But that still does not diminish the need for those who operate within the healthcare realm to recognize the impact cybercrime could have on their organization.

5 World Privacy Forum

The challenges facing healthcare organizations are many, both in terms of the range of security risks posed by cybercrime and introducing and educating on the threat within a culture that has not traditionally had to accommodate such imperatives. Security risks and issues that need to be addressed within the healthcare industry as they push out more information online include:

- Securing enrollment to ensure that first-time users to a portal are who they say they are before granting access to various applications
- Securing access to online portals to prevent the loss of patient's personal and healthcare information
- Securing access for physicians to clinical applications that contain patient data
- Securing access for payees and other third parties to sensitive data required to perform their job
- Securing the web session both before and after login
- Educating employees on the risks of phishing and malware

Driving Adoption of Healthcare Portals

Healthcare portals are destined to become more prevalent especially in light of Meaningful Use requirements around EHR adoption. Stage 2 Meaningful Use Core Measures requires eligible healthcare providers to "Provide patients the ability to view online, download and transmit" health information. This objective is one of 16 (for hospitals) or 17 (for eligible professionals) that healthcare providers must meet in order to be eligible for incentives tied to EHR adoption. Providers who cannot demonstrate compliance with these objectives are ineligible for reimbursement

A primary challenge of implementing stronger security within any online application is usability. One of the major goals of migrating patient services to the online channel is to provide easy and convenient access to data for all users within the healthcare ecosystem – including patients, providers and payees. Yet, any level of security that is applied must be done so without interfering with the ability of users to accomplish their goals or access the information they need quickly. For example, a reasonable concern that is voiced by providers is whether security will hinder their ability to access the information they need in order to administer patient care.

Consumers are also concerned about the privacy and security of healthcare portals. This apprehension is valid as many portals solely utilize password-only protection, which is substandard for resources that contain masses of sensitive data given the sophistication of modern cyber threats. According to RSA's Global Online Consumer Security Survey:

- 64% of consumers polled stated they were concerned with their personal information being accessed or stolen on a healthcare site
- 59% of consumers polled stated their concerns with their personal information being stolen makes them less likely to submit personal information to a healthcare site
- 64% of consumers polled stated that healthcare sites should implement a stronger form of security to identify users when logging in
- 95% of consumers polled stated they would be willing to use stronger security if it was offered at the healthcare site(s) they regularly visit

In order to drive adoption of online portals, healthcare organizations must be able to assure users that they can access their systems securely and that any personal information contained within or submitted to the portal will be protected.

Conclusion

Cybercrime is a very mature business. Cybercrime in the healthcare industry, however, is still in its relative infancy – and only because the exchange of healthcare information online in its relative infancy. Recent history provides ample evidence to conclude that the increase in healthcare data sharing via EHRs, personal health records, insurance portals, and prescription sites will inspire a commensurate increase in cybercriminal activity targeted at healthcare organizations.

When phishing started to make a name for itself earlier last decade, it was hard to anticipate that we would be addressing the sophisticated cyber attacks we see today. But just as most financial institutions have implemented security measures to protect access to customers' accounts and personal data, healthcare organizations will be doing the same.

In general, healthcare organizations face increased risks compared to financial services and retail organizations because the types of information they hold are more valuable to a cybercriminal (even more valuable than just credit card numbers) and there are more access points to get to it. And healthcare organizations can't just replicate what enterprises and institutions in other industries are doing - they need to adopt, implement, and utilize security solutions that are designed for their particular needs based on their risk profile, user environment, regulatory requirements and how sensitive information is used, shared, and accessed.

Together, consumers, healthcare providers, payers, and the pharmaceutical drug industry must become aware of the potential cyber risks they face. Cybercrime in healthcare is just starting to evolve, but could quickly become a devastating industry, economic, and societal problem. Any solution must start with healthcare organizations themselves recognizing the potential impacts of cybercrime and taking aggressive steps to protect the sensitive information they create and exchange with the same commitment they bring to protecting patients from harm.

About RSA

RSA, The Security Division of EMC, is the premier provider of intelligence-driven security solutions. RSA helps the world's leading organizations solve their most complex and sensitive security challenges: managing organizational risk, safeguarding mobile access and collaboration, preventing online fraud, and defending against advanced threats.

Combining agile controls for identity assurance, fraud detection, and data protection, robust Security Analytics and industry-leading GRC capabilities, and expert consulting and advisory services, RSA brings visibility and trust to millions of user identities, the data they create, the transactions they perform, and the IT infrastructure they rely on. For more information, please visit www.RSA.com and www.EMC.com.

H12105 CYBERC WP 0713

www.emc.com/rsa

EMC²

RSA