

# CYBERCRIME AND THE HEALTHCARE INDUSTRY

Access to data and information is fast becoming a target of scrutiny and risk.

Information contained in medical records has much broader utility than financial records, can be used to commit multiple types of fraud or identity theft, and does not change, even if compromised.

Healthcare professionals are in a tight spot. As administrative technologies like electronic health records (EHRs) and patient and provider portals begin to 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 controls to ensure the integrity and privacy of patient records and other sensitive medical data. Despite increased protection, healthcare organizations are a newly favored target among cybercriminals because of the wealth of personal data they collect which 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.

According to a recent report by Javelin Strategy & Research, fraud resulting from exposure of health data versus other kinds of sensitive information increased from 3% in 2008 to 7% in 2009. In addition, the study showed that criminals were able to exploit information from medical records to commit fraud for four times longer as compared to other types of identity theft.

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 \$1USD. But when that single card is sold with a full identity profile, the value can be up to twenty times more .

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 were the typical targets of criminals and have more experience and insight mitigating the risk posed by cyber threats.

*“Hello, this is the voice mail of Healthcare Company ABC. If you are calling regarding an e-mail you received indicating something about a complaint against you, please be advised that we did not send you that e-mail. It is a fraud, scamming-type of malicious e-mail and the attachment does contain a Trojan virus. Please do not open the attachment and delete the e-mail 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 e-mail 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 e-mail 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 e-mail 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.

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 ready to bear the same costs?

## THE RISE OF UNDERGROUND CYBERCRIME NETWORKS

For at least five years, an 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 or sell 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 communicate frequently and strike aggressively. They rely on a range of advanced attack methods and social engineering techniques to steal sensitive data and then cash out in a market where demand is well-publicized and fraudsters are well compensated.

While cybercriminals evolved their methods and grew their networks to attack financial services and retail organizations and work around security measures that have been implemented, 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.

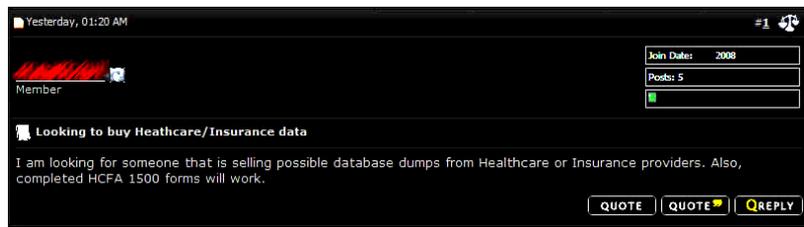
With the pervasiveness of information being made available electronically, healthcare organizations are increasingly attracting cybercriminals. As evidence of this, nearly one out of every six data breaches that occurred in 2009 was targeted at the healthcare industry, according to the Open Security Foundation. Certainly, that number 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<sup>1</sup>. 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.

---

<sup>1</sup> Javelin Strategy & Research

Figure 1: A cybercriminal seeking data that will enable him to file false medical claims



With access to data contained within EHRs, a fraudster can use that information to bill for services that were never rendered.

## HEALTHCARE DATA FOR SALE IN THE UNDERGROUND

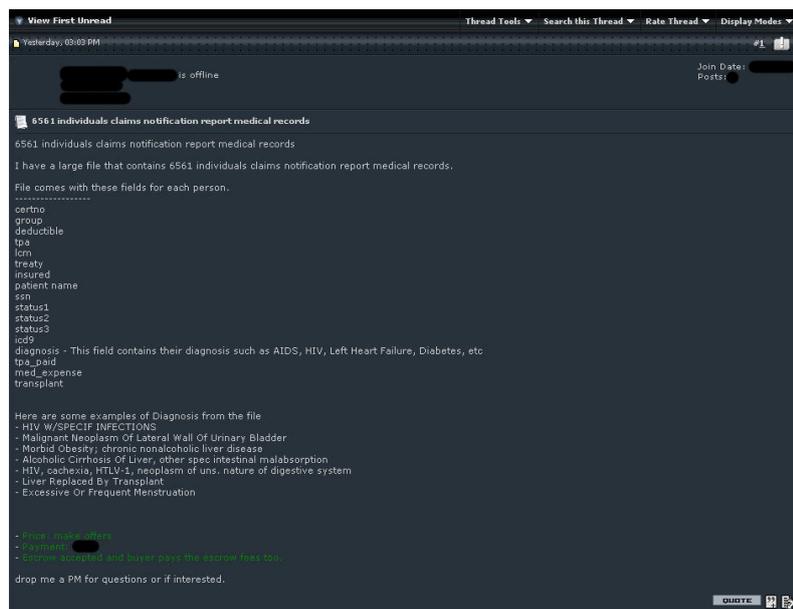
Cybercrime in the healthcare industry is particularly heinous because the cybercriminals target not just consumer data but also information from healthcare providers, insurers and pharmaceutical manufacturers and distributors. Using phishing, Trojans and other malware infections, fraudsters target internal 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.

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 1 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 shows another 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 records. The wealth of information shown for sale here is rather alarming – from personally identifiable information to medical history information including illnesses and diagnoses.

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.

Figure 2: A post in the underground seeking buyers for the medical records of over 6,500 patients



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 push to share and exchange medical information electronically is opening the door for healthcare organizations to become a target of cybercrime.

The harvesting of healthcare data by cybercriminals is both intentional and accidental. Intentional incidents are evident by the sheer number of data breaches targeting healthcare organizations as well as by the estimated 250,000 to 500,000 medical identity thefts that take place each year in the United States<sup>2</sup>. Accidental losses are a result of the rapid proliferation of Trojans and malware that both steal financial data and unintentionally collect other information such as login credentials to online healthcare and pharmaceutical portals.

The push to share and exchange medical information electronically is opening the door for healthcare organizations to become more focused targets of cybercriminals. The same cyber threats that have been used to attack financial institutions for years (including phishing, Trojans, malware, drive-by downloads and other schemes) are increasingly being leveraged to target users of healthcare portals. The types of healthcare data being collected and the ways criminals are attempting to monetize this data are still evolving. However, despite this still being in the “early days” of evolution, healthcare security professionals still need to recognize the impact cybercrime could have on their organization.

The challenges facing healthcare organizations are many, both in terms of the range of security risks posed by cybercrime and how to educate within an industry that has not traditionally been the focus of cybercrime. Security risks and issues that need to be addressed within the healthcare industry include:

- Determining the authenticity of an individual’s identity during enrollment online or via a call center to ensure that first-time users are who they say they are (before granting access, privileges, credentials, services, etc.)
- Secure access to online portals to prevent the loss of patient’s personal and healthcare information
- Secure access for physicians to clinical applications containing protected health information (PHI)
- Secure access for payers and other third parties to sensitive data
- Educating consumers, providers and employees about the risks of phishing and malware

---

<sup>2</sup> World Privacy Forum

Cybercrime in healthcare is just starting to evolve, but could quickly become a devastating industry, economic and societal problem.

## DRIVING ADOPTION OF HEALTHCARE PORTALS

A primary challenge of implementing stronger security within an 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 payers. 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 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 2010 Global Online Consumer Security Survey:

- 64% of consumers stated they were concerned with their personal information being accessed or stolen on a healthcare site
- 59% of consumers stated their concerns with their personal information being stolen makes them less likely to submit personal information to a healthcare site
- 64% of consumers stated that healthcare sites should implement a stronger form of security to identify users when logging in
- 95% of consumers 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 infancy – and only because the exchange of healthcare information online is in its infancy. The evolution of attacks against the financial services and retail industries 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 in this century 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, it is just a matter of time before 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 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 is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.

EMC<sup>2</sup>, EMC, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

©2010-2011 EMC Corporation. All rights reserved. Published in the USA.

CYBHC WP 0511

[www.rsa.com](http://www.rsa.com)

