International Journal of Research in Economics and Social Sciences (IJRESS)
Available online at: http://euroasiapub.org
Vol. 7 Issue 6, June- 2017, pp. 112~119
ISSN(o): 2249-7382 | Impact Factor: 6.939 | Thomson Reuters Researcher ID: L-5236-2015

Cyber Crime In Healthcare

Shilpashree.c.r[1],
Research scholar, dhsms, jss university, mysore

Roshan.k[2],
Assistant professor, dhsms,jss university, mysore

Dr.Divya rao.B.j[3]
Assistant professor, dhsms,jss university, mysore

Abstract-

The present era which is information based and internet based, most of human activity is dependent on systems which are integrated with the core services like banking ,health transport and communication etc one way these development are enhancing the services equally the other side it has a evil effect of crimes based on internet which are termed as cyber crimes. This paper attempts to explain the concept of cyber crime in relation to health care industry in terms of its operation, reasons and its impact.

Key words- cyber crime, impact, health care.

Introduction

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Meaning of cyber crime in healthcare

Healthcare security breaches and criminal attacks are surging in frequency, scope and sophistication, making them increasingly difficult to detect, prevent and mitigate. The past two years have seen a record number of breaches and records exposed. In 2015,more than 120 million healthcare records were compromised in data breaches, and in 2016 more than 315 major breaches were reported among healthcare organizations. The widespread use and exchange of digital personal health information has created a hotbed for cyber attacks conducted by sophisticated threat adversaries. Despite heavy investment and implementation of health information technology (e.g. electronic health

record systems, databases, registries, repositories, connected medical/personal devices and other software) organizations are increasingly vulnerable because they do not have sufficient cyber security resources, processes or encryption measures in place. In the healthcare industry, data breaches today are primarily the result of threats that are able to gain unauthorized access to records that would otherwise be preventable with appropriate measures deployed. It is therefore critical for healthcare stakeholders to elevate cyber security as a core asset that is integrated into care delivery, co ordination, communication and management.

Objectives of study-

This study is primarily focused on explain the concept of cyber crime and the ways in which cyber crime are operating in the globe along with special emphasis on healthcare industry.

Why the sudden focus of cyber crime is on healthcare?

As a new Cisco Healthcare white paper shows, healthcare has been in the cross-hairs for several years. However because of the relative lack of sophistication of healthcare information security to detect attacks, most have gone unreported. The theft of someone's bank balance doesn't go unnoticed for very long. The theft of a large number of credit card numbers triggers banks to look for a common point of purchase (CPP), in order to identify the compromised merchant(s). The theft of someone's personal health information (PHI) or personally identifiable information (PII) takes much longer to be noticed. Unless the FBI is involved there is no single body to correlate all the identity thefts, and medical insurance frauds, etc., in order to identify the source.

The second factor has more to do with the market valuation of stolen data. The wholesale value of stolen credit cards on the dark net has declined rapidly over the past nine months as markets became flooded with card numbers. At the same time cyber criminals have discovered lucrative new avenues for the disposal of stolen healthcare information by parsing the data into market categories such as personal identities, prescription information, or insurance information. Criminals are able to make much more money by selling these buckets of information to different groups, rather than selling the medical record as a whole.

Market values of stolen information vary greatly each day. The price of a medical record continues to increase, while the price of a credit card number continues to decrease. By some estimates, a stolen credit card has a value of less than one dollar, while a complete medical record can fetch in excess of $45.

Reason for Rise of Cyber Crime In Healthcare

Cybercriminals are increasingly targeting healthcare institutions and successfully deploying malware and ransomware to exploit hospitals' need to recover quickly.

The healthcare industry has recently come under heavy fire as a target of cybercrime. Ransomware attacks on hospitals in California, Indiana, Kentucky, and Maryland, forced some officials there to make quick decisions in order to get their systems back up and running to avoid disruption of patient care.

The research team at Duo Security today released a report on the current state of healthcare endpoint security that compared the company's healthcare industry customers' device cybersecurity to that of other industries. According to the findings, the healthcare sector has yet to come up to speed on information security.

Here's a look at the key reasons cybercriminals are targeting healthcare institutions.

1. Healthcare is historically not very secure.

In 2009, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act that required hospitals to switch from paper to electronic health records (EHRs). With this came a flood of new health information technology and concerns that some of these vendors were bypassing security measures in order to get their products to market quickly, leaving the already newly digital healthcare institutions open and susceptible to cyber attacks.

Healthcare institutions are still holding on to legacy pieces of software, which makes them a much easier target, says Mike Hanley, director of Duo Labs. He adds that educating users about when it's time to update software and systems or making them aware of phishing emails can be difficult.

2. It's life or death.

Because lives are at stake, healthcare professionals and their patients often can't afford to have systems down or wait for an incident response team to come in and clean up the mess. This makes them prime targets for ransomware attacks. They often pay the ransom in order to get their systems back up and running, Hanley says.

It's front page news if a hospital in a major metropolitan area goes dark due to a cyberattack, he says, which is bad for the hospital's reputation and as well as patient well-being – you can't have people avoiding the hospital for fear of having their patient records stolen or compromised.

3. The data is lucrative.

In addition to being ripe for the ransomware-picking due to the need for fast recovery times, hospitals also house a lot of private data. When cybercriminals steal a patient's healthcare records, they're often able to acquire multiple pieces of information: social security number, medical history, insurance provider, the patient's medications, and so on. "There's a larger concentration of sensitive information [that can be resold]," Hanley says.

4. An application-heavy environment provides a broad attack landscape.

According to the Duo Labs report, Duo Security healthcare customers are logging into twice as many applications as the average user in other industries. "This in itself is not a security risk or problem, but more diverse systems ... [may] require them to use old systems," Hanley says, which could put them at risk of attack.

5. They have an affinity for Windows and out-of-date browsing.

The healthcare industry is still using out-of-date, legacy systems. The report found that 82% of healthcare organizations are using Windows, and 76% are running on Windows 7.

They're also partial to Internet Explorer (IE) 11, and 22% of Duo Security healthcare customers browse on unsupported versions of IE.

Hospital employees wash their hands to avoid getting the common cold and they need to employ the same basic measures to keep their information security systems healthy, Hanley says. "[It's about] getting back to the basics, user education, security hygiene."

Cybercrime plagues the healthcare industry

As we look ahead to the third year of the ACA, we can only hope that the prognosis for 2016 is better than the last couple of years. The scale and intensity of healthcare related cybercrime is a critical and growing threat to the U.S. medical system. According to U.S. Department of Health and Human Services, the top 15 data breaches so far in 2015 (January to October) have affected well over 110 million people. In other words, the personal information of nearly half the US adult population has been compromised in some manner by a data breach of their healthcare insurance provider. If data breaches were a virus, we'd call this a pandemic.

In the past year, organizations such as Anthem, Premera, Excellus, UCLA Health, and CareFirst have announced major data breaches, bringing the five year total of compromised patient records to more than 143 million. To put it simply: cybercrime is the new healthcare crisis. Any overarching factor that makes healthcare more expensive for insurers, providers, and patients

puts further pressure on an already strained system. The Ponemon Institute, a well-regarded security industry research firm, estimates cyber attacks against hospitals, clinics and doctors cost the U.S. healthcare industry more than $6 billion a year.

On an individual level, when a patient's insurance information is used fraudulently, the stranger's treatment history can be mixed into the original patient's EHR, creating the potential for misdiagnosis and treatment errors. Unraveling these fraudulently tainted EHRs and related patient insurance liabilities is notoriously complicated and time-consuming. Ponemon Institute research finds that victims of medical identity theft spend an average of $13,500 to restore their healthcare records, remedy their credit and reverse fraudulent claims. Unfortunately, fewer than one-third of healthcare providers offer any form of assistance to patients whose data has been compromised.

The reported data breach figures likely understate the severity of the problem, as some organizations may not yet be aware they have been breached and others may not have reported the incident. According to the HIMSS, 2015 Cybersecurity Survey, 64 percent of healthcare organizations have experienced an external cyber-attack during the last twelve months. The Identity Theft Resource Center, which tracks data breaches across industries, reports that more data breaches happen in the medical and healthcare industry now than in any other sector, accounting for 46 percent of the reported breaches in 2014. These attacks create administrative and public relations crises for many healthcare providers and distract from their core mission of providing quality patient care.

The healthcare sector represents a juicy target for cyber criminals because patient information–such as social security number, insurance ID number, credit card number, address, and medical history– is a tremendously valuable asset that can be easily used to commit fraud, financial theft, and identity compromise. In addition, medical data has more lasting value than other types of information. A stolen credit card can be cancelled and fraudulent charges disputed, but resolving medical identity theft is not as straightforward. On the black market, medical records sell for 10 to 20 times higher than credit card records.

Because the healthcare insurance industry is known to be behind the technology and cyber security curve, cyber criminals know they will not encounter much resistance gaining access to their networks, and that they will be able to lurk undetected for longer periods of time. As EMV credit card technology is more widely adopted across retail industries, cybercriminals are moving on to lower-hanging fruit, including healthcare insurers.

New IT initiatives that are promoted by the healthcare industry a way to enhance the quality of care, also add information security risk. A growing number of nurses and doctors are using Wi-Fi-enabled communication devices and tablet computers instead of clipboards and sheets of paper. Similarly, internet-connected devices have been introduced to patient bedsides in various forms– fetal monitors, electrocardiograms, temperature monitors, or blood glucose monitors– and are increasingly used in remote care. These devices– in addition to many more emerging Internet of Things (IoT) technologies– face the same security risks as networked computers, but often have not been designed to the same information security standards.

Combatting the scale, scope, and sophistication of cybercrime is outside the expertise of most healthcare organizations. Their primary purpose, after all, is to provide patient care. Staying on the cutting edge of global cyber security defense technologies and figuring out how to manage the brand new challenges of IoT will require tremendous effort and investment. The healthcare industry should

start by taking a page from financial services: implementing more robust and automated fraud detection technologies to rapidly detect breaches, and planning for consumer friendly response and remediation once a breach occurs. Because organized cybercrime is targeting patient records, the security of that data should be considered most critical. This may seem obvious, yet Anthem's compromised database wasn't even encrypted.

Any healthcare organization collecting, storing, and transmitting patient data is vulnerable--from the smallest physician practices, clinics, and labs to the largest hospitals, HMOs, PPOS, and insurers. It is already proving difficult remain profitable in the new ACA system. As government regulation and public scrutiny heats up in the aftermath of this year's onslaught of breaches, failure to secure sensitive information is going to be increasingly damaging to profits and reputations, not to mention the healthcare system as a whole.

Consequences of Increased Cybercrime for the Healthcare Industry

The rise in cybercrime is no secret, with news of major breaches routinely making national headlines. What many don't realize, however, is that cybercrime is in the midst of an exponential rise across industries and the global business landscape, and that lack of knowledge is the greatest risk of all. Both the frequency and cost of cyberattacks is growing at a ferocious rate, and the healthcare industry is not immune to the trend. With the significant increase in use of electronic medical records (EMRs), the Federal Government has issued multiple warnings specific to the vulnerability of healthcare providers. In recent months the FBI has warned of the growing trend, singling out the American healthcare industry as lagging far behind other industries in its ability to adapt and protect.

According to the U.S. Department of Health and Human Services, nearly 1.6 million people had their medical information stolen from healthcare providers in 2014. This is worrisome not only because it paints healthcare providers as an easy target, but because the information that can be stolen from providers is widely believed to be more valuable on the black market. Medical information is routinely sold on the black market for use in everything from the purchase of ill-gained medical equipment and pharmaceuticals to outright identity theft of credit worthy Americans. Additionally, medical information theft can be harder to detect and cleanup. Unlike the financial industry's responsibility with credit card identity theft, victims of medical identity theft often have limited legal rights to recover financial losses.

The issues of cybersecurity are challenging and complex, but far from impossible. Addressing those problems and overcoming them will take more than the local IT department. It will require senior management leading the charge and engaging every player within the organization; from the executive office to the most junior intern. Without a top down and bottom up approach, working seamlessly, simultaneously, risk will grow to both the organization and those it serves. Those growing risks don't stop at data theft and often lead to regulatory fines, loss of reputation and significant impact to a company's bottom line. All of this is manageable with a proper assessment and mitigation plan.

There are many ways to defend against the increase of cyber threats. Performing a thorough assessment of your organization in order to highlight weaknesses and develop a strategy is a good start. Below are a few areas you should consider when conducting your own assessment:

- Organizational culture towards security
- Firewall and Antivirus software

- Logical Access Control over your applications and network
- Physical security of sensitive information
- Strong password parameters and requirements
- Backup policies and procedures
- A comprehensive disaster recovery plan
- Limited network access

Preventing cyber-crime in healthcare

The healthcare industry is being transformed by technology, as an example, people are using mobile devices and apps to measure their fitness, wellness and physical health. Data is flowing from wearable devices directly into apps and mobile phones. With all this data, pharmaceutical companies are closer than ever to offering personalised treatments.

Indeed, at the same time, there is an ever increasing number of cyber hacks into people's medical records and connected devices, resulting in personal identities being stolen. Organisations worry about breaching individuals' privacy rights and some have stalled digital health initiatives due to concerns of increasing regulation and fines. However, we believe effective security and privacy strategies can enable the right balance between digital opportunity and risk, so that advancements in digital health, positively enrich how we care for ourselves and others; and how we measure, monitor and treat our own health.

KPMG's second event, *Innovation and Information Protection in Digital Health*, saw over 30 digital health innovators, technologists, security experts and senior executives gathering to discuss the challenges facing digital health innovators.

Early on, Mark Thompson Privacy Director and David Ferbrache, Technical Director, both from KPMG in the UK, broached the topic of the organised cybercriminal. We discussed the scary truth that today's cybercriminal has a business model, a strategy and clear objectives. Later we were treated to a series of presentations from individuals at the frontline of digital health.

Among these were some intriguing topics. We discussed a business model that provides the individual patient risk rankings directly to the general public, rather than to insurers. We heard about a paperless healthcare system and the possibilities being offered by blockchain. We had insight into insurers' use of data from wearable healthcare devices. We even rounded off the event with a fascinating talk on the latest developments in consumer genetic testing, specifically the alternative approach from the application DNAnudge. This app allows users to test themselves and have the results underpin wellbeing advice, even as far as dietary habits. The worlds of preventative medicine and consumerism really are colliding.

Running throughout all of the insights and anecdotes of the day was the advice that security and privacy considerations must be accommodated from the outset as digital healthcare moves towards becoming a mainstream commercial reality.

This article discusses each of the topics presented to us during the event in more depth, and pulls out the key issues that arose and what our tactics should be when facing these issues going forward.

International Journal of Research in Economics and Social Sciences (IJRESS)
Available online at: http://euroasiapub.org
Vol. 7 Issue 6, June- 2017, pp. 112~119
ISSN(o): 2249-7382 | Impact Factor: 6.939 | Thomson Reuters Researcher ID: L-5236-2015

Cybercrime in healthcare ;what needs to be done

With hacks and breaches hitting major corporations such as Sony, JP Morgan and the US Postal Service, the storage and protection of data came under intense scrutiny last year.

During this calendar year, the issue of online data theft has continued to cause alarm, with healthcare and the sensitive data stored by the sector being targeted. Such breaches and increasing concern has led to reform, closer auditing and additional resources being dedicated to cyber security in the health sector.

Healthcare A&E

The clearest example of this was the recent Anthem breach in February this year. The second largest American insurance provider was targeted by hackers, resulting in a data loss of over 80 million people – the largest data breach in history. Hackers gained access to the servers and extracted vital information, such as names, dates of birth and addresses.

While stolen credit card details can be combatted with a simple cancellation of the card, information stored by medical bodies, such as social security numbers, can cast the shadow of identity theft over people for years.

To the present day, further questions are being asked of the company and how they went about protecting peoples' data, both through the processes implemented and the levels of access employees within the company had to the data.

Then, in March, the news broke of the Premera breach, a Chinese state-sponsored attack resulting in the loss of data for 11 million people. This again became an ongoing story, with lawsuits recently being brought against the company accusing them of being negligent with their customers' data and not disclosing the breach in a timely manner.

Resuscitating the industry

There are two clear areas of security that need to be addressed by the healthcare sector in its attempt to stem the number of attacks occurring: IT infrastructure and the accessibility of data. By addressing both of these areas, there is hope that the healthcare sector will be able to protect itself and its sensitive data more securely.

A recent study by Agari, an email security expert, uncovered that the healthcare sector had the worst practises when it came to email security of any industry, with issues such as default passwords being used and a lack of appropriate security protocols.

It transpired that an email from a healthcare company is four times as likely to be fraudulent than one from a social media site. When viewed alongside breach damage reports, such as the one that afflicted Anthem, this makes for fairly damning reading.

The basics of IT security, such as email security and anti-virus software are more essential now than ever before. Despite being seen as a low-level solution, neglecting both the software and the practises that are associated with them can lead to threats entering your network through basic unlocked doors. It is vital that these basic processes are given just as much time, resources and respect as the most high-tech solutions available.

Despite the world of cybercrime often having high-stakes, a significant number of breaches still occur when somebody, for example, leaves a laptop in the back of a cab or on the train.

From individual shops being targeted to multi-billion dollar companies being taken down by international hacking rings, human error is often overlooked. Instead, infrastructure and security measures are often scrutinised for weakness in the wake of an attack.

Although individual errors and losses are difficult to legislate for, one way that this can be negated is a single page login that directs any access to data through a company-controlled page before the network can be accessed.

Data in recovery

Data can also be managed by using a layering system. Members of staff can only access the data that they have been given clearance for and need, rather than having access to the entire system on their device.

Then, if a breach should occur, through human error, the amount of data lost or stolen is minimised, limiting the damage to the organisation. This is especially important in BYOD usage, with a high percentage of healthcare professionals using a smartphone or tablet to regularly access sensitive data.

With much of the data used nowadays being stored in corporate clouds, a monitoring system for data access can also give companies transparency, and a method to track the access of data and quickly be alerted to suspicious behaviour.

In the light of recent attacks, it is clear that something needs to be done in the healthcare sector in order to protect data that is both incredibly sensitive and of high value on the black market.

But with strained budgets, outdated IT infrastructure and medical professionals often dealing with IT issues that they do not have expertise in, this is not an easy solution. However, by paying appropriate attention to the core components of IT security and beginning to manage the data being accessed by individuals, often through a BYOD policy, healthcare companies and insurers can begin to treat some of the most obvious haemorrhages that are leaking data.

Conclusion

The industry has now come to rely heavily on digital technologies, which increase risks such as denial of service and data breaches. Current healthcare cyber-security systems do not rival the capabilities of cyber criminals. Security of information is a costly resource and therefore many HCOs may hesitate to invest what is required to protect sensitive information.

Bibliography

1. https://www.ncbi.nlm.nih.gov/labs/articles/26578272/
2. https://www.bnncpa.com/resources/library/consequences_of_increased_cybercrime_for_the_healthcare_industry
3. http://www.information-age.com/why-vpn-security-still-thorny-topic-it-123459455/
4. http://techonomy.com/2016/03/can-we-stop-cybercrime-in-healthcare/
5. https://home.kpmg.com/uk/en/home/insights/2016/12/preventing-cyber-crime-in-healthcare.html
6. https://www.itnonline.com/article/rising-danger-cyber-crime-healthcare
7. http://www.healthcareitnews.com/blog/growing-pains-cybercrime-plagues-healthcare-industry