KYND

Cyber risks in the healthcare sector

Healthcare is the most breached industry with Personal Health Information (PHI) being more valuable on the black market than credit card credentials or regular Personally Identifiable Information (PII). When a data breach occurs at a private company, the loss of PII can be inconvenient to consumers, reputation-battering for the organisation, and may lead to identity theft but if a security incident takes place at a healthcare service, the ramifications can be incredibly serious.

A broad movement towards digitisation of medical records has resulted in the increased reliance of Healthcare companies on computer systems to collect and transact highly sensitive personal health and medical data. There is a high exposure to administrative errors due to the reliance on employees to input accurate information into systems. Legacy computer systems are often unsegregated, which increases the potential that one event could have a severe impact on operations.

Lack of security in the sector has resulted in a 50% increase of data breaches, from June 2017 to May 2019 and an exponential rise is continuing into 2020.

Business exposure and implications

Data breaches

Delays or disruption could seriously impact patient care or even cost lives. Healthcare facilities simply can't afford the outages, downtime, or general post-breach scrambling that an attack would cause, making them "easy money" for criminals. Ransomware is common, with no choice but to pay the ransoms. Examples of stolen medical data include: patient data, administrative paperwork, biometric data and prescription information.

High recovery costs

Data breaches in the healthcare industry are extremely costly compared to all other sectors. Recent research has highlighted the cost per stolen record is 3x higher than the cross-industry average. Significant advertising expenditures required to restore public relations integrity is a big contributor to this.

Huge attack surface

The sheer number of patients, visitors, and contractors on site at any one time would give any admin team a challenge to monitor, never mind secure. This combined with common 'Bring Your Own Device' protocol within all sizes of healthcare organisations raises the susceptibility and exposure to cyber attack.

Medical research is valuable

Medical institutions are also targeted for the purpose of stealing research. Medical research can take many years and cost millions to develop, but it can be stolen in minutes. Motives for stealing research may vary, but most are financially based.

Medical device compromise

Remote tampering with pacemakers, insulin pumps and digital pens used for writing prescriptions; these devices may be exploited to enable data theft or to gain access to other healthcare infrastructure or systems.

Key industry statistics

67%

of UK healthcare organisations experienced some kind of cybersecurity incident during 2019 alone[1]

26m

is the total number of patient records exposed in the largest single healthcare data breach in the US in 2019[2]

10%

of UK healthcare organisations have been breached more than 10 times in 2019[3]

£92m

is the total cost to the NHS in 2017 as a result of the devastating "WannaCry" ransomware attack[4]

What types of risks exist?

There is a variety of different threats that the healthcare industry could be impacted by, but the most common include:

Phishing
Malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers or stealing passwords in the process.

Viruses
Code which infects computer systems, corrupting or deleting data.

Hacking
An individual or group attempting to gain access to company systems with the intent to steal or destroy data.

Ransomware
A malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

Key industry statistics

96%
of IT professionals surveyed believe cyber-attackers are outpacing the security capabilities of medical organisations[5]

83%
of surveyed healthcare organisations said they've seen an increase in cyberattacks over the past year[6]

$7.13m
was the average cost of a data breach for healthcare organisations in the US in 2019[7]

33%
of healthcare companies cite unaware employees as the main vulnerability that has significantly increased their risk exposure over the past 12 months[8]

Case Study

Type
"Locky" ransomware attack on a nationally recognised medical and surgical hospital.

Scenario
A hospital employee received an email requesting urgent payment that contained a malicious Word document disguised as an invoice and mistakenly clicked on the email attachment.

Sting
After the document was opened and asked the user to enable macros to ensure the readable format of the data, it also executed a malicious script that installed the latest version of the "Locky" ransomware virus on the victim's computer. The hospital had to declare an "internal emergency" due to systems, databases and critical information being encrypted, and hospital staff members being locked out and unable to access the network. For the hospital to regain access and restore their files, the ransomware demanded $17,000 to be paid in Bitcoin for a decryption key.

Investigation
Relying heavily on online records to operate daily and look after their patients properly, and faced with a long backup process and catastrophic, potentially life-threatening disruption, the hospital gave in and paid the ransom.

Conclusion
Ransomware is one of the most difficult types of malware to deal with upon infection, but some key security measures can be implemented to prevent the increasing threat of such attacks in the first place, including regular data backups kept offline, email policy procedures, and keeping all the organisational systems up to date and patched.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch

broker@kynd.io
www.kynd.io

References:
[1] http://www.pharmatimes.com/news/cyber_attacks_hit_more_than_half_of_healthcare_orgs_in_last_year_1322396, 2020, PharmaTimes Online
[2] https://www.hipaajournal.com/2019-healthcare-data-breach-report/, 2020, HIPAA Journal
[3] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, 2019, ENISA Threat Landscape Report 2018
[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf, 2018, Securing cyber resilience in health and care
[5] https://www.prnewswire.com/news-releases/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-will-be-worse-reports-new-black-book-survey-300950388.html, 2019, PR Newswire Association LLC
[6] https://www.carbonblack.com/resources/cyber-security-in-healthcare/, 2020, Cyber Security in Healthcare
[7] https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year, 2020, 2020 Cost of a Data Breach Report, IBM Secur
[8] https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf, 2019, EY Global Information Security Survey 2018