Grapevine MSP
Technology Services

Cyberthreats & how to tackle them in Healthcare

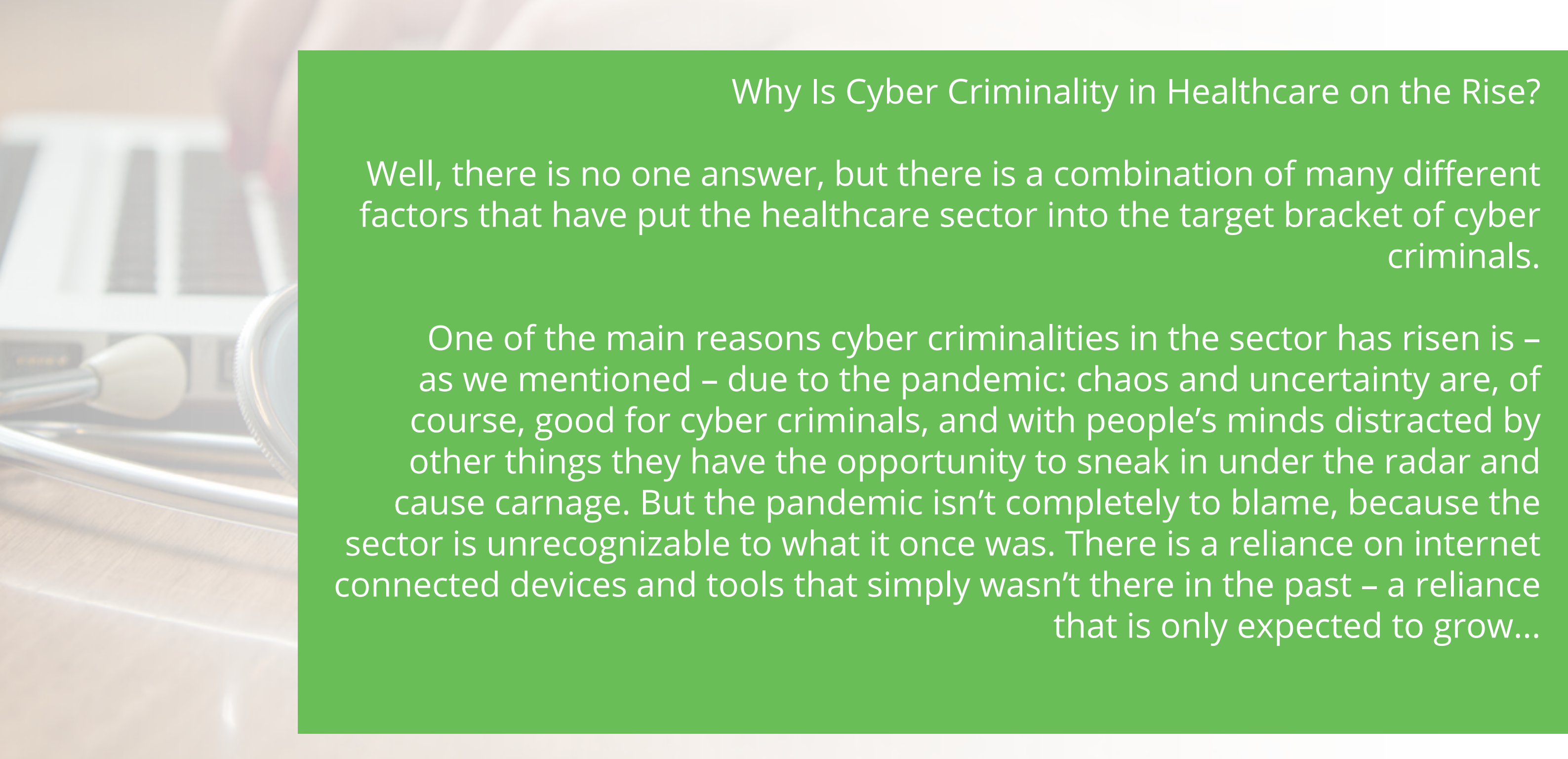
Your Business – Prepared and Secure

Cyber Threats in Healthcare

Recent times have been particularly difficult for those that work in the healthcare sector. The pandemic has caused pandemonium all around the world - and healthcare professionals have gallantly put their own health on the line to ensure that we stay fit and healthy through the worst of times.

It is this that makes it particularly unfair that we have to write these articles. Unfortunately, cyber criminals have seen the pandemic – and the increased workload that those in the healthcare sector have experienced – as an opportunity. Yes, as a nation we are number one in the world for cyber security, but cyber criminality in the US has risen considerably since the onset of the pandemic – especially in the healthcare sector.

So, why is this?



Why Is Cyber Criminality in Healthcare on the Rise?

Well, there is no one answer, but there is a combination of many different factors that have put the healthcare sector into the target bracket of cyber criminals.

One of the main reasons cyber criminalities in the sector has risen is – as we mentioned – due to the pandemic: chaos and uncertainty are, of course, good for cyber criminals, and with people's minds distracted by other things they have the opportunity to sneak in under the radar and cause carnage. But the pandemic isn't completely to blame, because the sector is unrecognizable to what it once was. There is a reliance on internet connected devices and tools that simply wasn't there in the past – a reliance that is only expected to grow...

Cyber Threats in Healthcare

The internet of things (IOT) in healthcare – as much as it has allowed healthcare to advance - can be a real threat. For those that don't know "the IOT refers to a system of interrelated, internet-connected objects that are able to collect and transfer data over a wireless network without human intervention." [1] In layman's terms, think of any object that has sensors which can gather and transfer data across a network with no human interaction – in a hospital setting an example could be on a heart rate monitor. (The patient could be asleep with it on whilst the nurses are in the office, but if the patient's heart rate drops below a certain level an alert is sent automatically to the nurses in the office.) If a cyber criminal was to gain access to these internet connected devices, they could reap havoc on the entire hospital – potentially at the cost of people lives.

Arguably the biggest threat to security in healthcare is – regrettably – the people. Healthcare workers are usually compassionate and are equipped with levels of empathy and patience that the rest of us couldn't hope to achieve, but modern healthcare requires more than that. Healthcare teams aren't educated enough on not only the dangers that the cyber environment poses but how to maneuver it in the safest way possible.

Let's take a look at some of the most common forms of cyber attack that face the healthcare sector now.

Cyber Threats: Phishing

Phishing:

With data in Healthcare being a particularly valuable target for cyber criminals, Phishing attacks are particularly prominent. They are predominantly used to target Emails. When undertaking a Phishing attack, the cyber criminal will take on a false identity in order to pull the wool over their target's eyes, in turn granting them access to sensitive information such as bank details or passwords. Phishing is a particularly popular method of attack because of the variety of different ways that the attack can be carried out. The aim is to make their target believe that not only are they emailing them from a legitimate source, but that the message itself is legitimate and requires immediate attention. They want the target to reply quickly with very little forethought, so to make this possible they often pose as someone of significance, usually either their employer or someone higher in the hierarchy than them.

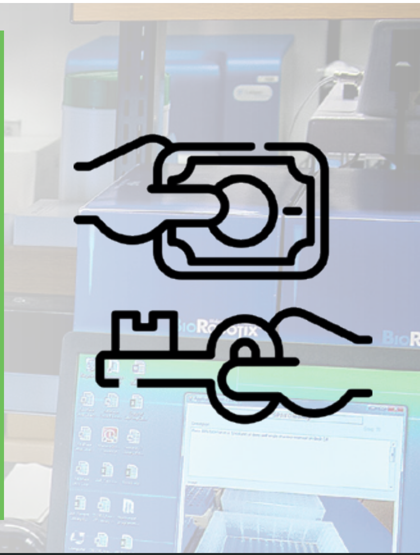
For example, in 2021 "The Department of Health and Human Services' breach reporting tool showed over 1.3 million patients of Centene subsidiaries were impacted by the massive Accellion File Transfer Appliance vulnerability hack and subsequent data exfiltration. The impacted data included contact details, dates of birth, insurance ID numbers, and health information, such as treatments and medical conditions. A number of impacted entities have also received emails from the attackers, adding to the extortion attempts." [2] The successful attack of data for 1.3 million patients was a massive problem, and all stemmed from one accidental allowance of access.

Cyber Threats: Ransomware

Ransomware:

Healthcare is the perfect target for a criminal looking to undertake a Ransomware attack. A hospital has extremely large amounts of data that can be encrypted, they have a lot of dollars in the bank to pay the ransom, and the board typically hasn't got the technical prowess of others in the industry. A successful Ransomware attack can severely hinder the hospital's ability to stay on schedule, provide care, and ultimately save lives.

Ransomware disables or encrypts the files on the system, and, whilst doing so, it provides the cyber criminal will full ownership of your data. They will then demand a ransom in return for the safe return of the data.



For example, in 2021 "The San Andreas Regional Center in California experienced a health care ransomware attack that may have exposed the PHI (Protected Health Information) of over 57,000 individuals. The breach included first and last names, birth dates, Social Security numbers, full-face photos, health plan beneficiary numbers, telephone numbers, email addresses, health insurance information, diagnoses, and disability codes." [3] Not only did this cause a huge data breach but it also slowed down the service and severely affected the reputation of the practice negatively.

It is understandable for people to say, "Just pay them, surely giving them money is better than them getting client data", and they would be right, but it isn't that simple. First, for a healthcare organization, being seen to pay cyber criminals what they demand is not the image that they want to project to their patients or the people they support - they want to be seen as a trusted pillar of professionalism, not an entity that will pay lowly criminals to get their own sensitive data back. Secondly, they are criminals – do you really think they are going to say "Thank you very much" for the potentially tens or hundreds of thousands of dollars and simply hand your data back? No, they are going to take your money and then demand some more; paying simply advertises that you are willing to give in to their demands.

The HIPAA Privacy Rule

It is apparent why you would want to tackle the threats in a practical sense, but there are also regulatory and compliance requirements in the healthcare industry that you must adhere to as well.

HIPAA:

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. It brought the flow of American healthcare information into the modern age and comprises of guidelines for how sensitive information is maintained by the healthcare and healthcare insurance industries. Predominantly, it outlines that it is prohibited to disclose protected information to anyone other than a patient and the patient's authorized representatives without their consent.

HIPAA Privacy Rule:

The HIPAA privacy rule is the particular piece of legislation that you need to take notice of, and it reads as follows:

"The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information") and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization.

The HIPAA Privacy Rule

The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.” [4]

Not remaining Cyber secure will not only affect the quality of service that you can provide to your patients and the people you support but also leave you subject to legal ramifications when not remaining compliant to HIPAA’s rules.

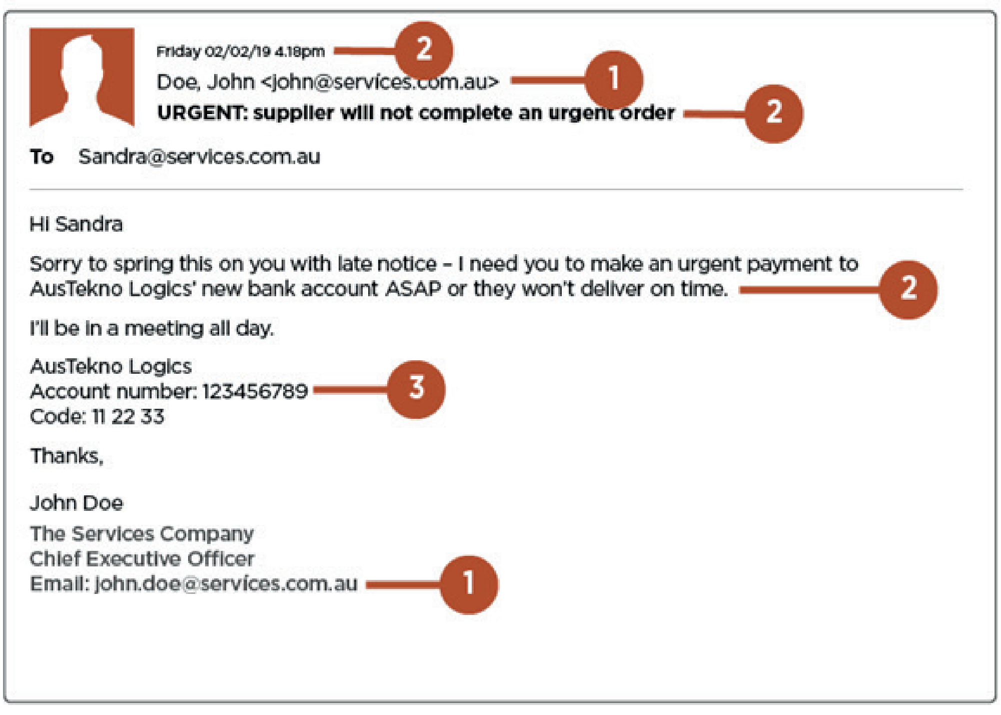
Combat Cyber Threats in Healthcare

Healthcare is the perfect target for a criminal looking to undertake a Ransomware Phishing scams and Ransomware attacks have become two of the most popular forms of attack for cyber criminals all over the globe. This is due to the ease of which an attack can be completed successfully.

There are ways to combat them though, and these methods may not be what you expected.

Combat Phishing and Ransomware Attacks.

No, we aren't going to recommend an expensive tool that you will have to implement around the entire practice, but instead we would simply recommend educating your team on what a Phishing Email looks like, and what the red flags are to look out for. Let's look at an example of one now.



Friday 02/02/19 4.18pm

Doe, John <john@services.com.au>

URGENT: supplier will not complete an urgent order

To Sandra@services.com.au

Hi Sandra

Sorry to spring this on you with late notice – I need you to make an urgent payment to AusTekno Logics' new bank account ASAP or they won't deliver on time.

I'll be in a meeting all day.

AusTekno Logics
Account number: 123456789
Code: 11 22 33

Thanks,

John Doe

The Services Company
Chief Executive Officer
Email: john.doe@services.com.au

Combat Cyber Threats in Healthcare

We will now explore the elements of this email that may cause you to not trust the recipient, in turn meaning it could be a Phishing Email and potentially contain a link to authorize a Ransomware attack.

1. It is impossible to know who the Email is from; business and professional emails shouldn't look like 'normal' email addresses. If you cannot be certain of the validity of an email address, check it. We all glance over email addresses to check them, but look closer - the "i" in "services" is, in fact, a different character. These differences are very hard to spot, but it is worth taking the time. If the recipient claims to be someone you have communicated with before then simply create a new email and message them with the trusted email you already know - if they confirm it then great, and if they don't then you know the original was a scam.

2. Most professional Emails won't put you on the spot like this; there is too much urgency in the message. As we covered in the previous article, scammers create a sense of urgency to encourage you to behave in a certain way without any forethought. DON'T RUSH but take your time. It is integral before moving on that you find out if the email is genuine or not.

3. Always verify changes to payment details directly – NEVER deviate from company procedure regarding payment. It may be quicker to do it yourself this way, but if company procedure takes you through the accounting team, then back to finance, on a long laborious journey, then so be it - you would rather that then it be you that hands over money to a cyber criminal.

The only difference between a Phishing Scam and Ransomware scam is that this Email doesn't have a link embedded, so follow the same procedure of vigilance when links are present too. You must always proceed with care, examine links closely and if you are in any doubt walk away or get advice from a superior member of staff.

These are just some of the ways to combat Phishing and Ransomware attacks. Take your time and be certain before you act – and instruct your team to do the same.

Cyber Threats in Healthcare

At Grapevine, our team of dedicated engineers can meet any technical challenge you may come across. We take our time in getting to know you, your business, your employees, and your goals for the future so we can then find the best technological solution for you to guarantee constant security and progression. Our years of experience leave us primed and ready with all the tools needed to ensure a top-quality service, now and into the future. Contact our team and let us start our journey together today.

Contact our team and let us start our journey together today.

Click here to book your free discovery call.

Grapevine MSP
Technology Services

2236 Orpheus Court, Bakersfield, CA 93308

(661) 369 8427 | Grapevinemsp.com