THE CYBER THREAT TO GLOBAL HEALTH

The growing risk of cyberattack to the healthcare industry

CONTENTS

Healthcare – The New High-Profile Target 4

A Change of Cyber Scenery 5

Vulnerability in the Healthcare Sector 6

- In normal times... 6
- Enter Covid-19... 7
- What does this mean for cybersecurity? 8

Mitigating the Risk (Without the Price Tag) 9

- Identify, Prioritise, Invest 10
- Invest Time, Communicate Effectively, Educate the Workforce 10
  - People 11
  - Processes 12
  - Technology 13

Know Your Regulations 16

- GDPR 16
- NDB Scheme 16
- Privacy Act 2020 NZ 17
- HIPAA 17
- PIPEDA 17
- Health Data Law UAE 17

Outlook 18

CYBERSECURITY IN THE HEALTHCARE INDUSTRY

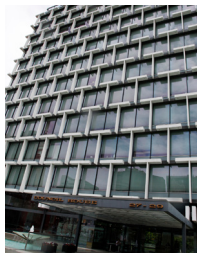

HOSPITALS


TRANSPORT


CARE HOMES


RESEARCH


INDUSTRY


AUTHORITIES

- People
- Process
- Technology

IDENTIFY

PROTECT INFORMATION:

Confidentiality

Integrity

Availability

INVEST

- Time
- Communication
- Education

PRIORITISE

- Minimal cost
- Minimal disruption
- Maximum impact

Whether it's theft or chaos, the healthcare industry is a prime and vulnerable target. Act now: the risk is real.

HEALTHCARE – THE NEW HIGH-PROFILE TARGET

The healthcare industry has rapidly shifted into the spotlight this past year. Not just hospitals, but the entire landscape: academic research, translational research and development, medical and pharmaceutical logistics, and everything in between. Right now, all attention is on the vaccination distribution supply chain, and this presents a very vulnerable target to cybercriminals.

A dangerous concoction of desperate governments and even more desperate citizens, with enormous costs, the lives of people and national economies at stake means that **extortion is a very low-hanging fruit for cybercriminals around the world**.

Once regarded as sacrosanct, health services are no longer immune from being the targets of crime and war. This much has been clear since the attack on the UK's National Health Service (NHS) in 2017, in which ransomware locked around 200,000 devices and resulted in some 19,000 appointments being cancelled with a cost of GBP 92 million[1].

Primarily, **healthcare service providers are targeted for their stores of comprehensive individual profile data** which can be sold for **identity theft and financial fraud**. In addition, passing this detailed information to third parties illegally may be profitable for marketing purposes, political voter targeting, or sophisticated scams such as fake health insurance. Individual facilities have even been extorted, with one research hospital in the UK hit by ransomware which, when they refused to pay, resulted in patient personal information being posted online[2].

Such **'name and shame' tactics are particularly effective on healthcare targets** because of the heavy regulation imposed on data privacy.

Threats to publish confidential data or give up the organisation name to regulatory bodies are powerful ransom negotiation tools, especially when many healthcare providers cannot afford the fines they would incur if they didn't comply.

Furthermore, in the context of a pandemic, the potential reasons for targeting healthcare go beyond data theft and into espionage, extortion, or political gain. **Incapacitating medical infrastructure in a manner similar to the NHS attack could now bring an entire country to a standstill**, resulting in the need for greater social restrictions, lockdowns, or travel bans. And ultimately, it would risk the lives of tens of thousands of people.

The recent attack on the Covid-19 vaccination manufacturer Pfizer is a prime example of possible state-sponsored espionage for political gain. Though the perpetrator is still unclear, the UK's National Cybersecurity Agency had already issued a warning of potential attacks by Russian intelligence attempting to access data on promising vaccination programmes. In addition, IBM identified an attempted attack on the cold transport delivery chain of vaccines across the EU which they said showed the sophisticated hallmarks of state-sponsored cyber-espionage[3].

Whether it's theft or chaos, criminals or nation states, the healthcare industry is a prime and very vulnerable target.

1 https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
2 See, for example, the Forbes article: https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#4d95da1018e5
3 https://www.independent.co.uk/news/world/europe/pfizer-biontech-vaccine-cyber-attack-covid-b1768946.html

A CHANGE OF CYBER SCENERY

The world of cybercrime that belonged to computer geeks and lone ranger hackers is gone and the criminal gangs that took over are now part of **a vast network of illegal online trade of attack techniques and data. This new cybercrime marketplace has ushered in a new age of dedicated cybercriminal organisations** such as the infamous Maze group (now dissolved) operating as a business with development, deployment, marketing and sales teams.

Organised criminal groups are reported to be behind 55% of breaches in the last year, up from 39% on the previous year[4]. This trajectory will certainly continue.

Individual hackers now operate as a network of 'affiliates': essentially freelancers who breach security systems, create software packages and then publish them for a fee. Just like with ordinary Software as a Service (SaaS), Ransomware as a Service (RaaS) is becoming the prevailing method by which organised criminal groups deploy attacks. These **packages are often designed and tailored to create maximum damage** or extract the maximum amount of data from companies that these 'freelance hackers' have carefully researched and mapped out.

For a more detailed introduction to ransomware, watch The Evolution of Ransomware[5], provided by Cyber Citadel. An in-depth analysis of ransomware and its mitigation strategies can be found in the Cyber Citadel white paper on The Issue of Ransomware[6].

4 Verizon DBIR 2020
5 https://www.youtube.com/watch?v=wNSbPDlv1FE
6 https://www.cybercitadel.com/your-money-or-your-data-ransomware/

Cryptocurrency

A cryptocurrency, the most notable of which is Bitcoin, is a decentralised, trust-free currency that exists outside the control of any national government. Anyone can create a unique address from which they can send or receive the currency almost completely anonymously.

Blockchain

All transactions made with cryptocurrencies are verified against a public ledger or blockchain, which is hosted simultaneously by many people running nodes of the network all over the world. Blockchains have many legitimate uses but also allow cyber criminals to easily and anonymously trade goods and services outside the regulated financial system.

The Dark Web

The Dark Web is a (relatively) small network of websites which are not indexed by any search engine and can only be found if the user learns the web address from an existing user. These websites can then only be accessed using the Tor browser, which hides all information about the location or identity of users from the host and each other. This anonymity has been used to create numerous illegal marketplaces, where buyers can contract hackers, purchase stolen information and orchestrate the spread of malware. These marketplaces are very difficult to shut down even by law enforcement, as the locations of the hosting servers are not known, and the anonymised traffic to and from the website cannot easily be blocked by an internet service provider.

When we think about motivation behind cybercrime, we think about money, extortion, espionage, gaining competitive edge, reputation damage, or political gain. Of course, these *are* still all the motives, but in a world of cybercrime organisations and professional freelance hackers, these are the motivations behind the *buyers*. The people orchestrating the hacking often couldn't care less.

This is dangerous: the **hackers have no personal justification, allowing them to be clinical, ruthless, and indiscriminatory**, much like a hired assassin. **This also makes them more invisible** and difficult to trace and affords the buyer the same privileges.

Cybercrime is no longer a game. It is **organised, professional, and efficient**, and criminals work with their product as with every other industry in the world: on a basis of supply and demand.

Along with this new ethos has evolved an ecosystem fit to facilitate it: a 'dark' business world. Here, cryptocurrency is the new money, blockchain the new bank, and the Dark Web the new trading floor.

These marketplace services provide all the network connectivity and anonymity that professional criminals are looking for.

VULNERABILITY IN THE HEALTHCARE SECTOR

In normal times...

Setting aside the unprecedented Covid-19 pandemic, the healthcare industry still presents many characteristics which make it vulnerable to cyberattack. Partly this is because of the **wide range of interacting sub-sectors involved**, as mentioned previously, and **the need for efficient and extensive communication** between them. For example, medical services such as hospitals, emergency services and care homes need to maintain close contact with healthcare operations units such as medical supply storage and distribution, cleaning services (for tools, equipment, operating theatres and other facilities), and testing facilities where pathology, histology, and other laboratory-based work is carried out.

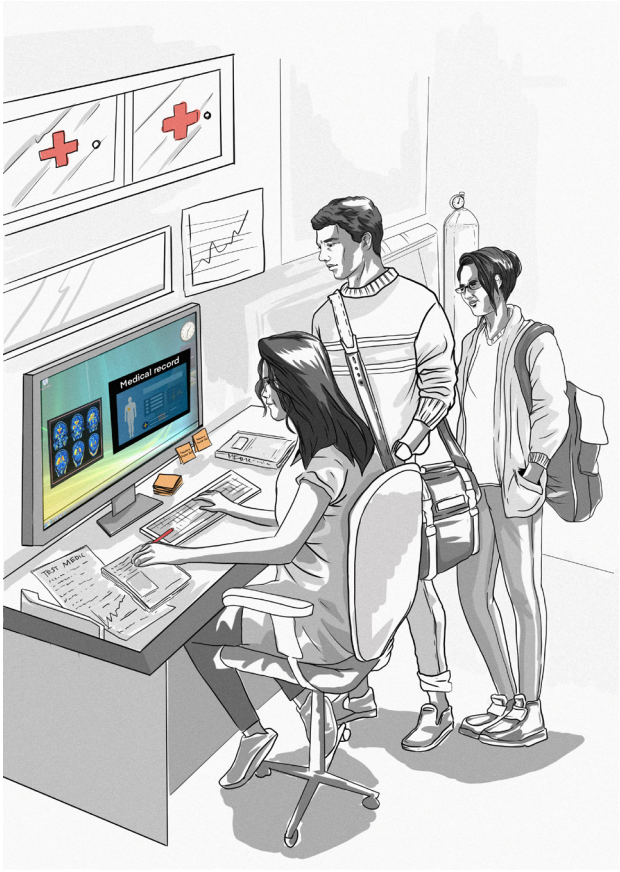
The industry is also vulnerable because of the possible consequences. **A security breach in this industry could have immediate, physical impact**: emergency response units being suddenly without access to blood databases or patient history, or cryogenic storage no longer reporting its status resulting in operations teams ignorant to a critical failure.

In September 2020, a ransomware attack on Dusseldorf University Hospital rendered computer systems inoperable. One woman who was due to have lifesaving surgery had to be transferred but died in the ambulance on the 30km journey. The incident led to police opening the **first-ever case of homicide resulting from a cyberattack**. The hackers exploited a known flaw in a VPN protocol about which German cybersecurity authorities had issued a warning earlier that year[7]. These **warnings should not be ignored** and addressing them should be a priority.

The threats in this industry are real.

In addition, **the sector is heavily dependent on the reliable and secure access to confidential patient data.** From medical history, lifestyle, family data, addresses and contact information, place of work, insurance information and more. In fully integrated healthcare systems this information needs to be accessible from any public health facility along with many private facilities (such as private care homes). In some healthcare systems this data may need to be securely transferred to another provider or insurance company where a customer decides to switch.

7 https://www.bbc.com/news/technology-54204356



As more facilities and operators look to move their services online and make their administration paperless via services such as e-prescriptions and online appointment systems to improve speed and efficiency, they must do so with digital security in mind or put their data at risk as well as their services.

The medical sector is another which suffers from **network heterogeneity**: comprising outdated legacy systems running old versions of Windows, state-of-the-art Internet of Things (IoT) devices for monitoring sensitive machines, and a haphazardly connected mix of data storage systems spanning the technological ages. These issues are particularly prevalent where aging – but still reliable – machines require outdated software to function but have been connected to the network to enable efficient storage of data.

There is a great reluctance within the scientific and medical community to update systems, whether it be for financial reasons or because these systems are stable, reliable and familiar.

In a rapidly developing cyber landscape, **this is something the medical community will have to address**. The security of these systems presents too great a backdoor into the rest of the digital infrastructure to remain as they are merely for convenience.

Unquestionably, **the resulting cost of a serious data breach for a health service provider would be far greater than any software update**, but it is often difficult to pass such expenditure through budget committees, especially in the public sector where business works on small margins and individual facilities rarely turn over profit.

Many of these **problems can be exacerbated by 'shared communities'** – spaces which are jointly used by both the public and private sectors or by healthcare providers and academic institutions. The current situation in London presents a case in point. Universities there such as University College London and King's College London operate hospital groups comprising many hospitals with associated laboratory facilities (both managed by the NHS), connected both physically and digitally to university research facilities (managed by the colleges).

As anyone in the industry knows, research and development funding is not straightforward, so a lab running a microscopy facility may want to update the system software but may not have the funding to do so. Of course, a cybercriminal does not care either way: if they can use a device operating Windows Vista to deploy ransomware which can make its way onto the wider network and over to the hospital system next door, then they will do so.

Enter Covid-19...

Whilst the world is grappling with a pandemic which has disrupted trade, isolated employees and destabilised finances, **cybercriminals are exploiting this global disaster for their own gain**.

Tactics include **impersonating** executives, governments and key organisations; **taking**

advantage of fear and financial instability; and **capitalising on the increased vulnerability of networks** due to remote working.

The healthcare industry has been placed under immense strain. Not just because of the increased demand in its services, but a forced and rapid expansion of facilities and enormous political pressure to perform. Test and trace services have presented a monumental data processing task, and raised issues surrounding privacy and data protection that even the healthcare industry has not faced before.

Grappling with this array of difficulties has been challenging and **rapidly acquiring technology into any organisation always leaves vulnerabilities** in the network.

Whilst it would seem that the bulk of healthcare work still requires staff to be on site, there is an enormous amount of administration, IT support, operations, logistics, senior management and more, which is now being carried out remotely.

This means **virtual meetings, data storage** and sharing online, a greater volume of and **reliance on email**, connecting to organisation servers, and even accessing desktops remotely. In fact, the world is generally spending more time on the internet – increases of 20% or more were reported in countries such as Italy and the UK within just the first few months of national lockdowns[8].

What does this mean for cybersecurity?

Increased email traffic means increased opportunities for phishing and whilst this type of attack itself is not very sophisticated, it only relies on the mistake of a single individual opening an attachment, following a link, or in some cases just viewing the email in full to be successful.

In addition to a higher volume of emails, many employees are receiving update-type communications from senior members of their organisation who would not normally contact them. **Unlikely to question information or instructions from senior executives, employees are at high risk from being targeted by impersonators.**

Google raised the issue of a surge in Covid-19-related malware and phishing scams back in April of last year, when it reported around **18 million daily attempts, in addition to 240 million daily spam messages**[9]. The number of scam emails claiming to be from the World Health Organisation (WHO) has also risen such that Google has worked with the organisation to implement DMARC (Authentication and Reporting)[10] making it more difficult to impersonate the WHO whilst enabling legitimate emails to arrive in inboxes.

Files, online resources, and virtual meetings are all being shared via email links. This is dangerous because **emails are easily replicated and employees will often follow links sent to them without thinking, or properly inspecting sender details**. Especially if the sender is a senior member of staff (or impersonating one).

The European Association of Cancer Research (EACR) raised this issue in an email sent out to all its members warning of phishing scams that targeted Board members, purporting to be the Association president and requesting help in transferring funds due to banks being closed as a result of the pandemic.

Most of the malware in circulation is not new, just rebranded and repurposed for the Covid-19 era. In particular, Microsoft highlighted malware known as Trickbot as the most commonly employed piece of malware in Covid-19 branded attacks. This software – originally used in attacks on banks to gain account information – is used to

8 https://blog.cloudflare.com/on-the-shoulders-of-giants-recent-changes-in-internet-traffic/

9 Google Cloud, see Identity& Security blog post: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

10 DMARC = Domain-based Message Authentication, Reporting, and Conformance

drop additional malware such as ransomware or remote access malware into a system. It is normally deployed through an attachment (or link to an attachment) on a convincing phishing email which instructs the recipient to open it.

To reiterate, in the healthcare industry these kinds of virtual attacks can have real consequences. At Brno University Hospital in the Czech Republic, a phishing atttack resulted in the forced suspension of scheduled operations and redirecting of patients to another hospital due to system shutdown and limited access to patient data and test results[11].

Emails and file sharing are not the only problems. Many companies use applications only ever designed to be run internally, but driven by remote working, these applications now face private home networks, public networks and the open internet. Under these conditions, employees are not protected by a corporate firewall and data traffic often cannot be monitored. Such applications must be rigorously tested to ensure they do not pose a risk to the company and any remote connections must be secured.

Furthermore, **with support staff working remotely, if anything were to go wrong, the IT department is not necessarily at hand to respond immediately**.

Just as the healthcare community tells the world to remain vigilant about an indiscriminate virus to which everyone is vulnerable, the cybersecurity community is telling the healthcare sector to **be vigilant towards indiscriminate cyberattack.**

11 https://brnodaily.com/2020/03/13/news/serious-cyber-attack-targets-brno-university-hospital/?rel=author

MITIGATING THE RISK (WITHOUT THE PRICE TAG)

Mitigating cyber risk can be tricky and doing so requires serious investment. However, t**his investment is not solely financial**; throwing money at cybersecurity will only get you so far. A company might invest millions in building a watertight network, but if an employee accidentally provides their credentials to a cybercriminal by clicking on a link in a phishing email, then all that investment will have been a waste.

What is needed is **dedicated time and personnel, an effective system of communication, and a commitment to providing training** to staff so that they are educated on the risks.

The healthcare industry presents many challenges. The sector operates on a particularly tight budget, and any steps taken cannot disrupt services for a prolonged period of time, since this itself could risk patient health.

Thus the aim becomes to **introduce mitigations at minimal cost and minimal disruption, but with maximal impact.**

Identify, Prioritise, Invest

Healthcare is an old and highly evolved industry, with systems and processes built up over hundreds of years. Recent digital developments have sought to streamline services in order to increase output, reduce inpatient times, and cut costs and paperwork.

This **continuous evolution has led to inconsistent integration of different systems, especially where different services and facilities might be evolving at different rates**.

Multi-Factor Authentication (MFA)

MFA is a security authentication method used to verify a user's identity by requiring two or more credentials. Only if users can successfully provide multiple sets of credentials are they then granted access to the computer or authentication system.

Many cloud-based services such as Office 365 now offer this as an easily activatable setting, making its roll-out both fast and simple.

Whilst some hospitals might now be entirely paperless, the local authority health service departments might not be digitised at all, resulting in the need for duplicate filing systems and increasing the risk of error or mismanagement. Additionally, as other facilities are brought online, they will need to be granted access to shared systems and these processes can often leave holes for potential hackers to exploit.

The key here is to **identify these vulnerabilities as quickly as possible** – *before* the new system or process is installed – so that organisations can **be proactive in mitigating risks** rather than reactive to breaches when it may be too late.

When identifying risks, it is essential to consider *all* the potential weak components of a network. This means **consider the people and processes that make up an organisation and not just the technology** holding the network together. Technological improvements are all for nothing if the people or processes in an organisation are vulnerable. Of course, it is important to have a good firewall system or implement Multi-Factor Authentication (MFA) as examples, but if local authority staff are printing off hard copies of patient data on shared printers, or worse, at a public printing service connected to a public network, then it does not matter how secure the internal network is.

Once vulnerabilities have been identified, they will need to be prioritised. This is particularly important for cost effectiveness and minimising disruption. Once prioritised, a plan can be designed to mitigate; this **mitigation should be built upon a three-pronged framework of time, communication and education**.

Invest Time, Communicate Effectively, Educate the Workforce

Time needs to be given to cybersecurity and discussed regularly at policy and planning meetings. Decisions to implement new technology, protocols, or develop more secure processes must be **effectively communicated to both senior management and general staff**. Communication needs to be targeted, since information may be relevant to different employees and **the right information needs to reach the right people**. Providing information to employees which is irrelevant to them will only result in them ignoring potentially vital information and will cultivate apathy towards cybersecurity. This is particularly important in the healthcare sector where **staff often only have the time to read and digest limited amounts of information**.

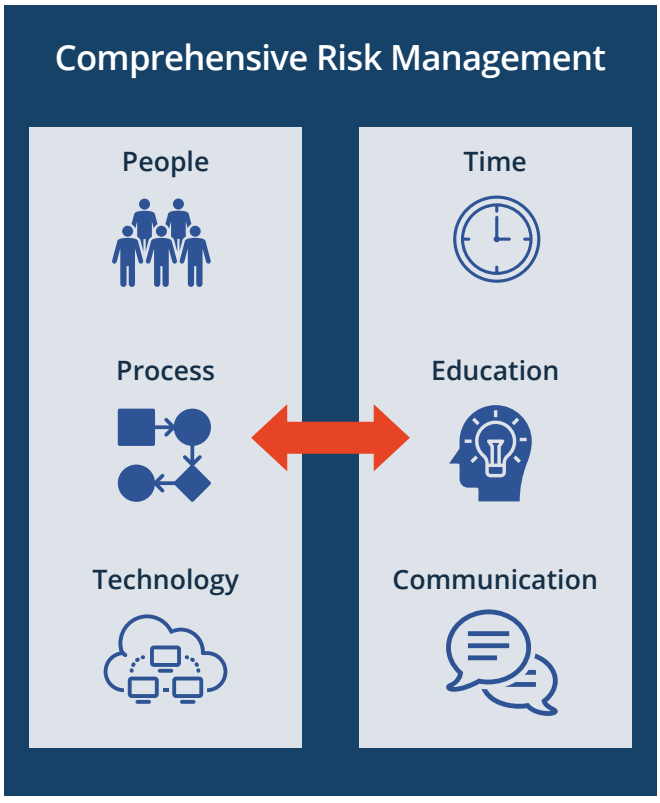
Finally, **staff in the healthcare industry need to be educated on the cyber risks** of *their* work. It is common practice for new employees across the healthcare sector and R&D sectors to receive initial training, including general health and safety practices, hygiene practices, handling of cryogenics or compressed gases, using personal protective equipment, or emergency procedures in cases of fire, chemical spills, or infectious disease outbreak. It would make complete sense to append this list with **compulsory, basic**

cybersecurity training, and this would *not* require a great deal of additional organisation, time, or money.

A basic cybersecurity awareness, for example the ability to recognise spear phishing emails or carry out protocols for reporting suspicious cyber activity, would go a long way in improving security and would **aid in continual network monitoring** and thus decrease an organisation's reaction time to a cyberattack.

Training in emergency procedures in the event of a network breach would also greatly **contribute to an organisation's response plan** and reduce the impact of attacks.

Implementing a comprehensive risk management programme is the job of senior leadership. **Executives and directors must recognise the risks of cyberattack and must make addressing these risks a priority.** Only when senior leaders **initiate the conversation and drive forward mitigation** plans will the rest of an organisation begin to take these risks seriously as well.



The Principle of Least Privilege (PoLP)

The principle of least privilege is the idea that at any user, program or process should have only the minimum privileges necessary to access the information and resources in order to perform its legitimate function.

To do this, directors must make **cybersecurity a standing item at meetings and appoint a dedicated executive** to the role of liaising with IT services and security providers and reporting back to the rest of the senior team. The introductory video from Cyber Citadel, Board Directors Take Note![12] is a good starting place for leaders to get to grips with their role in improving cyber culture within their organisations. More information can be found in the detailed Guide for Board Directors[13].

People

For now, at least, **it is the people not the technology who make up an organisation**. When thinking about cyber risk, think first about **which staff are most vulnerable to attack**. This might be because they are a senior member of the organisation and have security privileges which make their digital credentials valuable to cybercriminals, or because they are client or public facing and therefore more exposed to third parties and external networks.

Another issue, highly applicable to many healthcare workers, is that **the stressful work environment means they are more susceptible to social engineering** tactics that often accompany phishing emails.

Whatever the reason, all organisations should **work under the principle of least privilege**, in which employees are given only the minimum amount of security privileges required to carry out their job. In addition, employees should not be permitted to access databases or company servers from public

12 https://vimeo.com/421446336
13 https://www.cybercitadel.com/cyber-security-guide-for-board-directors/

networks, or other private networks not protected by the organisation's firewall.

This may not be very practical at first. For example, if healthcare staff are required to do home visits, they may need to have access to certain databases whilst off site. Technology may be able to help here, for example an organisation could **set up a VPN (a Virtual Private Network) to enable staff to securely connect to an internal server** from an external network. Over the course of the pandemic, this has become a standard tool for many companies and it should now be applied to all remote connections going forward.

It is crucial that staff understand why such measures are so important, because then they will be far more accepting and likely to follow new protocols rather than cut corners. In turn, **it is essential that management and IT services take the time to understand employees' needs and facilitate their work**. Cooperation from both implementers and users is at the heart of successful cyber policy.

Processes

Identifying and addressing the risk of people is only valuable if standard procedures are themselves secure. The workforce needs to be directed to **use secure protocols** when connecting to servers and databases, for example by using a VPN and by logging in **with secure passwords**. Secure passwords themselves should be well defined and enforced by IT services: the same passwords should not be used for all logins, should contain a combination of letters, numbers and symbols, and should be changed after a substantial time period.

Furthermore, there should be **clear policies regarding the storage and sharing of data**. Data should not be stored on personal devices or on personal external storage platforms such as USB flash drives or SD cards. Any external hard drives storing sensitive data should only be used for work purposes and should be **encrypted and password protected**. Most now come with this feature and older storage devices should be retired in favour of these more secure newer editions.

All organisations should have a cyberattack response plan. All staff should know what to do in the event of an attack, and **good lines of communication** should be set up from IT services and information security officers to management staff who can direct their teams efficiently following an incident.

Lack of planning has been evident in recent attacks on the healthcare sector and has made worse the scale of attack and response time. In the case of Brno University Hospital in the Czech Republic, one head nurse reported having to improvise and use personal USB flash drives to back up their most essential data followed by a personal laptop tethered to a mobile internet connection to distribute emergency guidelines to their team via email.

Pre-existing data backups and the centralised distribution of carefully planned protocols and emergency procedures would have made a huge difference to the hospital's response. This team were lucky to have a manager that reacted so quickly and effectively, albeit using personal devices which is less than ideal. But many would have been left *completely* in the dark and without *any* saved data.

This really highlights the **importance of proper processes such as backing up data**: it should be done **regularly and using multiple methods**. Backups are the ultimate insurance against any cyberattack, but in particular ransomware, which is currently the most prolifically employed method of attack and one that leaves healthcare providers open to extortion.

Technology

The role of technology in cybersecurity can be summarised by addressing two questions.

1. What technology is currently present in the network and how much of the network vulnerability is a direct result of the technology itself?
2. How can the organisation best benefit from new technology, and how can it facilitate new approaches to more secure people and processes?

To answer the first, **an organisation must understand its network architecture**. In an ideal scenario, organisations should **employ a "Security by Design" principle** which means that security is considered as the network is built and each time a new element is incorporated into it.

However, the reality is that this has not happened in the healthcare industry. Rather the network has been built up over decades, with parts of it pre-dating the internet and much of it pre-dating serious cybersecurity. So, with the idea of starting over not feasible, we must **be realistic about the ways the network can be made more secure**.

Identify what aspects of the network design or what nodes of that network are making it vulnerable to attack.

The first thing a security provider such as Cyber Citadel would do is to run a scanner over the network to **search for systems running old software or software which has not been patched** with the latest security updates. Next, a full **Vulnerability and Penetration Test (VAPT)** should be run to highlight the weak spots of the network infrastructure and **highlight the components which need to be prioritised for improvement**.

Vulnerability and Penetration Tests (VAPT)

A vulnerability assessment is an automated comprehensive scan of a cyber network which detects technical vulnerabilities and can be used to inform a penetration test to increase its effectiveness

A penetration test is a human-led investigation involving an authorised, simulated, cyberattack on a computer system, performed to evaluate the security of the system and provide both technical *and* business solutions

Addressing update and patch problems can be an incredibly powerful starting point. For example, the devastating attack on the NHS in 2017 was mounted by the WannaCry ransomware which exploited systems using the Microsoft Windows 7 software that had not been patched[14]. This ransomware also attacked Telefonica, FedEx, Deutsche Bahn, and LATAM Airlines; the healthcare industry is not alone in its vulnerabilities and **everyone can learn from each other about mistakes made in network design and maintenance.**

Updating and patching should thus be a priority for any healthcare provider. Systems that cannot be updated or run supported operating systems should be reviewed and replaced. This will fortify the whole network, homogenise it, and make it far easier to monitor and maintain.

Particularly important in the healthcare sector is securing the outer perimeters of a network. **Many medical devices are now Internet of Things (IoT) devices**. Machines such as X-ray, MRI, and CT scanners are all connected to the network, allowing livestreaming of data and results to

14 https://www.acronis.com/en-gb/articles/nhs-cyber-attack/

control computers, and from here the data can be uploaded to cloud storage. Moving forward, an increasing number of healtcare providers are also now employing remote patient monitoring (RPM) using IoT devices which report on various vital measurements. Whilst these devices are expected to save the healthcare industry US$63 billion by 2022[15], they are digitally very vulnerable, and hackers may thus be able to access data through first breaching an IoT device, and then travelling laterally through the network.

One journal reported in 2019 that **82% of healthcare organisations experienced a cyberattack on their IoT devices**[16].

Attacks on such hardware devices are also becoming **increasingly sophisticated** and a recent article even investigates the use of deep learning techniques to add or remove medical data from 3D volumetric images[17], which demonstrates how attacks have gone beyond stealing or holding data to ransom and now might include malicious sabotage.

Two mitigations can help secure these vulnerabilities. The first is to **make regular backups of IoT device data** to more than one medium: do not just leave it to automatic uploads to cloud systems, or even to storage directly onto computer systems. Make regular backups to external drives which can be disconnected from the system and are thus unreachable to hackers.

The second mitigation is to **reconsider network architecture**. Specifically, **the network should be segmented to prevent any lateral movement** of malware across it. A department such as medical imaging, with many IoT devices making huge data acquisitions over long time courses should not be directly connected to other departments. Compartmentalising departments in this way will reduce the impact of targeted attacks and reduce the risk of individually vulnerable systems.

Quick Reference: The Essential 8

The Australian Government (Australian Signal Directorate, or ASD) recommends an ***'Essential 8'*** list improvements to cybersecurity which can be implemented to different levels of 'maturity' depending on the risk status of the business and the sensitivity of their data.

1. **Application control**
2. **Patch applications**
3. **Configure macro settings**
4. **User application hardening**
5. **Restrict privileges**
6. **Patch operating systems**
7. **Multi-factor authentication**
8. **Daily backups**

It is important to **be aware of the hardware and systems connected to the network**. Not just connected to the internet, but also to any data storage servers, intranet systems, or direct device-device connections (which can act as a gateway into the wider network). Often devices which may appear disconnected are in fact not, and it is these forgotten or unaccounted-for devices which pose the greatest risk, as they are not necessarily being monitored and will not be first in line for disconnecting in the event of an attack.

There are a number of good resources and checklists that can be used to help organise and direct cybersecurity improvements.

One such resource is the **Australian Signals Directorate (ASD) Essential 8** (see box), a list of eight guidelines for improving cybersecurity set out by the Australian Cyber Security Centre (ACSC)[18]. Although originally designed for businesses, they

15 https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/industries/healthcare
16 https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-a-cyberattack-on-their-iot-devices/
17 https://arxiv.org/abs/1901.03597
18 https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

provide an excellent starting point for public or private healthcare providers.

Another list of eight is provided by the UK National Cyber Security Centre **principles of zero-trust architecture**[19]. These are listed in the 'Quick Reference: Zero-trust Architecture' box.

In zero-trust architecture, **every aspect of the network is treated as hostile** and something connected to that network should not assume to be able to connect with everything else. Trust is then obtained by users, devices and services through authentication, device health and authorised access to services.

It is important to realise that **this will take time and cannot all happen at once**. Deploying a zero-trust approach should be done in phases, and of course all traditional security methods already in place should stay there during any transition period.

Even if an organisation decides that the zero-trust architecture model is not suitable or possible to deploy, there is much that can be taken away from its concepts.

Quick Reference:
Zero-trust Architecture

1. Understand your network structure: users, devices, and services
2. Create and require strong user, device, and service identities – these are the new perimeters
3. Know the health of your network users, devices, and services
4. Use well-defined policies to authorise requests
5. Authenticate everywhere, preferably with multi-factor
6. Focus monitoring on devices and services
7. Don't trust any network, including your own; trust can only be obtained by network users, devices, and services – not by a network itself
8. Use services with built-in support for zero-trust architecture

19 https://github.com/ukncsc/zero-trust-architecture/

KNOW YOUR REGULATIONS

Due to the sensitive and valuable nature of the data held by healthcare providers, the **regulations regarding data handling, sharing and storage are strict.** Below is a broad selection of some of the key regulations in place across the globe. Any healthcare provider would be wise to thoroughly investigate the legislation with which it must comply – in its own region or in any region it trades or exchanges data with.

GDPR

General Data Protection Regulation (GDPR) is a regulation in EU law on data protection on privacy. It is based on **seven principles**[20], and applies to any data within, from, or passing through EU nations. **In 2020, a series of guidance updates was published** which cover 'codes of conduct and certification', 'accountability', and 'criminal offence'[21].

The GDPR states that "83(4) GDPR sets forth fines of up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher."[22]

The 7 Principles of GDPR

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

NDB Scheme

The Notifiable Data Breaches Scheme is enforced in Australia through the Privacy Act 1988. **All organisations must take reasonable steps to protect the personal information they hold** from misuse, interference and loss, as well as unauthorised access, modification or disclosure. **This extends to situations where an entity engages a third party** to store, maintain or process personal information on its behalf.

NDB makes it mandatory for companies and organisations to **report data breaches** that are likely to result in harm to an individual whose personal information is involved to the Office of the Australian Information Commissioner (OAIC) and any affected or at-risk individuals[23]. The notification must also **include recommendations about the necessary steps that should be taken in response** to the breach.

The NBD Scheme imposes maximum penalties for misuse of personal information by entities covered by the Privacy Act, from $2.1 million for serious or repeated breaches, to $10 million, three times the value of any benefit obtained through the misuse of information, or 10% of a company's annual domestic turnover.[24]

20 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
21 https://ico.org.uk/for-organisations/guide-to-data-protection/whats-new/
22 https://gdpr-info.eu/issues/fines-penalties/
23 https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/
24 https://www.mccullough.com.au/2019/04/09/its-no-secret-10-million-penalties-to-be-introduced-for-privacy-law-breaches/

Privacy Act 2020 NZ

The Privacy Act 2020[25] in New Zealand is an update to the 1983 Act. The update mainly a**ddresses the transfer of information overseas** and is therefore also very relevant for any organisations trading with or within New Zealand. It also imposes a requirement for organisations to **notify the Privacy Commissioner of a data breach**, similar to the NDB scheme, and makes it **a criminal offence to mislead an organisation over personal information or destroy data if it has been requested**.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA)[26] is federal legislation in the United States which constitutes **three parts: the Privacy Rule, the Security Rule, and the Breach Notification Rule**. The Privacy Rule establishes the permissions and required uses and disclosures of protected health information. The Security Rule sets the requirements for the confidentiality, integrity and availability of electronic health data. And the Breach Notification Rule requires all enterprises to provide notification following a data breach.

HIPPA imposes fines that can range from $100 to $50,000 per violation (or per record), to a maximum penalty of $1.5 million per year for each violation.[27]

PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA)[28] is the Canadian counterpart legislation, although in this case **only really applies to private-sector organisations** which have commercial activity. Public healthcare facilities such as hospitals are generally governed by provincial laws, and federal agencies governed by the Privacy Act. However, **PIPEDA may apply in certain circumstances and healthcare professionals themselves may be governed by a combination of these**, so extra care must be taken to ensure all requirements are met.

Under PIPEDA, if an organisation is found to be knowingly in breach of PIPEDA requirements, they can be fined up to $100,000 for each violation.[29]

Health Data Law UAE

Following on from the introduction of GDPR, the UAE imposed **new centralised regulations** under the Federal Law No. 2 of 2019 (Health Data Law)[30]. This legislation roughly follows GDPR and is based on four sections as outlined in the box.

Health Data Law UAE

- Data processing
- Data security
- Data localisation
- Data retention

Sanctions imposed under the UAE Health Data Law for non-compliance include the potential suspension or withdrawal of the licence to use the central IT system, a formal notice or warning from the relevant health authority, and/or fines ranging from AED1,000 to AED1,000,000.[31]

25 https://www.privacy.org.nz/tools/knowledge-base/view/535
26 https://www.cdc.gov/phlp/publications/topic/hipaa.html
27 https://compliancy-group.com/hipaa-fines-directory-year/
28 https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
29 https://www.privacypolicies.com/blog/costs-non-compliance-privacy-laws/
30 https://www.pwc.com/m1/en/publications/healthcare-data-protection-in-the-uae.html
31 https://www.pwc.com/m1/en/publications/healthcare-data-protection-in-the-uae.html

OUTLOOK

More so than ever before, the healthcare sector must be digitally protected.

The risks of cyberattack are now potentially catastrophic and so organisations cannot sit passively on outdated and poorly secured networks hoping that they will not be targeted. Evidence over the last year shows that this will prove disastrous and if an attack on the scale of the NHS ransomware attack of 2017 were to occur during the pandemic, the effects would be devastating.

Healthcare as an industry, which must include everything from Research and Development, to hospital facilities, pharmaceuticals, and local authorities, must pull together and **work on proactively securing networks, segmenting vulnerable systems, backing up data, and securely communicating with each other**. Time and resources must be invested, but much can be done without breaking the banks of health service organisations. Training, response plans, and IT services and executives effectively communicating will build more cyber-aware workforces and cyber-secure organisations.

Although there is now an abundance of regulation across the globe, there is great diversity to the interest and approaches of nation states. Whilst some governments are taking the initiative to improve the security of the health industry, other countries are yet to even pass data privacy laws. **Healthcare as an industry must therefore drive its own digital revolution.** By following the principle of security by design, the sector can **introduce new technology to improve efficiency whilst maintaining security and meeting regulatory requirements as and when they are introduced**.

In the absence of government aid, it will be imperative for facilities to **identify and prioritise the most critical vulnerabilities**, and third-party security providers such as Cyber Citadel can be there to provide guidance and support to achieve this in the most cost-effective manner.

One thing is certain: in the post-Covid era the healthcare sector is seen more than ever as a critical national industry. This has made it a prime target for cybercrime, whether it be for data theft, espionage, or for pure chaos. **The sector must act now to protect its data and ultimately save lives.**

Cyber Citadel

Jonathan Sharrock
jonathan.sharrock@cybercitadel.com

www.cybercitadel.com

Cyber Security specialists

With highly-satisfied clients in over 26 countries across 5 continents, we provide Penetration Testing, Vulnerability Assessments, Red Teaming, Incident Response, Malware Analysis, Asset Discovery, Source Code Review and Forensic Analysis.

We have particularly deep expertise in multi-lingual Web Application and Network Infrastructure Penetration Testing.