The cyber threat to care homes

Healthcare Practice
April 2022

LOCKTON®

Introduction

Care homes are a safe haven; a space for individuals requiring specialised attention, care and support. To date, there are around 5,500 care providers operating in 11,300 care homes across the United Kingdom, housing over 400,000 residents.[1] As part of the healthcare sector, providing specialist assistance combined with daily activities, care homes support residents with their medical requirements and needs, delivering skilled and cohesive support.

Notwithstanding the inherent nurturing character of the healthcare sector, no sector is immune from targeted cyber-attacks.

With the evolution of digitalisation, and the emergence of new technologies within the healthcare sector, care homes are adopting technological advancements into their practices and operations. They are now more connected to the wider healthcare ecosystem than ever before. Historical and current medical records, daily recordings of vital signs, treatment plans and other confidential and sensitive data, flow between hospitals, clinics and care homes, improving the quality and efficiency of the services provided.

One emerging technology in particular, the Internet of Medical Things (IoMT), or healthcare IoT, is revolutionising the healthcare sector. IoMT applications are being utilised to improve treatments, manage diseases, reduce errors, improve patient experience, manage drugs and lower costs.[2]

This technological revolution is welcomed and is clearly here to stay. However, commensurate with the considerable positive impact of these technologies, there are emerging threats. The greater the demand for technological speed, efficiency, convenience and control, the greater the vulnerability to cyber events.

In the midst of this digital advancement, the security, safety and wellbeing of the residents, employees, and other third-parties, must be identified, understood and mitigated.

Types of cyber threats

External threats

The types of external cyber threats are wide and diverse. Each threat is driven by a specific motive and a desired end result, with consequences as varied as the threat itself. External threats loom large and necessitate a strong cyber security stance.

Data breach

The ICO defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".

Denial of service attack (DOS)

A method of taking a website out of action by overloading or 'flooding' the server.

Port scanning

A technique employed to identify open ports and services on a network, potentially with a view to exploiting weaknesses illegally.

Whaling

A type of spear phishing (i.e. specifically directed) attack, such as an e-mail spoofing attempt, that targets senior members ('big fish') of a specific organization, seeking unauthorized access to confidential data.

Malware

Malicious software that involves programmed code or scripts designed to disrupt the performance of PCs, laptops, handheld devices, etc.

Pharming

A method of deceiving an individual into ending up at a fake website, even though the correct URL has been entered.

Theft of data

Stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.

Web application based attacks

Any attempt by a malicious actor to compromise the security of a web-based application, including, for example SQL (Structured Query Language) injection attacks which attempt to access and manipulate databases.

Spear phishing

The same as phishing, except that it is a directed attack against a specific target.

Doxing

Discovering and publishing the identity of an internet user, obtained by tracing their digital footprint.

Phishing

A method of accessing valuable personal details, such as usernames and passwords, often through bogus communications such as emails, letters, instant messages or text messages.

Locked accounts

Where customers are (usually temporarily) unable to log into their accounts as a result of criminal activity on systems such as, for example, DOS attacks.

Social engineering

In a cyber security context, the general art of manipulating people online so they give up confidential information.

Ransomware

A type of malware that prevents the use of a system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

Internal threats

Despite the measures that could be taken to protect the network perimeter, no number of fire walls, multi-factor authentication methods or versions of antivirus software, will protect a business against insider threats. Cyber risks are not always external or malicious; they can and do originate internally within an organisation.

Insider threat profiles include:

- **Negligent insiders:** human error/negligence, employees unintentionally mishandling data (either directly or through lost devices), or compromising security (e.g. phishing emails, incorporating unclean memory sticks, inappropriate use of social media/posting photos etc.)
- **Criminal and malicious insiders:** deliberate criminal acts including mishandling of data or compromising network security for personal gain
- **Credential thieves:** those who target insiders' login information.

Cybersecurity risks particular to care homes

Sector specific

All organisations have a cyber risk but what are the cyber risks particular to the care home sector?

- Many businesses in this sector operate with modest cybersecurity budgets, limited IT support and outdated IT systems. Funds are often allocated towards operational necessities rather than cybersecurity measures and frameworks, making care homes a vulnerable target for cyber threats. Cybercriminals actively select organisations that are perceived as valuable or an easy target.
- Care providers handle large volumes of personal and sensitive information relating to the residents, the residents' family and other third-parties. Some of the information is highly regarded by cyber criminals as much of it is 'static information', i.e. information that cannot be changed, such as National Insurance numbers. These data command a high price on the Dark Web as they may be utilised for identity theft and other fraudulent activities.
- The sharing of data with other health professionals through common online channels and platforms creates a wider threat surface. The networks may be used to gain access to larger healthcare organisations and governmental bodies, leaving the care homes vulnerable to liability claims.
- Cybercriminals may manipulate, destroy or hold to ransom, electronic medical or other sensitive data. Again, this potentially leaves the care home open to liability claims, regulatory investigations and reputational damage.
- The use of wearable and ambient devices, which allow carers to monitor the health, safety and wellbeing of the residents on a consistent basis (reducing the frequency of physical check-ups) is a vulnerability. If those devices are connected to a server, cybercriminals can potentially hijack the devices, and disrupt their function.
- A cyber incident may cause a network outage, causing vital medical data to be inaccessible, including in the context of obtaining prescriptions.

It is crucial for all healthcare organisations, especially those which may have limited cyber resources, such as care homes, to understand thoroughly the diverse nature, impact, and origin of cyber risks, and to prepare for them effectively.

When care homes suffer a cyber-incident, the losses may be significant and varied.

Unlike other sectors, where the impact of cyber events may typically include financial loss, business interruption or reputational damage, consequences in the healthcare sector may extend to the health and safety of individuals. This fact alone puts this industry in a category of risk all of its own.

Cyber risk management

Regardless of the origin of cyber exposures, implementing a robust cyber risk management framework is crucial. It is important for care homes to consider four parts of the process:

Governance

Cyber risk is not 'just' a technical issue but an organisational risk that threatens all aspects of care homes and needs to be dealt with at governance level, as the operational, financial and reputational consequences of a cyber-incident may be detrimental for the survival of any healthcare organisation.

To protect the organisation appropriately, the management team must ensure clear responsibility and ongoing vigilance.

Despite the recent surge in cyber-attacks, and particularly ransomware assaults, research by the Institute of Directors indicates a disconnect between the IT staff, who live and breathe cyber-security and understand the consequences, and the management team.

It is vital that there is a strong alliance between the management and the organisation's cyber risk professionals; not just communication of the relevant cyber performance figures, but also the contextual and situational awareness to bring those performance measures to life.

The cyber threat does not stand still — it is a dynamic environment that requires constant monitoring to allow for the development of appropriate response measures.

Human factors

Human error remains the greatest cyber threat to any organisation and arguably the most underrated.

Error can manifest in many ways, including:

- clicking on phishing links;
- inadvertent data breaches or sharing of other sensitive information;
- weak passwords;
- inappropriate use of public Wi-Fi; and
- failing to implement software updates regularly.

Investing in cyber security awareness and education for employees is critical and dynamic, as threats change and become increasingly sophisticated.

Security

Taking account of the rapidly changing cyber space and the varying motives driving cyber-attacks, care providers are urged not only to understand the nature and types of cyber risks, but also the gaps and weaknesses within their operational models that increase their exposure and appeal to cybercriminals. This might include, for example, software vulnerabilities, lack of cyber expertise, weak cybersecurity and hygiene, and dependence on IoMT.

As cyber-attacks morph and threat actors find new ways to exploit vulnerabilities and avoid detection, it is vital that care providers look very closely at their cyber hygiene protocols.

Examples of good protocols include:

- multi-factor authentication for remote access (MFA);
- an endpoint detection and response (EDR) solution rolled out across the IT environment;
- privileged access management (PAM) and permissions across the IT environment;
- secure offline backups;
- an Incident Response Plan specific to ransomware that is updated and tested regularly;
- a Business Continuity Plan addressing network outages, off-line communication, and data recovery protocols;
- remote desk protocol access from outside the network;
- updated software and patching protocols;
- high-level employee awareness training;
- password management software;
- vulnerability assessments, including penetration testing, red-teaming and table-top exercises; and
- appropriate separation of Operational Technology and Information Technology.

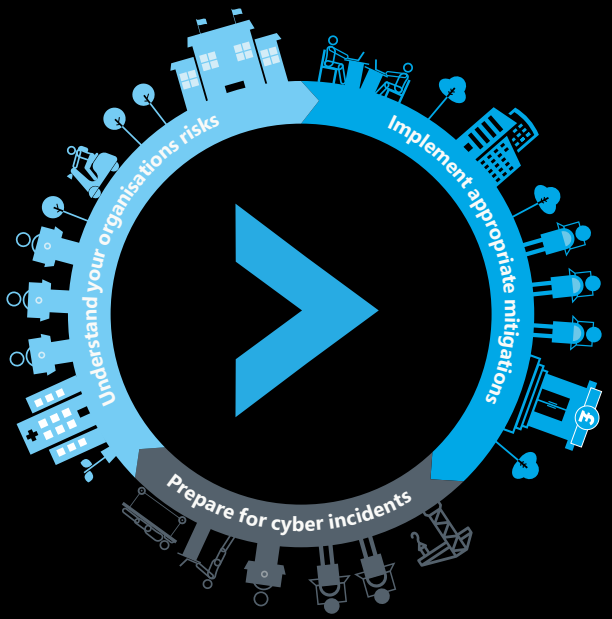
Partnering with a good cyber security firm will be of real benefit in the identification and mitigation of cyber threats, both internal and external, such that an organisation is well-protected from cyber threats but also adequately prepared in the event of the organisation experiencing a cyber incident.

The below chart from the National Cyber Security Centre highlights 10 steps to cyber security.

National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. The NCSC recommends you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.



1. **Risk management** Take a risk-based approach to securing your data and systems.
2. **Engagement and training** Collaboratively build security that works for people in your organisation.
3. **Asset management** Know what data and systems you have and what business need they support.
4. **Architecture and configuration** Design, build, maintain and manage systems securely.
5. **Vulnerability management** Keep your systems protected throughout their lifecycle.
6. **Identity and access management** Control who and what can access your systems and data.
7. **Data security** Protect data where it is vulnerable.
8. **Logging and monitoring** Design your systems to be able to detect and investigate incidents.
9. **Incident management** Plan your response to cyber incidents in advance.
10. **Supply chain security** Collaborate with your suppliers and partners.

Risk transfer

An important risk mitigation process is the transfer of risk to insurance.

Contrary to popular belief, property, casualty and other traditional policies are not always designed to respond to a cyber-incident. In fact, in the last several years, insurers in these areas have taken steps to specifically exclude coverage related to a cyber-attack from their policies. Specialist cyber insurance is often a better option. Although some overlaps exist, as they do with all lines of insurance, traditional insurance policies lack the depth and breadth of standalone cyber cover and will not come with experienced cyber claims and incident response capabilities. Insurers in non-cyber markets have not always fully considered the implications of cyber exposures, nor have they tackled the potential aggregation over their various types of policies.

Cyber insurance

Standalone cyber insurance is a relatively recent form of insurance that, in general terms, covers losses relating to damage to computer systems and networks and privacy-related breaches. Issues relating to data breaches are typically included because they often arise in the 'cyber' context.

Cyber policies have matured considerably since the earliest policies were developed some 25 years ago. While cyber insurance has not traditionally formed part of the 'standard business insurance suite', the exponential rise of cyber threats means that for any organisation, a standalone cyber policy should no longer be considered a discretionary spend.

A market-leading cyber policy will have two components:

First-party coverage

This cover typically extends to the insured's own costs, including:

- breach response costs. A fundamental part of a standalone cyber policy is the first party breach response services, i.e. a breach "team" which includes the provision of IT forensic consultants, legal counsel, and public relations and crisis management consultants. Their focus is to investigate the incident, mitigate damage and ensure the business is operational again as soon as possible. This assistance is very welcome when the business is in a particularly vulnerable position post-incident. Cyber threats create considerable pressure, confusion, and concern, so having immediate access to experts, including experienced ransom negotiators where necessary, is critical
- extortion demands
- extortion expenses (e.g. ransomware negotiations)
- digital asset losses
- computer hardware losses
- business interruption losses and
- reputational harm reimbursement.

Third-party coverage

This cover typically extends to damage and costs in relation to third party claims, including:

- privacy third party liability, including for data breaches and the failure to protect confidential information
- privacy regulatory fines and expenses (to the extent insurable)
- system security liability to third parties for cyber events, such as spreading of malware to third parties
- liability to others for disruption of services or products.

Cyber purchasing process, limits & cost

Each insurer will have a multi-page application for what it considers to be normal elements of a healthy and secure network. Generally, insurers will want to know how a business is performing in the following areas:

People

- Training and awareness
- Access control

Process

- Governance frameworks
- Policies and procedures
- Management of vendors
- Management systems
- Audit regimes

Technology

- System design
- Software configuration
- Encryption protocols
- Detection and monitoring

The cost of a policy is based upon the limit of liability sought, together with the risk perceived by the insurance underwriter. There is generally no set formula nor 'standard' premium, although underwriters will take into consideration the size of the business' revenues, the amount and type of sensitive data it holds, and the risk controls in place.

Any limit purchased needs to be weighed against the perceived exposure of the organisation. Listed below are some broad considerations, though these should be discussed with your broker prior to settling on an appropriate limit.

- Breach response costs such as IT forensic fees to triage, contain and then rebuild systems, legal advice (necessary in the aftermath of an incident), as well as any notification costs required. An estimate of these costs should be undertaken to gauge exposure.
- There has been an exponential growth in ransomware threats over the past few years. The healthcare sector is a vulnerable industry due to the number of sensitive data records held. Ransomware can come with a sizeable ransom demand. These types of claims are now regularly hitting six and sometimes seven or eight figures.
- Another key exposure for any care organisation, again based on the sensitive data held, involves estimated costs of dealing with potential privacy breaches.
- Business interruption losses i.e. while the business or the systems may be offline. Also important in this context will be the 'waiting period' – the period of time which must pass prior to a valid claim being notified (typically 10-12 hours). The degree of comfort will vary from business to business.
- The impact of 'silent cyber' must also be considered. Historically many businesses may have relied on more traditional policies (particularly a professional indemnity (PI) policy) for some 'silent cyber' cover in the event of a cyber-incident (i.e. cover which is non-affirmative but nor is it specifically excluded). From 1 January 2021, Lloyd's markets require cyber-related losses in PI policies to be dealt with more clearly i.e. cyber cover must be specifically affirmed or excluded. Non-Lloyd's markets are also reviewing their positions. This could mean that there is limited or reduced cyber cover available under an existing PI policy, thereby increasing the need for a standalone cyber policy. (Even if cyber cover is affirmed, it is important to note that PI polices may only include limited (if any) first-party costs). If there is an existing cyber-policy in place, the limit ought to be reviewed.

Cyber market appetite

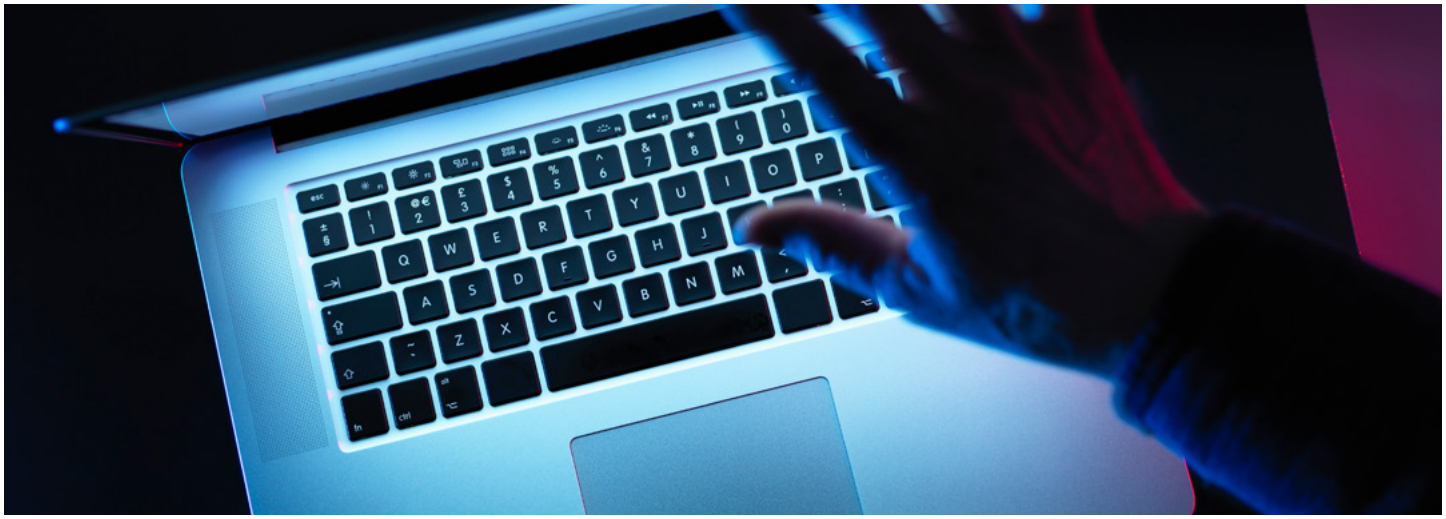
The cyber market continues to harden as ransomware losses hit the marketplace with regularity, driving the following responses from cyber underwriters:

- Retentions are typically being increased.
- Coverage is often restricted by the inclusion of ransomware-related sub-limits and coinsurance (or both).
- Where sufficient cyber hygiene controls are lacking, ransomware-related exclusionary language is increasingly common.
- Minimum rate increases of 80% - 100% are typical, even for clean risks with best-in-class controls.
- Rate increases of 100% and above are not uncommon for highly exposed industries, such as healthcare.
- Supply chain exposure is causing reverberations around the marketplace and sharpening underwriter focus. Additional questions are being asked of clients specifically in relation to their exposure to the Accellion, Microsoft Exchange, SolarWinds, Kaseya and Log4j events.

Greater scrutiny around security controls, which mitigate the ransomware threat, are also front and centre of the markets' underwriting process.

Note

- Typically, theft of funds is not covered within a cyber policy. A separate crime policy might be appropriate for this type of cover.
- Bodily injury and property damage is typically excluded from a cyber policy.



Lockton's credentials

Lockton's global cyber and technology team of more than 20 specialist cyber brokers and advisors offers a wide range of expertise in risk identification, protection and management.

How we work with our clients

We support our clients by maximising insurer interest to obtain best terms. We ensure the pre-submission stage is comprehensive and that every point is reviewed so that our clients are not negatively impacted by a lack of information. Our leading proprietary wording is supported by some of the biggest syndicates. The wording is updated annually and has backed some of the largest claims in the market. Our expertise is integrated, with our cyber claims specialists working alongside the placement team.

References

1. https://www.gov.uk/government/publications/care-homes-market-study-summary-of-final-report/care-homes-market-study-summary-of-final-report

2. Alsubaei, Shiva & Abuhussein (2017). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment

Get in touch

To learn more about any of the information above, or to find out how Lockton can help you mitigate these risks, please do not hesitate to get in touch with us.

Contact

Andrew Nicholson
Partner, Head of Healthcare Practice
Lockton Companies LLP

E: andrew.nicholson@lockton.com

Authors

Vanessa Cathie
Vice President
Lockton Companies LLP

E: vanessa.cathie@lockton.com

Reem El Khatib
Risk and Research Manager
Lockton Companies LLP

E: reem.elkhatib@lockton.com

Independence changes everything

10466