Crack down
Home Office urged to tackle rogue operators

A long hard look
Care is no longer seen as a last resort

Aedifica
Investor deepens relationship with Bondcare

MAY 2024 | VOLUME 32 | ISSUE 2

CM CareMarkets

Independent. Intelligent. Insightful.

Market volatility

Heading to the polls

LaingBuisson
INTELLIGENCE + INSIGHT

With care homes adopting technological advancements into their operations and are now more connected to the wider healthcare ecosystem than ever before, **Claire Williams**, principal associate at Mills & Reeve, explains that it also increases vulnerability to cyber events

Safeguarding data & business operation

With increasing digitisation of healthcare records, communications and decision-making, care home operators face an array of cyber security threats. These threats, both internal and external, have potential to jeopardise patient safety, imperil data integrity, create reputational damage and interrupt operations to the detriment of residents, staff and shareholders. Steps can, and should, be taken to understand and plan for each risk, maximising your ability to respond. The risks attached to cyber incidents are significant and can ultimately result in business failure.

Understanding cyber threats

External threats are well known. In ransomware attacks, malicious software infiltrates systems, encrypts data, and the third party controlling that malware demands a ransom for the data's release. In May 2017, the 'WannaCry' ransomware affected over 60 NHS trusts (as well as healthcare facilities worldwide), leading to an inability to view patient records, cancellation of surgeries, diverted ambulances and difficulties for patients to access their doctors. The cost of that attack to the NHS has been estimated at around £92m.

Phishing attacks, a leading cause of personal data breaches in the healthcare sector,[1] use deceptive emails or messages to entice users into revealing sensitive information. Phishing emails have developed in sophistication and can be indiscernible from a legitimate email to the causal viewer. In 2021, the Irish Health Service Executive was infected by malware originating from an innocuous Excel attachment to a phishing email, which ultimately shut down 80% of the organisation's IT systems, causing a cascade of cancellations, equipment failures and treatment delays. Full recovery of the systems took over six months.

Coordinated denial of service attacks such as that affecting several public healthcare institutions in Singapore in 2023 are relatively easy for the disaffected to arrange. Flooding servers with requests can readily overwhelm networks to disrupt services and compromise patient care.

Cyber threats are not always from an external source. Your people are generally your biggest asset as a care home operator, but in certain instances they may be a serious risk. With access to an organisation's hardware, a disaffected employee may have ample opportunity to damage the vital operational systems upon which the business relies. USB connections, ineffective access controls and poor security practices are all possible gateways for the motivated individual to attack.

Complex landscape

In today's rapidly evolving health and care sector, harmonious data exchange between different systems and their stakeholders is crucial. It enables patients to transition seamlessly between providers, which improves user experience and reduces costs.

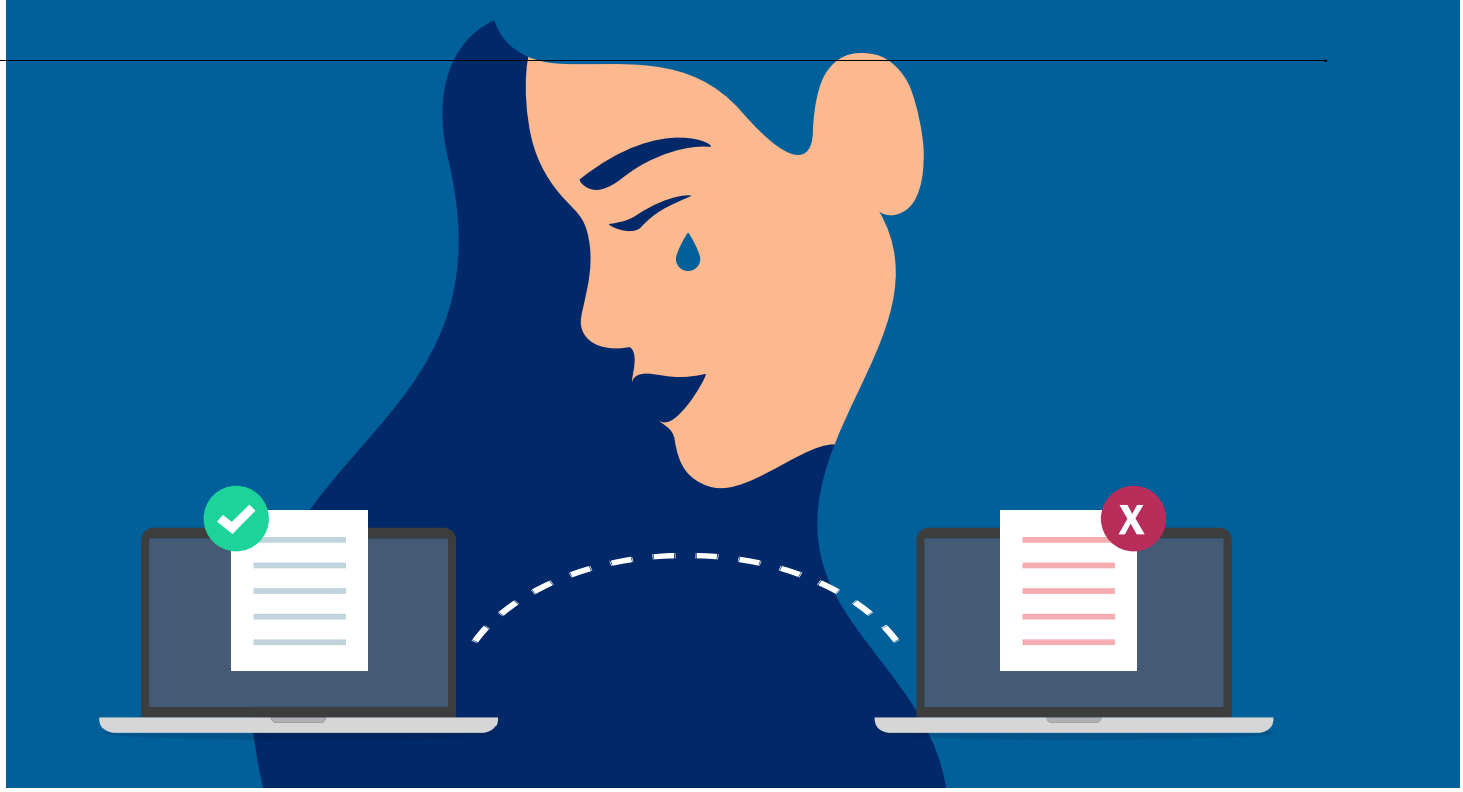
Electronic health records have become commonplace in the health and social care systems of many high-income countries. Early adoption of digitisation in advanced economies enabled rapid improvement, but now leaves the sector with a growing problem – that of fragmentation. Providers in the UK often use multiple separate electronic record systems which tend not to (but must) communicate well with each other.

The use of multiple, disparate systems poses a cyber security risk as each system contains inherent vulnerabilities. A single point of failure in one system provides an entry point for a malicious actor to exploit. Once within a relevant security perimeter, a third party may readily move from one system to another until internal scanning highlights an issue. In the absence of scanning and monitoring methods, identification of such internal movement can take many months. In the Irish Health Service Executive example mentioned earlier, the virus introduced moved undetected through the systems for eight weeks before the malware was activated.[2]

Balancing security and care continuity

Cyber resilience demands significant planning and investment. Operators must allocate monetary and operational resources for appropriate and robust security, including access controls, firewalls, and intrusion detection systems. Software and hardware must be continually updated, and appropriate specialist staffing or third-party support must be retained. Balancing resource allocation between operational necessities and cyber security is a key concern.

Security measures are crucial but



do need to be tailored to the organisation and circumstances. They must be designed with an understanding of the organisation's staff and their needs in mind. Every layer of access control has the potential to impact on the care that the employees can provide.

When security measures disrupt workflows (e.g. where there are frequent password prompts), it can hinder ability to provide timely care. Ill-planned or overly complex changes to security measures may lead to spikes in support requests, which must be addressed promptly. Frustrations with systems result in higher staff turnover and thereby hinder the ability of care homes to provide their services and prevent user dissatisfaction.

Risk-based prioritisation

Risk assessment plays a pivotal role in making appropriate security decisions, allowing care providers to proactively manage potential threats. Armed with a risk assessment that covers the financial, legal, reputational, operational and clinical risks that may result from different types of cyber security breach, care home operators can triage issues based on their severity and potential impact. By understanding and prioritising threats across various domains, you will enhance your resilience while maintaining effective service delivery and limiting your regulatory exposure.

Essential interventions

Interventions appropriate for each care home operator will vary but are both technologically and organisationally focused.

From a technological perspective, care home operators should look to implement multi-factor authentication to ensure that only authorised personnel can access sensitive systems. At the same time, datasets should be segregated so that employees can only access data relevant to their role.

An outward facing security perimeter must be established, including encryption and the use of firewalls to filtering incoming and outgoing traffic. To counter internal threats (and to catch those which slip through the external barriers) intruder detection systems are needed to monitor network activity for suspicious behaviour and alert staff to potential threats.

A significant reason that the 'WannaCry' ransomware affected the NHS so badly in 2017 was the failure of the organisation to apply a known fix for a software issue (a 'patch'). Regularly updating operating systems, applications, and software patches addresses security vulnerabilities. Use of reliable anti-virus software helps detect and prevent malware infections. Equally, regularly backing up critical data ensures that it can be restored in case of data loss due to cyber incidents or hardware failures.

From an organisational perspective, pre-planning the steps to take during a security breach in a hard copy incident response plan increases the possibility of mounting a coordinated and effective response. Any plan must, of course, be tested at regular intervals to identify gaps and refine procedures.

Care home operators must also build into their contacting processes a means to evaluate the cyber security practices of vendors or partners who may have access to their systems or data, with ongoing checks made periodically throughout the relationship.

Finally, staff should be properly trained to use the systems provided to them, as well as receive guidance to enable them to identify and report phishing emails and other suspicious activity.

Success in combating cyber threats hinges on the attitude, capabilities, and investment made by care providers. By fostering awareness and implementing effective cyber security measures, care homes can protect their data, their reputations and the quality of the services they provide.

NOTES

1 https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/#:~:text=Phishing%20is%20a%20leading%20cause,increase%20of%2033%25%20from%202021 (accessed 5 April 2024)

2 https://www.knowbe4.com/hubfs/UK-Ireland-Report_EN-US.pdf