IBM **Security**

5 key considerations for **healthcare organisations** when tackling cyber security during COVID-19

1. Digital shifts during COVID-19 mean security attacks are changing

The COVID-19 pandemic has led to dramatic digital shifts in health and care; the move to online consultations is one example and staff have been redeployed. In turn, we have seen the overall threat model starting to evolve as attackers use the vulnerabilities of this change to compromise system services. As the threat landscape changes, preparation can be key. Organisations can help prepare for the next attack with structured incident response planning.

2. Cyber security capabilities must evolve as the landscape changes

Continual review of cyber security is essential to keep up with emerging opportunities and risks. Regular assessments can provide an understanding of the cyber security baseline, in order to make informed decisions on what to put in place to help mitigate new or re-prioritised risks.

3. Understanding the risk benefit of digital transformation can help break down cyber security barriers to change

With a sudden trend in home working, and a rapid shift to caring from home or within the community, more data and devices are open to vulnerabilities. Shifting healthcare services or interventions to digital systems involves risk, but by analysing the risk benefit of technical vulnerabilities in terms of patient safety and mitigating it, cyber security teams can help enable digital transformation that can potentially benefit the patient experience.

4. Cyber security should be ingrained across organisational strategy

There are 24.8 million attendances in A&E per year across the NHS in England[1], and a high percentage of those have diagnostic treatment, including medical imaging, which is digitised across the NHS. A cyber-attack in this area is more than an IT issue; it could lead to an A&E backlog, ultimately having the potential to create a patient safety issue. Changing the language of cyber security to reflect its impact on patient outcomes and care quality can help to normalise it as part of an organisational strategy, instead of an add-on initiative, and can help engage board level and executive management from the outset. A clinically-led approach to vulnerability ranking and threat intelligence can be a powerful opportunity to impact patient care.

5. **Collaboration can be key to success; we can learn from other industries, across the public sector, academia, other trusts and private organisations**

Learnings can be taken from other industries such as aviation, in terms of the transparent and anonymous reporting culture for near misses and incidents. The NHS shares common ground with other public sector organisations and can take learnings in areas such as protective monitoring and designing strong network architectures. The data security and information governance regime[2] from NHS Digital along with their Data Security and Protection Toolkit[3] means that trusts can collaborate on an individual level as well as a national level to understand cyber security maturity in order to optimise it. Insights can also be shared from organisations such as IBM, that have cross industry experience and technical expertise.

Hear from your peers

Watch The King's Fund panel discussion on cyber-threats witnessed during the pandemic and how to be ready for future challenges, with input from NHS Digital leadership, Digital Health Lead at Imperial College London and leadership from IBM and a key partner.

Watch the webinar →

3 areas that healthcare organisations can review as part of their cyber hygiene process

Be prepared

With the threat landscape evolving and the nature of attacks changing, organisations need to have the right teams in place for rapid support and have the right planning in place to be prepared. IBM's X-Force Incident Response and Intelligence Services (IRIS) provides support with a 24/7 global incident response hotline, proactive readiness for a security incident, and COVID-19 health specific threat intel for improved resiliency and adaptation.
Learn more

Understand your security posture

Benchmark review is essential for organisations to understand where they are and where they want to get to. IBM's Rapid Cyber Resilience Assessment provides a NIST based assessment approach for conducting a quick, light touch review of the environment to identify the key risk areas in the face of the pandemic.
Learn more

Ongoing identification of threats

When an incident response plan is in place, and security posture has been reviewed, continual surveillance for future attacks is necessary to keep up with emerging opportunities and risks. IBM's SOC and X-Force Red vulnerability ranking enables clients to focus their time and resources remediating only the most important vulnerabilities – those that elevate risk the most, maximising the limited resources.
Learn more

Source:

1. digital.nhs.uk/data-and-information/publications/statistical/hospital-accident--emergency-activity/2018-19
2. digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance
3. digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit