Jun 18, 2020 17:46 BST

The link between patient safety and cyber security

Stuart Kurutac, security consultant at NCC Group

The healthcare industry is arguably one of the most appealing targets for attackers. The difficult choices to be made between spending limited funding on medical devices or security and the prevalence of legacy equipment, likely as an outcome of the lack of funds, are key in creating this attraction.

Although the NHS suffered quite severely from the WannaCry ransomware attack, it appears that various types of healthcare organisations in the US are continuing to experience continued and increased ransomware attacks in the

wake of 2017. These incidents have spurred at least one study looking at the long-term effects that ransomware attacks and data breach remediation steps have on the quality of care delivered by hospitals.

Although the link between cyber security and patient safety could be considered obvious to some, there are still, perhaps, several key stakeholders that may not have these two views aligned closely enough. How can we improve the awareness of the effect that cyber security issues pose to patient safety and outcomes?

How is clinical risk in IT systems currently managed?

The Mitre Corporation have developed a set of instructions for applying the Common Vulnerability Scoring System (CVSS) rating system to medical devices. The current version provides clarifications and examples specific to the healthcare industry and medical devices. For example, where patient safety becomes a concern, the guidance marks the relevant questions with PIPS (Potential Impact on Patient Safety). Identifying security issues and associating the impact they can have on patient safety will be valuable in removing the separation of clinical and cyber perspectives.

In the UK, there are two standards for clinical risk management developed by the NHS Digital Clinical Safety team, DCB0129 and DCB0160, which apply clinical risk to the manufacture, deployment and use of health IT systems respectively.

These standards could be used to apply more meaningful context in security assessments. For example, DCB0160 talks about Hazard Logs, which could allow security issues to be correlated directly to patient safety risks. Furthermore, using the information from the opposite perspective could allow additional security issues to be identified based on the safety risks and the associated mitigating controls. Additionally, engaging with a Clinical Safety Officer (CSO) where possible would undoubtedly prove beneficial, as they will help in understanding not just the impact from individual devices but from more complex systems, clinical workflow and the long-term effects on patient outcomes.

What does the future hold for patient safety and cyber security standards?

The healthcare industry is one of few sectors where we can correlate security issues directly to potential impact on human life. However, those assessing the security of healthcare devices must strike the balance between acknowledging this while avoiding increasing the risk rating of issues to a critical or 10 because of the patient safety aspect.

We also need to be conscientious that the recommendations we are making are appropriate for the situation. For example, using multi-factor authentication and password managers would be suitable for enterprise applications. However, applying similar protection mechanisms for systems that need to be accessed in an emergency would be too restrictive and negatively affect patient safety.

This is because legacy devices are common in healthcare settings, and in many cases, they do not have functionality of their own to be sufficiently secured by modern standards. However, they cannot simply be deactivated or replaced due to the critical care they still provide and financial constraints that prohibit new, expensive devices from being procured.

Ensuring physical controls are in place to prevent unauthorised users from accessing devices is one way to help reduce the negative impact on patient safety. Another is to implement network segregation so that legacy devices are isolated from other devices and IT infrastructure. If network connectivity to other systems is required, restrictions should be in place so that only essential services can send or receive data. These should not be long term mitigations – instead, they should be part of a policy that looks to schedule the decommission and replacement of devices based on the increasing risk they introduce to patient safety over time.

Cyber security issues are inevitable in technology reliant on software. Thankfully, a cultural shift away from the notion that organisations should be maligned for the presence of vulnerabilities in their products is happening. Whilst a number of Medical Device Manufacturers (MDMs) have public vulnerability disclosure programmes, this cultural shift needs to be encouraged and accelerated so that more MDMs engage with the security community and incorporate cyber security in the development of their products from the start. This will not only enhance patient safety before going to market but will also aid in achieving compliance more easily in an increasingly stringent regulatory landscape.

Ultimately, these and other initiatives should be implemented with the aim to create a widespread understanding of cyber security and patient safety as one and the same. With this mindset in place, the security industry and healthcare providers will be able to work together in a collaborative way, with patient safety front of mind.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970