Top 5 causes of cybersecurity incidents in Healthcare

5

Doing “just enough” to be compliant

Frameworks such as NIST 800-53 are great if you implement them with risk and privacy as the main driver, but if you only implement the minimum baseline, and conduct “checkbox” audits you are leaving risk on the table. The OCR provides a 9-point checklist for conducting a HIPAA compliant Risk Analysis and it is vital that internal security/privacy staff understand and implement this, or the entity uses a professional third-party cyber risk assessor to evaluate threats and vulnerabilities to PII/PHI assets. The controls in the framework help mitigate those risks, but they shouldn’t be the sole focus of the information security program.

4

Supply Chain/Third-Party risk

Healthcare providers tend to have large, and often complex supply chains. Hospitals and other provider buildings tend to be transient environments with patients, visitors, contractors, delivery people, etc. Historically we have seen a lack of investment in securing the supply chain or performing risk analysis of third parties. This has started to improve over recent years as more healthcare entities move to cloud based solutions and inherit a lot of controls from the Cloud Service Providers (CSP), but this isn’t a practical solution for a lot of the smaller companies and on-premise solutions, especially coupled with legacy systems, remain a huge vulnerability.

3

Legacy Systems

When budgets are not available for system upgrades there are often known vulnerabilities that can be exploited. The risk is increased when error messages are too descriptive; during Coalfire penetration testing we are often able to obtain application names, version numbers, patch status, etc. from uncredentialed pen testing. If we can do it, so can the malicious actors. With this information it makes it a lot easier to conduct spear phishing and gain access to specific systems which may not have been patched for a number of years.

2

Insider Threats

Sometimes malicious, but more frequently accidental. Hospital staff working long hours are susceptible to dropping their cybersecurity guard, for example clicking on links in malicious emails, or holding doors open to secure areas for unauthorized people. Inadvertently giving out small pieces of information on C-Suite and senior hospital staff which can be combined into a targeted Whaling attack is another vector to be considered.

1

Lack of, or poorly executed Risk Analysis

The most common Office for Civil Rights (OCR) finding during breach investigations is that a thorough Risk Analysis had not been conducted, and as such the vulnerability that was exploited should have been identified and mitigated. Budget constraints are often cited as the reason for not having regular Risk Analyses and some healthcare entities mistakenly purchase a (much cheaper) compliance gap assessment which only looks at meeting the HIPAA security rule requirements, not the threats to PHI.