



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Healthcare: Cyber Risk Continues to Climb, Industry Slow to Act

August 11, 2016

TLP: WHITE | *The NJCCIC assesses with high confidence the cyber threat and overall risk to the healthcare industry is high and increasing. In contrast to the large insurance breaches of 2015, assessed to be the work of Chinese threat actors conducting industrial espionage to support their largely state-run healthcare industry, profit-motivated hackers pose the greatest threat to the majority of healthcare organizations today.* As demonstrated by the continued increase in breaches, many healthcare providers have not yet adopted the necessary strategies and cybersecurity practices to effectively mitigate the elevated risk to their networks, systems, and devices. As of August 9, the US healthcare sector has accounted for 211 data breaches resulting in the compromise of at least 11.9 million records, according to the [Identity Theft Resource Center](#). The three largest incidents so far this year, exposing 9.2 million records collectively, involved the remote exploitation of a provider's network by external cyber threat actors.

- Arizona-based [Banner Health recently announced](#) the largest healthcare breach of 2016, which compromised the records of 3.7 million patients and employees, as well as customers who used payment cards at their facilities. Within the stolen medical records, the criminal hackers made off with social security numbers, insurance policy numbers, and claims information. In a separate healthcare incident announced this week, [Newkirk Products](#) began notifying 3.3 million Americans whose insurance information was accessed by an unauthorized source.
- Once compromised, insurance policy numbers and other protected health information (PHI) are often sold in illicit marketplaces on the [dark web](#) and can be fraudulently used to obtain medical services. On Monday, a [St. Louis woman was charged](#) with identity theft after using someone else's insurance information when admitted to a hospital on three occasions in 2015, resulting in \$20,000 of medical costs billed to the identity theft victim.
- In addition to the impact on patients and employees, the financial and operational consequences of breaches and other cyber incidents can be severe, and potentially crippling. On top of the costs associated with investigating and remediating a breach, complying with notification requirements, and providing victims with identity theft protection, HIPAA penalties have increased dramatically and are likely to continue rising. On August 4, [Advocate Health Care Network](#) agreed to a \$5.5 million HIPAA settlement, the largest to-date for a single entity.
- For several years, researchers have issued warnings of the potential for remote, malicious tampering with medical devices such as [pacemakers](#). However, [two successive intelligence reports](#) from the cybersecurity firm TrapX have demonstrated the threat to medical devices has already manifested in numerous real-world intrusions of healthcare organizations. The examples of compromised devices included magnetic resonance imaging machines, radiation oncology systems, picture archive and communication systems, and blood gas analyzers.

Healthcare organizations of all types and sizes must allocate appropriate resources to identify, evaluate, and mitigate cyber risk. For many, particularly private practices and smaller providers, this will require engaging with third-party contracted services in order to conduct network architecture reviews, vulnerability assessments, penetration testing, networking monitoring, and active defense against denial of service attacks and other malicious tactics.

- Regardless of an organization's size or role in the healthcare process, all computer systems, web services, and medical devices that receive, analyze, transmit, or store patient or employee data are potential targets for exploitation and must be secured and monitored for compromise. Additionally, extensive logging of network activity is vital to identifying, analyzing, and determining the nature and extent of intrusions, theft, or attacks.
- Two areas that all organizations can address to effectively reduce risk are email and user passwords. Awareness training for all employees and frequent reminders of how to identify email-based threats can reduce user-initiated malware such as [ransomware](#) and [Trojans](#). [User passwords](#) must be long and complex, and not shared across multiple accounts. Additionally, [two-factor authentication](#) should be implemented on all possible systems.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.