MANN GROUP
CYBERSECURITY

Ransomware and the HIPAA Security Rule

The U.S. Dept. of Health and Human Services (HHS) Office for Civil Rights (OCR) has published their fall newsletter titled *"What Happened to My Data?: Update on Preventing, Mitigating and Responding to Ransomware"*

The HHS OCR newsletter states that ransomware *"…attacks pose a serious threat to HIPAA covered entities, business associates, and the electronic protected health information (ePHI) that they hold."* They emphasize that complying with the HIPAA Security Rule offers significant protection from cyber attacks including ransomware. They focus on the following HIPAA requirements:

- *Risk Analysis (45 C.F.R. §164.308(a)(1)(ii)(A)) and Risk Management (45 C.F.R. §164.308(a)(1)(ii)(B)).* HIPAA requires an annual risk assessment and analysis from covered entities and their business associates. A recent study showed that only 40% of healthcare providers have completed an assessment within the last 12 months.

The Mann Group offers HIPAA risk assessments at a low price to healthcare providers and their business associates. We also help companies manage their supply chain to ensure business associates provide adequate cybersecurity diligence.

- *Information System Activity Review (45 C.F.R. §164.308(a)(1)(ii)(D))*. HIPAA requires an appropriate level of system monitoring and event management in order to detect and contain a breach. A recent study showed that 26% of hospital respondents and 93% of physician organizations currently report they do not have an adequate solution to instantly detect and respond to an organizational attack.

The Mann Group helps organizations navigate the swamp of security tools, products and vendors to identify needs based on the organization's unique risk profile. We also help companies document and manage their processes for monitoring, logging and review of security related events within their infrastructure.

- *Security Awareness and Training (45 C.F.R. §164.308(a)(5))*. HIPAA requires that employees are trained appropriately in order to minimize human error as a potential cause of an ePHI data breach. Exploiting human weaknesses to social engineering using targeted "spearphishing" has become the most common mode of ransomware attack. "Cyber Hygiene" should be part of every organization's training curriculum in order to equip employees with tools and information to protect the organization and themselves.

The Mann Group provides cyber hygiene workshops and instructor led onsite training at a low price. We deliver hands-on training for users on good cybersecurity habits. We also provide limited penetration testing and assessments.

- *Security Incident Procedures (45 C.F.R. §164.308(a)(6))*. HIPAA requires organizations have documented policies and procedures for managing security related incidents. These procedures can greatly limit the damage of an attack. HHS recommends organizations create response plans specifically for ransomware attacks. A recent study found that 87% of healthcare organizations have not had a cybersecurity drill with an incident response process.

The Mann Group helps companies develop and maintain their security incident management policies and procedures. We also facilitate pen & paper incident response drills and walkthroughs.

- *Contingency Plan (45 C.F.R. §164.308(a)(7))*. HIPAA requires companies have contingency and business continuity plans documented and maintained. An effective and robust contingency plan is essential to recover from a ransomware attack. The ability to reliably recover lost data with backups and resume operations as quickly as possible is crucial in healthcare for the sake of patient safety.

The Mann Group helps organizations develop and maintain disaster recovery and business continuity plans. We also facilitate pen and paper disaster recovery drills, and assist organizations with supply chain risks and contingency plans. We can help organizations work with their service providers to test backup and restore capabilities.

The OCR fall newsletter is a call for action to all healthcare providers, as well as their vendors and business associates, who can include law firms, managed service providers, insurance agents, testing and lab services, hospitals, EHR SaaS providers, cloud hosting providers, web hosting and application hosting providers. By following the HIPAA Security Rule in body and spirit, healthcare organizations can prevent or minimize harm to patients and themselves from the increasing cybercrime threat.

Mann Group Cybersecurity provides cyber risk management services for small businesses in the Pacific Northwest. Reach us by phone at 360-388-1286 or email david@manngroupit.com to schedule a free initial consultation or visit manngroupit.com for cybersecurity news and information about us.