Healthcare Under Attack: Tools for any Budget to Reduce Cyber Risks

By: Kevin Harried
Chief Risk and Compliance Officer, One Call

onecall®

As the healthcare industry continues to innovate service offerings, increase access to data, and create operational efficiencies using advanced technology, there's an increasing risk from cybercriminals who work tirelessly to evolve techniques that challenge our defenses. This constant threat of cyberattacks and security incidents has a direct impact on the workers' compensation industry - it is a reminder that preparation and constant vigilance are the only defenses at our disposal to ensure our information is safe and protected.

Why is Healthcare at Risk?

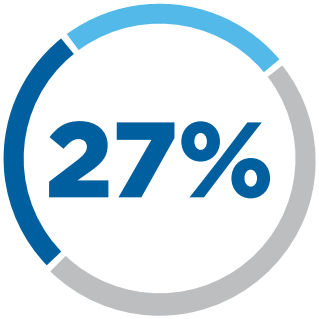
The data saved in electronic medical records (EMR) and handled daily by medical professionals is extremely valuable. It contains health, personal and insurance information used to commit insurance and identity fraud. Attackers don't even need to access healthcare systems to obtain information or disrupt services. They can use email to deliver sophisticated malware (viruses) to obtain records, ransomware to lock systems, and social engineering to trick personnel into providing data. Attackers like these methods because they are simple to deploy, hard to detect, and make any and all employees at your company a potential target – eliminating the need to compromise elaborate security systems.

Combat the Risks

We realize no company has unlimited budgets for security. Here are a few measures you can take, regardless of budget, to improve security.

Educate

Studies show human error causes at least 27 percent of all data breaches. This can be as simple as employees clicking on a link they believe is legitimate or responding incorrectly to an external inquiry. Educating employees on how to identify red flags and report potential threats can immediately reduce the risk and costs associated with a breach. In fact, the Poneman study points out that education programs can reduce the cost of a breach by up to $9 per record.



Studies show human error causes at least 27% of all data breaches.

Be Prepared

Studies show having a ready-to-go incident response plan and investigation team can reduce the cost of a breach by $14 per record. Treat a data breach drill as you would a routine fire drill. Just as a fire drill educates employees on their role during a building emergency, implementing and training a security first responder team will ensure you're prepared in the event of a potential data breach. Your team should be ready to quickly identify, report and respond to a problem. This can shorten the time of a data breach and assist crisis management personnel with communication to impacted stakeholders.

$14

Reduce the cost of a breach by $14 per record.

Actively Monitor, Identify and Escalate

The faster a potential breach is identified, the faster it can be contained. Statistics show companies that identify a breach in less than 100 days can save up to $1 million in post-data breach costs. Since no security is foolproof, the ability to rapidly detect, respond and contain a threat is just as important as prevention.

Data Classification

Garbage in is garbage out in this situation. Old data is bad data that collects rapidly if not destroyed when no longer needed. If maintained on your system, it also makes you vulnerable to an attack, even if you are not using it. Studies show eliminating old data can reduce breach costs by more than $5 per record.

Conclusion

An attacker only needs to be right one time to cause havoc, which means companies have to be right every time in order to prevent a security breach. This may seem like a tall order, but with the right preparation, education and monitoring, you can thrive in this rapidly changing technology-driven environment.

Reference: Ponemon Institute LLC. (2018). 2018 Cost of a Data Breach Study: Global Overview. IBM Security. Retrieved from https://www.ibm.com/downloads/cas/861MNWN2