Protecting patients' information

Deloitte's prescription: integrate cybersecurity from top to bottom

If you think having your credit card hacked is scary, Bari Faudree wants you to know that your digital health care record contains much more sensitive data. Cyber criminals already know it; on the black market, health records sell for an average of 50 times more than credit card information.

That's why health care organizations are attacked literally every day by people trying to access the wealth of personally identifiable information that's out there. The most dangerous threats may be outsiders masked as employees. "That's definitely a trend we're seeing," says Faudree, Cyber Risk Advisory Managing Director for Deloitte in the US. "It's causing a shift in thinking among health care companies because internal intrusions can go unnoticed for months and sometimes years."

Foiling thieves isn't health care company leaders' only challenge. They also have to prove to regulatory bodies that they have the cyber standards, controls, and vigilance necessary to prevent cyber risks and detect threats quicker.

That's why, in 2010, a major US health care organization accepted Deloitte US' offer to study and report on its ability to identify, detect, respond to, and recover from cyber threats. Based on that assessment, it engaged Deloitte US to assist in transforming its enterprise cyber security program, and helping it address regulatory compliance and operational efficiency.

"They viewed their primary needs from a technology perspective, so Deloitte US spent a lot of time with the board and leaders throughout the organization building an understanding of the benefits of a holistic approach to cybersecurity," Faudree says. "We ultimately changed executive leadership's awareness and perspectives, demonstrating to them how this was a business risk that required a deeper net of processes and mechanisms to manage cyber risks. They trusted our advice and made significant changes and investments that can help them more rapidly detect, manage, and respond to threats into the future."

During the past few years, Deloitte US helped the client design and implement new processes; conduct ongoing wargaming exercises; enhance its crisis management program; install an identity management solution for enterprise systems access; develop cyber playbooks to help it address cybersecurity incidents; train various stakeholder groups; and adopt an analytical approach to managing cyber risk that uses a dashboard to monitor its cyber risk posture.

"You know you're making an impact when you don't see the client's name on the evening news," Faudree says. "But, there are so many other positive outcomes of a comprehensive cyber approach that aligns with clients' strategic objectives. They can manage risk better, be more vigilant about compliance, and ultimately improve their ability to achieve their business goals."

Deloitte US and the client continue to work together to combat emerging threats. They currently are developing a ransomware playbook and wargaming exercise. "Infecting systems with malicious software that blocks access, then demanding money to remove the malware, is one of the hottest trends among cyber criminals," Faudree explains. "The fact that our client is ready to deal with that speaks to the higher maturity level of their program."

Learn more about Deloitte's Secure.Vigilant. Resilient.™ approach to cyber risk.