TOO LITTLE? NOT TOO LATE!

Terry Wilk, Senior Vice President | Coker Group

Has it happened to you or your organization yet? Are you paying attention to it? What are you doing to prevent it from happening? Do you have a plan to address it if it does happen? The "it" here is an event that has been occurring in other industries for years and we are beginning to see an alarming increase of these events in healthcare. The event is cybercrime.

Cybercrime is attacking healthcare in a big way. Almost daily, we read about security breaches in small, medium and large healthcare organizations that often effect hundreds, thousands or even millions of people and their private health and other personal information.

Cybercrime is an intentional attack against an organization's proprietary data assets. It describes any illegal activity in which a computer is used as a means to commit a crime against another individual's or organization's computer, network or data base. Cybercriminals are incredibly intelligent people who try to break into an IT infrastructure to snoop around, to inject electronic viruses and other malware, to expose, steal or destroy data, and to hold data and systems hostage for payment. It is a form of "digital mugging" with extremely serious ramifications.

Healthcare organizations have invested millions of dollars building massive computing capability, data bases, wired and wireless networks to connect people together to share information. Their goal is to facilitate communication, improve workflows, improve quality, lower costs and satisfy customers. But how much attention have these organizations given to protecting these investments from today's cybercriminals? Apparently, not enough as evidenced by the growing incidents of cybercrime in healthcare including recent ransomware payment demands. Unfortunately, digital mugging is on the increase along with security audits and six and seven figure penalty settlements.

How secure is your organization's IT infrastructure? What known and unknown 'holes' do you have in this infrastructure? What steps have you taken or should you take to protect your organization? Have you developed, communicated, and executed a formal IT security plan that proactively prevents, detects, and responds to cybercrime activities and enforces accountability throughout the organization?

Cybercrime can happen to anyone, anywhere. It is a critical business issue, not just a technical issue. Healthcare boards, executives and staff must take a direct interest in protecting their organizations from cybercrime. We need to work together to 'lock down' our IT infrastructures and ecosystems as tightly as possible and to stay alert to things happening in cyberspace.

To learn more about cybercrime and ways you can protect your organization from cybercriminals, contact Terry Wilk, Senior Vice President at twilk@cokergroup.com or by calling 678-832-2021.