Cybersecurity Now: Your Best Defence Is the Human Defence

November 2021 - Cyber-attacks against the Canadian healthcare system have increased at an alarming rate since the onset of the COVID-19 pandemic. Cybersecurity expert John Riggi points out that, “Cybersecurity is not an IT issue; it’s a patient safety issue.” and “Eventually, you will be breached. It’s not a matter of if, but when.”[1] All members of the healthcare community have a responsibility to take action to protect their clinic, team, and invaluable patient data.

An Escalating Threat

Cyber-attacks against Canadian healthcare organizations come in many forms. They range from attacks against individual physicians to large healthcare institutions, some of which have resulted in the exposure of thousands of patient records. Even before the pandemic, breaches were an increasing problem in healthcare. In 2019, 48 percent of security breaches in Canada were in the healthcare space.[2]

A dramatic spike in cyber-attacks has occurred during the pandemic. In the last two months of 2020, attacks on hospitals and healthcare institutions worldwide increased 45 percent – more than double the increase across all other industries. The dominant type of attack against healthcare organizations globally was ransomware, and Canada saw the largest increase at 250 percent.[3]

Targeting Busy Healthcare Professionals

Cybercriminals use “social engineering” to exploit natural human vulnerability and attack busy healthcare workers. The most common form of social engineering is “phishing”, which is an attempt to trick recipients into clicking on a link or downloading an infected file. Successful phishes can provide access to encrypted files, such as patients’ personal health information. The hackers then demand a ransom payment to restore access to the files.

Cybercriminals consider the human element to be the weakest link in a healthcare organization’s security. With just one click, clinicians and staff can unknowingly infect their entire organization’s IT systems with malware and other viruses. Cybercriminals are skilled at exploiting basic human psychology and tapping into fear, curiosity, and the desire to help. They design phishing email content to manipulate employees into clicking before verifying the link is safe.

The Human Line of Defence: How Secure is Your Clinic?

While a modern and robust IT network can be highly effective at preventing some cyber-attacks, technology is only one component of a strong cyber defence. A cybersecurity-aware “human line of defence” is critical.

Training healthcare teams on day-to-day cybersecurity and privacy awareness best practices is an effective way to bolster that defence. Saegis Shield is an accredited, comprehensive training program designed to establish and maintain ongoing cybersafe habits to thwart evolving new threats. This training helps physicians, and their teams avoid breaches and be prepared to effectively react if a breach should

---

[1] HealthCareCAN. *Key Takeaways from HealthCareCan's Summit on Cybersecurity.* http://www.healthcarecan.ca/2018/03/14/key-takeaways-from-healthcarecans-summit-on-cyber-security/

[2] Burke, D. (2020). *Hospitals “overwhelmed” by cyberattacks fuelled by black market*. CBC News. https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422

[3] Solomon, Howard. (2021). *What to do before and after being hit by hackers.* IT World Canada. https://www.itworldcanada.com/article/cyber-security-today-cyber-attack-numbers-for-december-were-bad-stiff-privacy-fines-in-europe-and-attacks-on-healthcare-sector-continue/440249

occur. Arming physicians and healthcare teams to spot and avoid malicious phishing emails could greatly diminish the incidence of cyber-attacks in Canada.