Empower Your Staff, Protect Your Patients

How can your staff be your most effective protection against cyberattacks?

While cyberthreats have been on the rise for many years, the past months have proven to be especially fruitful for hackers. Newfoundland faced a catastrophic attack this past fall, Ontario has seen multiple breaches with privacy issues and, in Saskatchewan, an employee using an infected device while it was connected to their workstation compromised an entire network.

Scammers prey on those who are weak, vulnerable, or distracted and the pandemic is a perfect storm. While healthcare teams are doing their best to keep themselves and their family healthy, cybercriminals are leveraging the concern about the pandemic to roll out attacks. Fraudulent emails have been sent posing as everyone from the World Health Organization to the Public Health Agency of Canada and have offered everything from personal protective equipment to an update on your COVID-19 test results.

On top of the pandemic, the war in Ukraine has added to concerns about cyberattacks. Cybercrime groups loyal to the Russian government have pledged to carry out digital extortion attacks against Western targets. A cyberattack on Global Affairs Canada in January 2022 is suspected of being carried out by Russian hackers. Big companies and institutions are not the only subjects of these attacks. Smaller businesses and individuals are increasingly the subjects of attacks and are proving to be easy targets. Scams include emails that use emotional appeals to provide aid or funding to those fleeing Ukraine. Senders have also posed as military personnel asking for payments in exchange for rescuing at-risk relatives.

Cybercriminals prey on human vulnerabilities – fear, curiosity, distraction, anxiety, exhaustion, burnout – and busy healthcare organizations in the middle of a pandemic are a ripe target. We are not alone in facing these threats, but the risks may be greater than they appear. Canadian health professionals simply cannot afford to wait to address cybersecurity vulnerabilities and they also do not need to.

Not an Information Technology issue

Many healthcare professionals, especially those in smaller clinics or family health teams, may assume that cybersecurity is a technical issue that demands a technical solution.

Cybersecurity expert John Riggi points out that “Cybersecurity is not an IT issue; it’s a patient safety issue.” Digital solutions for storing and sharing medical records and patient data create attractive opportunities for cyber criminals. With clinics increasingly sharing electronic medical records with labs, hospitals and pharmacies, the risk multiplies. Many clinicians have been working from home networks and computers that create additional vulnerabilities in the system.

The increased usage of electronic medical records in sometimes vulnerable contexts provides more opportunity for attacks to lock clinicians out of vital patient data or interrupt healthcare delivery altogether. In September 2020, it was reported that a patient in Germany died when University Hospital Dusseldorf was hit by a ransomware attack and network outage that prevented critical care. The nearest hospital was 20 miles away and the patient, who was in a life-threatening condition, died from treatment delays. Cybercriminals exploited this urgent need for continued operations to exact swift payment with minimal negotiation.

Any cyber incident can have devastating consequences to a clinic or healthcare institution by affecting patient safety, the ability to deliver care and patient confidence. Beyond disruptions to patient care and communication, protected health information is often sold online and held for ransom again. Not surprisingly, cyberattacks can lead to complaints and subsequent investigations by lawyers, hospitals, colleges, and privacy commissioners.

The Human Defence

While the attacks do leverage sophisticated technology, the most impactful solutions are not necessarily technical in nature. A cyberattack constitutes any deliberate attempt to breach the information system of an organization or individual but these attacks often exploit a vulnerability in people or process.

- Phishing constitutes emails that are made to seem familiar to recipients, enticing them to click on a link that can enable data theft.
- Ransomware, malicious programs that lock owners out of crucial data in exchange for a fee, is often enabled when staff click on unsafe links, use an unsafe USB stick, or click on an infected email attachment.

Healthcare professionals typically feel overwhelmed by the urgency of these threats, alongside the technical knowledge and tools they perceive are required for cybersecurity.

Experts say that the best defence against cyberattacks is empowering your staff with the knowledge they need to spot, report and safeguard against cyberattacks. In other words, your best defence is the human defence.

A staggering 93% of cyberattacks exploit unsuspecting and uninformed employees, and nearly all successful threats leverage social engineering and human interaction.

Our Role in Cybersecurity

If the human defence is the best defence, why are breaches still happening?

For many, the risk is still unknown or underestimated. This is at odds with experts like Riggi who note that attacks are inevitable. “Eventually, you will be breached. It’s not a matter of if, but when.” During the COVID-19 pandemic, we have seen healthcare become the most targeted industry with attacks increasing by 250%. Others recognize the threat but assume that attacks are only executed on organizations that are large, sophisticated, or frequented by high profile patients. Breaches in Canada have impacted a broad range of medical practices from large institutions to small family health teams. No one is immune and anyone who uses digital information and file sharing is at risk.

Some organizations deprioritize cyber training assuming the resourcing required is unfeasible, while the impact on patients is low relative to other urgent priorities. We know that outages directly affect patient care and that even core staff training can have a significant positive impact on the development of cybersafe habits and the protection of data.

Cybersecurity training has been shown to effectively enable staff to better protect data, and with attacks increasing, it is timely as well. Simple training programs for healthcare teams remove the administrative burden so staff can focus on learning and applying their knowledge. One Shield user said, “I certainly count us very fortunate that we were one of the early adopters of this new learning,

because within months we had a real-life situation where we were able to put it in practice. And that's when you realize if you don't know what you don't know that ignorance is not bliss. It really isn't."

Users of Saegis Shield, an online cybersecurity training program designed specifically for Canadian healthcare professionals, reported that after completing the cyber security awareness and privacy training course, their capacity to protect against attacks had vastly increased.

- The proportion of participants who knew how to report a cybersecurity incident increased 60%
- The proportion of participants who reported confidence in their ability to recognize a cyberattack increased 35%
- The proportion of participants who assumed an email attachment from a colleague was safe decreased 41%

At its core, cybersecurity is not about bits and bytes of data. It's about living many of the values assumed by healthcare professionals: safety, privacy, respect, and accountability. We have both the imperative and the knowledge needed to secure our patient data from cyberattacks. To continue to protect the Canadians who need us most, we must activate our human defence – our staff – now.

Take the opportunity to boost your cybersecurity today.

For more information on cybersecurity, visit https://saegis.solutions/shield