NEWS

How hospitals can protect themselves from cyber attack

■ Cite as: *CMAJ* 2020 January 27;192:E101-2. doi: 10.1503/cmaj.1095841

Posted on cmajnews.com on January 8, 2020

Hospitals and health care systems have become a major target for hackers. The announcement that LifeLabs, Canada's largest medical testing company, paid a ransom to retrieve the data of 15 million patients is just the latest in a string of cyber attacks aimed at stealing data or extracting money from health care organizations.

In September, the computer systems of three Ontario hospitals were crippled by a ransomware virus, an attack in which hackers encrypt data and demand payment to unlock it. And earlier in 2019, a similar attack hit Health Sciences North, shutting down computer systems across northern Ontario.

Hospitals are a popular target for several reasons, says Mark Gaudet, a cybersecurity expert at the Canadian Internet Registration Authority (CIRA). For one, they hold a great deal of valuable confidential data, and the move to electronic medical records has made those data more vulnerable. Hackers can get around $1 per record if they sell them in bulk, or up to $1000 for the records of specific people, he says.

Even if the hackers merely lock the data, hospitals can't afford to lose access for long and might be more willing than other organizations to pay a ransom. "We provide life and death services," says Dr. Joshua Tepper, CEO of North York General Hospital. "For that reason, we're perceived as a high-value target."

According to Gaudet, hospitals are also a relatively easy target because they have a "broad attack surface." It's hard to control physical access to equipment, he explains, and many medical devices use older operating systems that are difficult to update and easier for hackers to exploit.

But the biggest vulnerability for health care systems and hospitals is the same as for any other organization targeted by hackers, Gaudet says. "The main vector for attacks is people, through phishing or the more targeted spearphishing attacks," in which hackers gather information using deceptive emails or websites, he explains. "Ninety percent of breaches start with a person."

Health care workers seem to be more vulnerable to these kinds of attacks than others. One American study found that health care workers clicked on one out of every seven simulated phishing emails — a worryingly high rate, according to Gaudet.

That seems to be the cause of the September attack in Ontario that affected Michael Garron Hospital in Toronto. The virus spread from a single corporate laptop — likely someone clicked a link in a scam email or website, says Shelley Darling, director of communications for the hospital.

Although the attack did not lead to any patient information leaving the hospital's system, nor any payment to the hackers, the effect on hospital operations was severe. It took 10 days to restore access to most systems including electronic medical records, and even longer to restore some less critical systems, says Dr. Patrick Darragh, the hospital's chief medical information officer.

iStock.com/Farbentek

Recent ransomware attacks exposed cracks in health care cybersecurity.

In response to the attack, the hospital required all staff to take further training in cybersecurity and beefed up its firewall, says Darragh. According to Gaudet, such steps can reduce the risk of future incidents substantially. He says the training offered by CIRA, for example, which includes simulated phishing attacks, can decrease clicks on malicious links by two-thirds. “Hospitals need to create a cybersecurity culture,” says Gaudet. “They already do a good job on privacy and data management, but on cybersecurity they have a long way to go.”

Even with strong firewalls and fully trained staff, future breaches are probably inevitable. Tepper says hospitals need to have procedures in place to minimize the disruption, as they do for any other emergency, like a fire or flood. In the attack on Michael Garron Hospital, for example, email and pagers were affected, so it was difficult to disseminate information throughout the hospital quickly. Darragh says the hospital collected cellphone numbers, which are now kept on a list for future emergencies. And with electronic records unavailable, the hospital needed to ensure that all staff, particularly younger staff, were able to revert to using paper charts.

“We have to have the mindset that it’s a matter of when, not if,” says Tepper. “We need to prepare for it as we would for any other adverse event.”

Brian Owens, St. Stephen, N.B.