NS HOPA **Bulletin**

Risk Management Bulletin for HOPA Subscribers **February 2019**

Cyber Security

A recent news story highlights the dependence of health care providers on technology and the ever-present threat of cyber events to our members' abilities to carry out their operations.

Ransomware or other viruses can paralyze your operating systems, leaving you unable to provide services and generating huge expenses in order to return to normal operations.

Twenty-four hospitals in northeastern Ontario were recently hit with a "zero day" virus. Such a virus is a previously unidentified malicious software program so there are no known patches or solutions. "Zero-day" refers to the fact that IT personnel have 'zero days' to fix the problem that has just been exposed - and perhaps already exploited by hackers.

The CEO of Health Sciences North said the virus came from another hospital in the region. He estimated about 75 per cent of its computer systems were impacted. As a preventive measure, all systems were put on downtime, successfully avoiding the dissemination of the virus.

As a result, 21 of the 24 hospitals saw their main electronic medical record system, Meditech, put on downtime. The electronic medical record system for cancer programs in 12 hospitals was on downtime. Ten hospitals had their medical imaging system on downtime. Four hospitals had their email and servers for back office impacted.

The CEO said putting the systems on downtime slows down the efficiency of the hospital. For example, patients can usually get tests done and the results are readily available in the system. "That automation is no longer available," he said. "The information needs literally to be walked across the hospital or across various sites."

Staff were taken back to working with pen and paper as they were unable to access electronic records. Appointments were cancelled and other services were backlogged.

Once systems were operational again, appointments in cancer care were scheduled on Saturday and Sunday in order to clear the backlog. Other staff worked the weekend to enter data and reduce the backlog of information in the system.

The CEO said there was no request for ransom.

Information was restored from backups and the hospitals were back to full operations in approximately one week.

While the event at Health Sciences North does not appear to be the result of ransomware, the effects were similar.

Ransomware

Ransomware targets all of an entity's operating systems. The goal is not to steal sensitive information, but to paralyze operations until ransom is paid.

In March of 2016, the website of Norfolk General Hospital in Simcoe, ON was hacked and ransomware installed on the website. The website was pushing ransomware to computers that visited the website. Computers were restored from backups and no ransom paid.

Also in March of 2016, four computers at Ottawa Hospital were hit with ransomware. The ransomware encrypted information on the computers making it inaccessible. A spokesperson indicated "no patient information was obtained through the attempt." The hospital responded by wiping its drives and no ransom was paid.

The WannaCry malware attack in the spring of 2017 impacted hospitals, businesses and government offices in nearly 100 countries, including Canada.

Ontario's Privacy Commissioner reported that in 2016 and the first half of 2017, it had received 10 reports of ransomware attacks on clinics and doctor's offices. The Commissioner deemed ransomware an "increasingly dangerous" threat to the security of health records in the province. Another expert estimates that the total number of ransomware attacks has increased by 600% in the last year alone. Medical information, much more than other sensitive data such as banking information, is 10 times more likely to be targeted.

In 2018, CarePartners, a home care service provider to Ontario's Local Health Integration Networks (LHINs) and an Ontario-based community healthcare agency, disclosed that it "has become the victim of a cyber-attack by sophisticated actors." The cyber-attack breached CarePartners' computer system and as a result patient and employee information held in that system, including personal health and financial information, had been inappropriately accessed by the perpetrators. In response, CarePartners retained a leading cyber security firm to contain and determine the extent of the breach. In addition, LHINs and CarePartners voluntarily suspended the online referral system's capacity to receive patient assignments until the breach was fully contained and vulnerabilities fully closed. Patient care had not been compromised, the organization said. CarePartners said it will provide ongoing credit monitoring for any individual whose personal data may have been breached.

HOPA recently attended a webinar detailing how an unnamed American hospital was impacted by malware in 2017 that left all of its electronic information inaccessible. The study sets out the steps the hospital went through to restore its operations, including establishing manual work-arounds to provide direct patient care. The service provider of the hospital's hosted electronic health records system refused to allow the hospital to access the system until an independent forensic consultant declared the hospital's network "clean". It ultimately proved cheaper to replace all electronic devices rather than wipe and rebuild the corrupted ones. The total cost of the attack, from the additional labour costs for clinical staff to the cost of replacing all devices to the loss of profit due to patient diversion, was over $ 9 million (CDN.) It was approximately 3 months before operations returned to normal.

Cyber Insurance

It is important to understand that the costs incurred to restore operations after a virus or ransomware attack are not covered by a property insurance policy or a traditional liability policy, including the HOPA policy.

A property insurance policy does not cover these costs because they don't arise from damage to physical property.

A traditional liability policy does not respond, because such a policy responds to losses and costs incurred by third parties, that is, someone other than the Insured.

A Cyber insurance policy includes a number of coverages that responding both to claims from third parties and to the first party expenses incurred by the Insured.

Third party coverages include:

> Privacy Liability - claims for loss of or inappropriate access to personal health information and other sensitive information;
> Security Liability - claims for failure of network security which impacts other parties, such as third party service providers impacted by a virus that originates in your operating systems.

Costs associated with these events, covered by the insurer, include privacy breach notification, investigation costs and public relations costs. Cyber insurers may provide a Cyber Coach, or event management support, to walk the insured through all of the steps of responding to a cyber event.

Cyber insurance may respond to regulatory action by the Privacy Commissioner.

In addition, cyber insurance covers a number of first party costs. Coverage include the cost of forensic investigations, public relations costs, costs to restore electronic data, and loss of income or extra expense (business interruption) due to system shutdown. Cyber insurance may respond to cyber extortion, including negotiating and paying ransom.

HOPA would be pleased to answer any questions you may have in order to assess suitable cyber insurance products to address your needs.

This Bulletin should be understood to be general risk management information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

If you have questions, or would like additional information please contact:
Connie Morrissey, HOPA Claims Counsel
t. 902.832.8542 e. connie.morrissey@nshopa.ca

To obtain print versions of this bulletin please contact: hopa.admin@nshopa.ca