HR HealthCheck

Ransomware Attack on Three Ontario Hospitals Highlights a Growing Cybersecurity Risk

Date: October 10, 2019

Three Ontario hospitals were recently targeted in ransomware attacks that highlight the emerging risk of cyberattacks on public institutions and healthcare providers. The CBC first reported these attacks, which are the latest in a growing list of public institutions whose computer systems are infiltrated by hackers. Are you prepared?

What is a Ransomware Attack?

Ransomware is a form of malicious software that infects a network and encrypts systems and files. The encryption is usually accompanied by a message demanding payment in exchange for restoring access to the encrypted data. Payment is generally demanded in bitcoin (a decentralized digital currency).

Most ransomware attacks are launched either through direct hacking into a vulnerable system or through phishing emails that urge employees to click on files or links that then install malware that encrypts systems and files.

Recent Examples

Public institutions across Ontario and North America have been held hostage by ransomware attacks. Hospitals and healthcare providers are facing serious challenges in the wake of these attacks. The three infected hospitals in Ontario suffered service disruptions as email systems were taken offline, healthcare records became harder to access and patients were warned of longer wait times. In the same week that Ontario hospitals announced details of their ransomware attacks, three Alabama hospitals had to turn away patients after suffering a similar infection that shut down computer systems and blocked access to patient lists.

Are You Ready in the Event of an Attack?

Data security programs must treat the ransomware risk as a priority. Elements of a defendable data security program include enforcing least privilege access to data, two-factor authentication, access controls, and an ongoing information security awareness program that promotes strong phishing awareness. Of particular importance to the ransomware threat is a robust offline data/system

backup capability.

We recommend that hospitals and healthcare providers review their preparedness for responding to a cybersecurity incident such as a ransomware attack. A prepared organization has:

- an incident response protocol that provides for timely and decisive decision-making;
- assessed its cybersecurity insurance needs and purchased appropriate levels of insurance coverage; and
- pre-retained an incident response coach (and possibly other service providers) who can provide immediate assistance in the event of an incident.

Put Hicks Morley's Experience to Work For You

Hicks Morley acts as regular information and privacy counsel to many public sector organizations and understands the unique demands that they face. We also have over a decade of experience with data security incident response, are the Ontario School Boards Insurance Exchange preferred incident response law firm and have helped with numerous ransomware incidents in the past two years.

Get in Touch

If you would like to discuss cybersecurity preparedness or need help with a ransomware or other data security incident, please contact Jordan Simon at 416.864.7528.