HEALTH
ASSOCIATION
NOVA SCOTIA
EXPERTISE. SERVICES. SUPPORT.

HANS EDUCATIONAL WEBINARS

CYBER SECURITY

Cyber security incidents in the healthcare environment can have serious and devastating consequences. They have an impact on many areas: service interruptions, operational losses, patient safety issues, reputational losses, privacy breaches, potential civil actions or class action lawsuits, regulatory investigations/fines and financial losses.

Health care is one of the most critical functions in our society yet, when it comes to our security infra structure around technology and information protection, we lag far behind many other key industries such as financial services, oil and gas and transportation.

We are increasingly living in a digital age of healthcare. Recognizing the vital role critical IT systems now play in patient care, we are slowly evolving from a focus on simply protecting patient data to the broader goal of protecting the ability to care for patients and residents.

Unfortunately, even security infrastructure built with state-of-the-art technology is not enough to protect an organization in the current environment. Cyber security is much more than an IT function. Organizations increasingly recognize the need to treat cyber security as a core component of their broader organizational strategy.

A trick played on a single employee can pose a greater threat to a healthcare organization than a team of skillful hackers. There are many factors that go into managing cyber threats and the most important one is resilience. Resilience can be achieved through building organization-wide cyber intelligence, expertise, partnerships and a culture of security along with appropriate information technology solutions.

CYBER SECURITY

HEALTH ASSOCIATION NOVA SCOTIA
EXPERTISE. SERVICES. SUPPORT.

OBJECTIVES:

This webinar will examine the key elements that should be part of an effective and successful cyber security program. The following areas will be covered:

- The “human firewall”. Building resilience in the workplace and creating a security aware culture. Providing your staff with the tools to identify and manage risks. Measuring workforce resilience.
- Providing a policy direction and structure to your system. Building and managing an acceptable use and data security policy appropriate to your organization. Creating an accountability and governance structure for the management of risk.
- Creating and testing a privacy breach response plan and maintaining a privacy breach registry.
- Know and measure your risks. Identify your vulnerabilities and determine what your “crown jewels” are. Create an inventory of your critical technology and the sensitive data in need of protection. Classify the risk levels and ensure appropriate safeguards are in place.
- Identify and review risk levels associated with third party relationships. This involves system networks being utilized as well as ordinary external service providers.
- The role of cyber insurance in managing risk. Evolving trends and some key components of a reliable insurance policy.
- Ensuring regulatory compliance. The role of legislation such as PIPEDA and the provincial Personal Health Information Act. Knowing the key requirements and the enforcement structures.
- Responsibilities of the Board of Directors in providing oversight on this important area of risk management.

PRESENTED BY: Robert Dunn, LLB, CIPP-C
Barrister and Solicitor

DUNN LAW
Privacy & Information Security Solutions

DATE: February 8, 2022

PLEASE NOTE: The session will be recorded and made available for a period of three months for those who are unable to attend.

TIME: 10am - 11am

COST: The webinar will be offered free of charge as a value add of membership

RSVP TO: alex.cross@healthassociation.ns.ca

Zoom Link to Follow