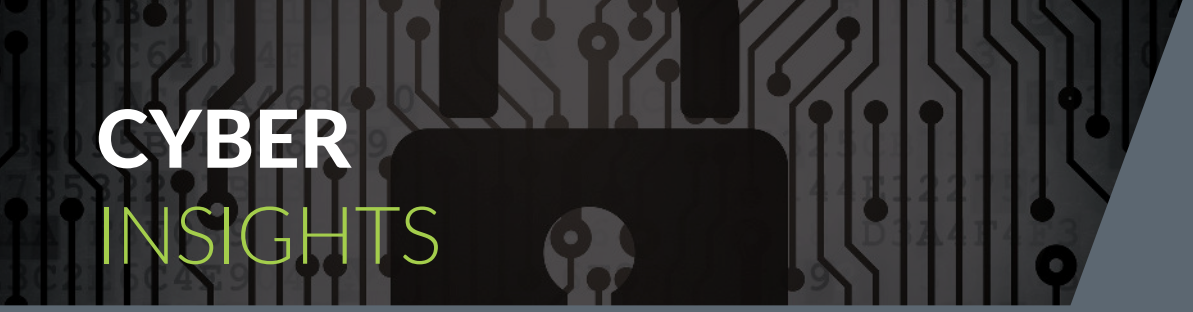

CYBER
INSIGHTS

HK HENDERSON

NAVACORD®

Cybersecurity Best Practices for Canadian Organizations

Safeguarding against cyber risks is crucial in today's digital landscape. As cyber threats continue to evolve in sophistication, taking proactive measures have become more crucial than ever before.

To enhance cybersecurity protection against malicious attacks like malware, ransomware, and phishing, companies can take the following six steps:

1. IMPLEMENT NETWORK SEGMENTATION

Network segmentation involves dividing a larger network into smaller sub-networks with restricted access privileges. This limits the potential spread of a cyber attack and prevents threat actors from gaining lateral movement across the entire school network if they breach one segment. Companies should segment their networks based on user groups and departments to reduce the attack surface.

2. PROVIDE CYBERSECURITY AWARENESS TRAINING

Educating all staff on cybersecurity best practices is crucial for preventing human-related cyber incidents like phishing attacks or accidental data exposure. Companies should introduce cybersecurity awareness training early, covering topics like password hygiene, multi-factor authentication, and identifying phishing attempts. Regular training and simulations can help reinforce these lessons. In addition, companies can run simulated phishing attempts aimed at staff. If a staff member falls for such a fake attempt, it serves as a clear signal that additional education and training are necessary. Some cybersecurity training companies provide this service to their clients.

3. KEEP SOFTWARE AND SYSTEMS UPDATED

Outdated software and systems with unpatched vulnerabilities provide an easy entry point for cyber criminals. Companies should implement processes for regularly updating all software, operating systems, and firmware to the latest versions. Enabling automatic updates where possible can simplify this process.

4. IMPLEMENT ACCESS CONTROLS AND AUTHENTICATION

Implementing strong access controls and authentication measures can prevent unauthorized access to networks and data. This includes enforcing complex passwords or passphrases, enabling multi-factor authentication (MFA) for all user accounts, and restricting remote access to internal systems through a virtual private network (VPN) protected by MFA. This adds an extra layer of security by requiring additional verification beyond passwords.

5. DEPLOY CYBERSECURITY TOOLS

Companies should deploy a range of cybersecurity tools to protect their networks and devices, such as firewalls, antivirus/anti-malware software, intrusion detection and prevention systems, and email filtering solutions. These tools can help detect and block various cyber threats before they cause harm. Another avenue to explore is endpoint detection and response (EDR) tools. In some cases, sophisticated cyber criminals have been able to bypass antivirus and firewalls but EDR technology continuously monitors endpoints for evident of threats and performs automatic actions to help mitigate them.

6. DEVELOP AN INCIDENT RESPONSE PLAN

Having a well-defined incident response plan can help schools respond effectively to cyber incidents and minimize their impact. The plan should outline roles and responsibilities, communication protocols, and steps for containment, eradication, and recovery. Regular tabletop exercises can help test and refine the plan.

CONCLUSION

Cyber insurance serves as a crucial safeguard for organizations, shielding them from the potentially devastating financial and operational consequences of cyberattacks. Not only does it offer a way to transfer a portion of the risk, it will also provide access to expert services like forensic investigations and public relations support in the event of a claim. Some insurance carriers go a step further by offering pro-active support for their clients, notifying them of potential vulnerabilities before an incident as opposed to only getting involved after an event has occurred.

By implementing these measures, Canadian organizations can significantly reduce their cyber risk exposure and create a safer online environment for staff and clients. Collaboration between Canadian companies, government agencies, and cybersecurity experts is also crucial for sharing best practices and staying ahead of evolving cyber threats.

If you have questions specific to your business, or would like additional information, please reach out to your HK Henderson Advisor.

LET US HELP YOU MANAGE YOUR RISK

Saskatoon
Regina
Moose Jaw

hkhenderson.ca
info@hkhenderson.ca
1.888.661.5959