

March 25, 2019

The Biggest Cyber Risks of 2019

Cyber breaches and attacks are becoming part of our everyday work lives. And the pace of technological change, and the ability of criminal elements to take advantage of these advancements, is incredibly fast. The days of leaving cyber security to the IT department and forgetting about it are passing as well. Cyber risks can cause reputational, financial, organizational, legal, and operational issues throughout your organization.

The public's confidence in your organization can be compromised in an instant and, once lost, can take years to re-earn or lead to a demand for a change in leadership that can address these issues.

To help simplify the risks that your organization is most exposed to at the current moment, here is a list of four topics all leaders need to ensure are being protected against.

1. **Data breaches with third party vendors** – Many times you allow consultants and outside vendors to access your privately held information. An example would be hiring a consultant to review your organization's benefits program. The consultant is given access to all your employee's data. To properly protect your organization, you need to ensure that the consultant has adequate cyber security procedures and policies and carries Cyber Event and Privacy Breach Liability, in addition to the normal insurance requirements. Many smaller firms have not identified the need for Cyber Event and Privacy Breach Liability, but all outside consultants and vendors should be required to carry it. If a third party loses your information, your own insurance program may not respond to the loss and your organization will then have to cover the significant related costs.
2. **Social Media and Mobile Apps** – More and more organizations are using social media to connect with the public. Instagram, Facebook, and Twitter seem like great gateways to the public, but they can also open your organization up to sharing information they should not release publicly. Be careful what you post or allow employees to post. In addition, follow the news to ensure that the apps you are using for your organization have not been breached or any issues have arisen.
3. **Phishing Attacks Continue to be a Threat** – Phishing attacks rely on unsuspecting users to click on malicious links, usually sent by email, that allow criminal access to your IT infrastructure. Continuous training of staff to recognize the attacks and not click on the link is vitally important. If an attack does occur, it will then be too late to think about prevention training. It needs to be continuous and provide up-to-date information, so your operations are not compromised.

2510 Sparrow Drive
Nisku, Alberta T9E 8N5

OFFICE: 780.955.3639
FAX: 780.955.3615
RMAAlberta.com

4. Personal Devices are a Ticking Time Bomb – Home computers and mobile devices have long been preferred targets for hackers. In the bid to be ever more mobile, we allow many employees to access private information on the go through phones, tablets, laptops, and home desktops. Staff can keep their devices safe by powering them down when not in use, making sure they have robust passwords, and making sure up-to-date security programming has been installed on all devices. In addition, your organization can look at installing cyber security software that can monitor usage in real time and report any threats.

As everything we do depends on technology these days, a cyber attack can disrupt any or all of your operations. Your organization needs to be aware of these threats and provide protection accordingly. At RMA Insurance, we value our members' patronage and want to work together to ensure risks are minimized in this area.

To get more information please contact our risk management team.

For enquiries, please contact:

Dayna Johnson
Client Relations Manager
780-955-8408
dayna@RMAinsurance.com

John Hackwell
Risk Advisor
780-955-4078
johnh@RMAinsurance.com

Darcy Hale
Risk Advisor
780-955-8406
darcy@RMAinsurance.com



2510 Sparrow Drive
Nisku, Alberta T9E 8N5

OFFICE: 780.955.3639
FAX: 780.955.3615
RMAAlberta.com