CYBERCRIME

How to protect small business

Developing a cyber response plan is critical for SMEs

BY NEAL JARDINE, *Senior General Adjuster, Cyber Practice Leader, Crawford & Company (Canada) Inc.*

The threat of cybercrime continues to grow, affecting organizations across all industries and of all sizes.

Ransomware attacks have increased 250% since 2016, according to an online article on Media Planet. Although large organizations receive the most attention, small and medium-sized enterprises (SMEs) account for over 70% of data breaches. Cyber security incidents can be costly to an organization, potentially damaging customer and stakeholder's confi ence, and trust.

Why are cybercriminals attracted to SMEs?

Due to their size, SMEs may lack the appropriate resources to handle an attack, according to an online article on *business.com*. In a Canadian Chamber of Commerce survey of approximately 260 businesses, only 26% of micro-businesses and only 55% of small businesses made investments in cybertraining.

The information cybercriminals target – credit card information, intellectual property, and personal identifi ble information (PII) – is often less guarded on an SME's system. Visa Inc. reports that 95% of credit card breaches are from SMEs.

Since larger organizations are likely to have more robust defense systems to deter cyberattacks, cybercriminals are more likely to target connected SMEs to gain access. Partnerships between SMEs and larger organizations can provide a back-channel for hackers, as was the case with Target in 2013, whereby access was gained through their HVAC vendor, an SME, according to *cnbc.com*.

SMEs can protect themselves by establishing a cyber incident response plan that incorporates a network of specialized experts to address all loss exposures in a concise fashion. The goal is to mitigate exposures in a timely manner and prevent future incidents.

While developing the plan, SMEs should address their scope, size of operations, involved parties, and simulate an attack in advance. A cyber incident response plan should include:

- defining the scope, detection and assessment
- federal and provincial regulations
- response team and incident manager
- methodology and i vestigation
- remediation and recovery

Scope, Detection and Assessment

A defined scope identifies which of the two cyber losses the SME might face: a *cyber incident* or a *data breach*. A cyber incident can be a malicious act or suspicious event that may or may not have compromised the electronic security perimeter or physical security perimeter of a critical cyber asset. A data breach is the loss of, unauthorized access to, or disclosure of personal information, resulting from the breach of an organization's security safeguards, says the Offic of the Privacy Commission of Canada.

Federal and Provincial Regulations

This distinction is critical due to the legislation that came into effect Nov. 1, 2018 under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Federal Privacy Commission must

now be notified if personal identifi ble information (PII) was accessed, viewed, or stolen, poses "a real risk of significa t harm" to the individuals whose data was involved. Each scenario requires its own risk mitigation strategy.

Incident managers need to be aware of the type of information the SME keeps and how it is stored. A data breach has a greater exposure due to the risk to PII, along with the responsibility to notify the privacy commissioner and possibly draft notices to the individuals whose data was accessed. An incident manager may choose to initiate a forensic investigation and maintain legal "privilege" if an investigation has not already commenced. The incident manager can involve a lawyer to assist with this portion and guide the business through the regulatory environment, thus avoiding costly fines

For SMEs that do not store PII, such as a small machine shops, variety stores, or restaurants, a cyber incident leading to a ransomware attack or other cyber event may not have the same risk or exposures. Incident managers can guide SMEs through the process and manage the loss.

Response Team and Incident Manager

An organization's plan should include a list of fir t responders and outline the composition of the incident response team. Most SMEs may not have a system administrator, risk manager or human resources department. A contact list should include the proposed incident manager and those responsible for maintaining the business' computer systems.

Methodology and Investigation

An organization's cyber incident plan should outline the methodology and investigation strategies to be used when an event happens. Consideration should be given to how to take certain systems offline thout impacting the entire business.

Remediation and Recovery

Finally, organizations need to keep track of the remediation and recovery efforts. According to research conducted by Kroll Ontrack, "while over half (57%) of respondents had a backup solution in place, three quarters (75%) were not able to restore all of their lost data, with more than one-in-five (23%) unable to recover any data at all." Organizations should outline where all data backups are located and frequently test the back-up process in their plans. cu

Neal Jardine is a senior general adjuster with Crawford's Global Technical Services (GTS), with more than 10 years of experience in adjusting property and casualty claims. He has a degree in computer science and worked in the IT field prior to joining Cr wford.