

# Cyber Security Risk Assessment Services

Crowe MacKay's Technology Consultants are dedicated to protecting your assets. Our team is committed to providing you the support and resources required to make informed software selections and execute seamless implementation. Let our trusted advisors reduce your business' vulnerabilities to malicious cyber attacks, giving you the confidence that your operations are safeguarded from exploitation.

## Why is a cyber security risk assessment needed?

When data breaches or cyber-attacks (virus, malware, ransomware) occur the impact has been documented as disproportionate compared to a company's income. They can result in a business having to stop operations for days or weeks, pay ransoms, and engage IT security remediation companies at a premium price ranging between \$50,000 to \$1 million.

Executing a Cyber Security Risk Assessment is the first step toward strengthening a client's defense and resilience to cyber security risks.

## Main types of cyber related attacks

### Ransomware

A cyber criminal encrypts your files and demands a ransom in order for you to gain access to them again.

### Operational Disruption

A cyber criminal takes action to disrupt your operations and requests payment to stop the attack, (i.e. denial of service).

### Data Breaches

A cyber criminal uses different techniques to steal information from your company, (i.e. personal identifiable information, intellectual property).

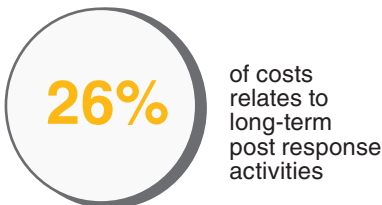
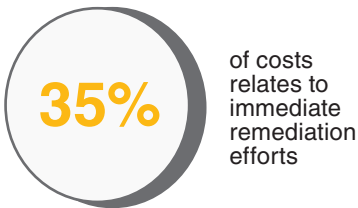
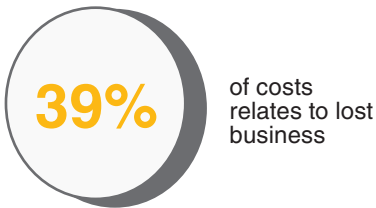
### Financial Fraud

A cyber criminal uses different steps to siphon funds from your company, (i.e. CEO fraud, credentials theft).



**\$6.3M**

is the average cost of reported data breaches in Canada



**Who should conduct a cyber security assessment?**

It's common for small to medium sized businesses to not have an IT resident staff with the necessary levels of qualification and experience to define and implement proper cyber security policies and procedures. They may rely on a Management Service Provider for part of their IT needs but this will not cover their whole digital footprint. If you are a business who does not have your own technology department, you can benefit from Crowe MacKay's cyber security risk assessment services.

**What does a cyber security risk assessment include?**

Analyze your digital footprint

Our technology consultants will first meet with you, and any of your IT suppliers, to discuss your current cyber security processes and procedures in order to analyze your overall digital footprint. This also includes a review of current implemented cyber security training policies, and system configurations.

Operational environmental scan

We assess your digital footprint information against our repository of nearly 70 cyber security risk elements and prepare a report with risk ratings and priorities. Client reports will vary in breadth, but include:

- Threat vectors analysis
- Cyber security risks related to operations
- Recommendations

Remediation

Following the provision of the report, our experts are available to execute the remediations. Common services include:

- Solution recommendations
- Training
- Cyber security strategy initiation and implementation
- Incident recovery procedures initiation and testing

**Contact Crowe MacKay's Technology Consulting Team**

Severin Pietri, Director  
(604) 697 9255  
severin.pietri@crowemackay.ca

Srinivas Rao, Director  
(604) 697 5206  
srinivas.rao@crowemackay.ca