CYBER CRIME:
HOW CAN IT AFFECT YOUR BUSINESS?

IRIDIUM RISK SERVICES EVOLVED

NAVACORD®

$5 Billion

Per year is the average cost of cybercrime to the Canadian economy

Source: CBC News

How much can Cyber exposures cost your business?

$200K

Average financial impact cost per Canadian small business

Source: Based on Canadian Underwriter Stat

600%

Increase in phishing attempts from Cyber criminals due to Working from Home amidst the Covid-19 Pandemic

Source: Infosecurity Magazine (2020)

67%

Increase in cyber attacks and a 72% increase in the annual cost of cyber crime over the last 5 years

Source: Accenture, Cost of Cyber Crime (2019)

53%

More than half of organizations that were victim of a ransomware attack opted to pay the ransom

Source: Blakes Cybersecurity Trend (2020)

31 out of 40

Oil and Gas companies that experienced a cyber breach found that employee error was the source of the incident

Source: Ernest & Young (EY) (2019)

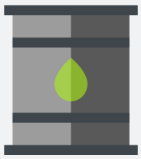
47%

Almost half of all cyber incidents took more than two weeks to recover and 23% took more than four weeks

Source: Blakes Cybersecurity Trend (2020)

45%

Of pipeline companies reported a cyberattack in 2017



Source: StatsCan (2017)

40%

Of businesses have experienced a ransomware attack in the last year

Source: Insurance Information Institute (2019)

206 days

Was the average time to identify a breach in 2019

Source: IBM (2019)

$3.92M

Was the average cost of a data breach in 2019

Source: Security Intelligence

Local Touch. National Strength.™

irsnavacord.com
403.263.9654

IRIDIUM RISK SERVICES EVOLVED | NAVACORD®

CYBER CRIME:
HOW CAN IT AFFECT YOUR BUSINESS?

IRIDIUM RISK SERVICES EVOLVED

NAVACORD®

A cyber insurance policy can help you deal with a cyber attack

Cyber insurance covers the costs for your business to discover **what happened**, **why it happened**, and most importantly, **what to do next:**

- A cyber policy provides you immediate access to expert resources, including breach coaching and cyber forensics firms to handle all cyber threats before, during, and after they've happened.
- Reimbursement for legal and public relations professionals to manage media and public statements if or when valuable information has been exposed.
- Restoration of encrypted data and reimbursement for ransom payments if necessary.
- Reimbursement for notifications costs and credit monitoring services for customers and employees exposed in a breach.
- Regulatory fines or penalties that might arise from a breach involving confidential data.
- Business interruption and extra expense coverage arising from a security failure at an outsourced service provider.
- Third party lawsuits and defense costs that arise from a breach.

Cyber threat to Energy Companies

What is Exposed?

- Sensitive design details
- Project specific information
- Client/owner/employee personal information
- Company finances/funds

Who is Affected?

- Owner
- Contractor
- Sub-Contractors
- Employees
- Third parties
- Suppliers

How does it happen?

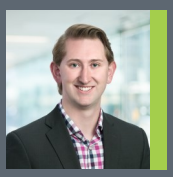
- Hacks into company's system
- Lost or stolen phone, tablet or computer
- Deceptive email misleading employees (phishing)

Potential Results

- Loss of critical or sensitive infrastructure
- Business interruption
- Loss of future business
- Privacy breach obligations

Your Team of Cyber Experts

Danielle Gorst
National Practice Leader, Financial Lines
D: 403.705.6550
E: dgorst@irsnavacord.com



Wesley Robinson
Risk Advisor
D: 403.705.1944
E: wrobinson@irsnavacord.com

Jessie Gwynne
Risk Consultant
D: 403.705.6533
E: jgwynne@irsnavacord.com

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