CYBER CRIME:
HOW CAN IT AFFECT YOUR BUSINESS?

IRIDIUM RISK SERVICES EVOLVED

NAVACORD®

US$10.5Tn

Projected cost of cybercrime by 2025, making cybercrime more lucrative than the global trade of all major illegal drugs combined.

Source: Cybercrime Magazine (2022)

How much can cyber exposures cost your business?

US$4.6MM

Average total cost of ransomware breach in 2021.

Source: IBM (2021)

600%

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

Source: Infosecurity Magazine (2020)

62%

Between 2019 and 2020, ransomware attacks rose by 62% worldwide and by 158% in North America alone.

Source: PBS NewsHour (2021)

46%

Of corporate respondents claimed that their organization faced between one and five cyber attacks in 2020.

Source: Parachute (2020)

95%

Of cybersecurity breaches are due to human error.

Source: Digital Information World (2019)

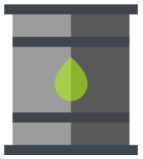
287 days

Was the average time to identify and contain a breach in 2021.

Source: UpGuard (2021)

50%

In 2021, more than half the ransomware attacks in Canada targeted critical infrastructure providers, including the oil and gas industry.



Source: National Post (2021)

39%

The Sophos State of Ransomware Report found that 39% of Canadian businesses suffered a ransomware hit in 2020.

Source: Sophos, Cybersecurity Involved (2021)

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)

56%

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

Source: Security Intelligence (2021)

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 happen.
- 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.
- Reimbursement:
    - Reimbursement for legal and public relations professionals to manage media and public statements if or when valuable information is exposed.
    - Reimbursement for notifications costs and credit monitoring services for customers and employees exposed in a breach.
    - Restoration of encrypted data and reimbursement for ransom payments if necessary.

Cyber threats to Energy companies

What is exposed?

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

Who is affected?

- Owners
- Employees
- Contractors
- Sub-contractors
- Third parties
- Suppliers

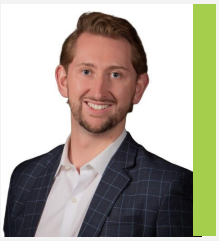
How does it happen?

- 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

EXPERT SPOTLIGHT



Wesley Robinson ***B.Comm***

Risk Advisor

D: 403.705.1944

E: wrobinson@irsnavacord.com

Wesley graduated from the University of Calgary's Haskayne School of Business with a Bachelor of Commerce in Risk Management and Insurance in December 2017. Wesley has devoted himself to understanding Cybercrime and the risks posed to corporations by these continually evolving exposures. With multiple years of experience handling the unique risks that the blockchain industry faces, Wesley has assisted Iridium in differentiating itself as industry leaders in the space.