IMCanadaConnect is Brought to you by the **ARMA Chapters of Canada** and sponsored by **WesternIM**

RIM LINING UP WITH IT, RISK, AND SECURITY: A NEW WORLD OF IG

WELCOME

RICK STIRLING

PRESIDENT

WesternIM

Rick.Stirling@WesternIM.com

NICHOLAS FONSECA

INFORMATION MANAGEMENT BUSINESS LEAD / PRIVACY MANAGEMENT LEAD

City of Leduc

NicholasFonseca@hotmail.com

IMCanadaConnect

ARMA INTERNATIONAL AND INFORMATION GOVERNANCE

IMCanadaConnect

CYBER RISK DEFINED AND WHAT IS IT?

- Any risk of financial loss, disruption of business, or damage to an organization's reputation due to the failure of its information technology systems. (Insurance Institute of Canada, 2020)
- Unintentional or accidental security breaches such as losing a memory stick or a laptop or falling victim to social engineering attacks.
- Deliberate and unauthorized breaches of security to access information systems for the purpose of destruction, espionage, extortion, or embarrassment of an organization, such as ransomware to lock businesses from accessing their data.
- Operational IT risks – Failing to install firewalls, failure to keep security software and software up to date, lack of proper security.

CYBERCRIME

- Cybercrime is a criminal offense committed through a computer or the internet that causes loss or damage to the victim's computer system, network, or data, denies access to data or service, or enables further related crimes such as extortion or the resale of stolen data. (Insurance Institute of Canada, 2020)

The Criminal Code of Canada has been amended to include the following as cybercriminal activity.

- Using a computer without authorization.
- Making mischief in relation to data.
- Possessing a device to obtain telecommunication facility or service without authorization.
- Stealing telecommunication service.

CYBER EVENT EXPENSES (RESULTING FROM EXPOSURES)

- Privacy breach resulting in personal identity theft (3rd party)
- Internet media liability (3rd party)
- Network security liability (3rd party)
- Technology errors and omissions liability (3rd party)

- Event – expenses (1st party)
- Extortion expenses (1st party)
- Restoration expenses (1st party)
- Regulatory expenses (1st party)
- Business interruption (1st party)

SOME CYBER INCIDENTS

- Colonial Pipeline
- Marriott
- The Running Room
- Equifax
- City of Atlanta
- Maersk
- LCBO
- Indigo
- Empire, Sobeys, IGA
- Bell
- Government of Nova Scotia
- Suncor
- Government of Canada
- And the list goes on……. Cyber attacks in Canada | KonBriefing.com

RISK MANAGEMENT AND ENTERPRISE RISK MANAGEMENT

- Risk management (RM) – Analyzing a risk to quantify the potential for losses in a specific investment and to decide what is the appropriate action to take (or whether to take the risk). (Insurance Institute of Canada, 2020)
- Enterprise risk management (ERM) – An approach to managing all of an organization's key business and opportunities with the intent of maximizing shareholder value. ERM is about avoiding (preventing), reducing, and eliminating risks through the creation of risk management strategies. (Insurance Institute of Canada, 2020)
- ERM doesn't always include cyber risk. It may be seen as an IT responsibility.

RISK MANAGEMENT AND ERM - CONTINUED

- Risk management can include **risk transfer**.
- Insurance is one way of risk transfer.
- **Avoidance** is an option. It's a risk management technique whereby the risk of a loss – in this case due to a cyberattack – is prevented by not engaging in the activity that presented the risk.

- Avoidance could likely mean missed economic opportunities.
- Insurers want their policyholders to exercise good cyber risk management generally, not just through risk transfer.
- Have a tested disaster recovery plan and business continuity plan, and an excellent cyber security plan.

CYBER INSURANCE RISK IS INSURABLE – OR IS IT?

- Insurance companies have relied on actuarial data to price policies or risk exposure.
- Rating has been based on location of the exposure (risk - the subject of insurance).
- Policies were standardized to some degree (not so for cyber risk and insurance).
- Cyber exposure is not subject to geographical boundaries.

- Cyberattacks can be targeted to specific verticals.
- Attacks can come from anywhere in the world.
- Cyber attackers have their own software available as a service, such as MaaS, Raas.
- Cyber attackers may use server space on hidden servers to launch their attacks.
- By 2025, it is estimated that cybercrime will cost 10.5 trillion annually. (Cyber Ventures, 2023)

CYBER INSURERS WANT TO KNOW …

- There is a cyber disaster recovery plan
- There is a business continuity plan in place
- That the plans are **relevant** and **tested**
- Adequate controls are in place, such as anti-virus software and firewalls; that patches are up to date; that unused software has been removed
- There is compliance with standards
- There is compliance with privacy and other applicable legislation
- Vulnerability and penetration testing has been completed

CYBER COVERAGES CAN INCLUDE …

- Data breach and data compromise
- Restoration of data or recovery of data
- Extortion / ransomware attack
- Business interruption and extra expense

- Misdirected payment fraud (e.g., MacEwan University)
- Network security, Data compromise and Electronic Media liability
- Others . . .
- **Coverage is not standardized.**

BECAUS
E IT'S
NOT A
MATTER
OF *IF* BUT
WHEN

CYBER INSURANCE COVERAGE CAN PROVIDE

- Coverage for internet of things exposures.
- Pre-breach offerings, such as security education, security analysis, cyber security monitoring, penetration testing.
- After a cyber event has been detected, professional services, including legal counsel, forensics, breach coaches, public relations and communications professionals, and other specialized services to deal with the cyber event.

CYBER INSURANCE QUESTIONS

- Have you ever been asked to assist with Cyber insurance coverage questions for your organization?
- Do you know what information you have across your organization? Has it been inventoried?
- Do security teams care about paper records?
- Have you ever taken a security person to lunch?
- Have you ever thought about asking your RISK folks if you can help with IM RISK?

If you don't know what you have, you can't manage it.

CYBER INSURANCE QUESTIONS

IT INFRASTRUCTURE AND RESOURCING

Databases for PII/PHI/PCI? YES NO

End of life/unsupported software and the rest of network? YES NO

Is any part of our IT infrastructure outsourced to third-party technology providers, including application service providers? YES NO

If you answered 'yes' to the question above, list your critical third-party technology providers below (up to a maximum of 10), plus a brief summary of the technology services they provide you.

CYBER INSURANCE QUESTIONS

DATA STORAGE AND MANAGEMENT

Please provide the approximate number of unique individuals that you collect, store, and/or process personally identifiable information from whether on your own systems or with third parties:

Data type number (or approximate) of unique individuals

Sensitive data (e.g., medical records, passport details, social security numbers)

Non-sensitive data (e.g., full names, addresses, email addresses, etc.)

Do you collect, process, store, transmit, or have access to any payment card information (PCI)? YES NO

If 'yes,' what is the estimated annual volume of payment card transactions (credit cards, debit cards, etc.)?

Please describe your approach towards protecting sensitive and confidential information (e.g., access controls, encryption, network segmentation, etc.).

Do you implement encryption on laptop computers, desktop computers, and other portable media devices? YES NO

CYBER INSURANCE QUESTIONS

RETENTION

Please provide details of how often you purge records that are no longer required

Do you have a data retention and disposition plan?

CYBER INSURANCE QUESTIONS

BACKUPS

Please provide details on how you store your back-ups of critical data (e.g., online back-ups stored on your organization's live environment, offline back-ups stored on a removable storage device that is fully disconnected and inaccessible from the live environment, back-ups stored with an online cloud storage provider, etc.).

Please provide details on the frequency of your back-ups, including the frequency of full system back-ups and the frequency of incremental/differential back-ups of critical data.

Please provide details on how you secure your back-ups (e.g., back-ups are disconnected and inaccessible from the live environment, multi-factored authentication is required to access cloud back-ups, etc.).

Please provide details on how you test your back-ups, including details on how frequently you test the full restoration of key server configurations and data from back-ups.

Please provide details on the number of back-up copies you take, including details on how you prevent separate back-up copies being impacted by the same event (if applicable).

CYBER INSURANCE QUESTIONS
BUSINESS CONTINUITY

Do you have a business continuity/disaster recovery plan? YES NO

If 'yes,' how frequently is it tested?

Do you enforce procedures to remove content (including third party content) that may infringe or violate any intellectual property or privacy right? YES NO

THOUGHTS AT THE END

- Cyber insurance will not go down in price or ease of acquisition in the near future and will be on an ever-increasing scale in both categories, if an organization can qualify at all
- The list of questions for qualification will continue to grow and become more complex
- One faulty answer to a single question might disqualify an organization from receiving coverage if a breach occurs or even getting coverage at all

Can RIM help on any of this – You bet!

QUESTIONS?

Rick Stirling

President

WesternIM

Risk.Stirling@WesternIM.com

Nicholas Fonseca

Information Management Business Lead/ Privacy Management Lead

City of Leduc

NicholasFonseca@hotmail.com

THANK YOU!