

BC ASSOCIATION  
of **CLINICAL**  
**COUNSELLORS**



 MITCHELL & ABBOTT  
INSURANCE BROKERS

 NAVACORD®

 NORTON ROSE FULBRIGHT

# Your Business has been Hacked: *Now What?*

What BCACC Members should know about cyber incidents,  
the experts that can help and the role of insurance

# AGENDA

1. Introducing our panelists
2. An update on cyber threat intelligence
3. The State of the Cyber Insurance Market
4. Protecting Your Network System
5. Who to call – The Role of Breach Counsel
6. The Insurance Offering for the BCACC

# Our Speakers



J.P. Mitchell (Moderator)  
Managing Partner,  
Mitchell & Abbott  
Group



## Mitchell & Abbott

Since 1921, the Mitchell & Abbott Group Insurance Brokers has a proven track record when it comes to providing insurance protection to commercial clients, regardless of the size or nature of their operations. Mitchell & Abbott is a member of the Navacord group of companies and has a specialization in developing insurance solutions for membership associations across Canada. Mitchell & Abbott is proud to represent the BC Association of Clinical Counsellors when it comes to membership insurance needs

The Right Insurance Protection For You



Patrick Bourk  
Vice President  
Cyber & Professional Lines  
Navacord



## Navacord

Navacord is a leading insurance and risk management brokerage firm dedicated to providing expert solutions to businesses and individuals across Canada. Navacord preserves the independence of its broker partners and builds on the deeply rooted, long-standing business relationships of its top experts who are making a difference in the communities they serve.

Local Touch. National Strength.



John Cassell  
Partner, Canadian Co-Head  
of Cybersecurity & Data  
Privacy  
Norton Rose Fulbright



## Norton Rose Fulbright

A global law firm with more than 3,000 lawyers and legal staff advising clients across more than 50 locations worldwide. NRF is recognized for its client service in key industries, including a global cybersecurity and data privacy practice composed of 80 dedicated lawyers based in the world's key jurisdictions. The practice group is recognized by the world's top insurance companies by appointment to the breach response panels of their claim's teams.

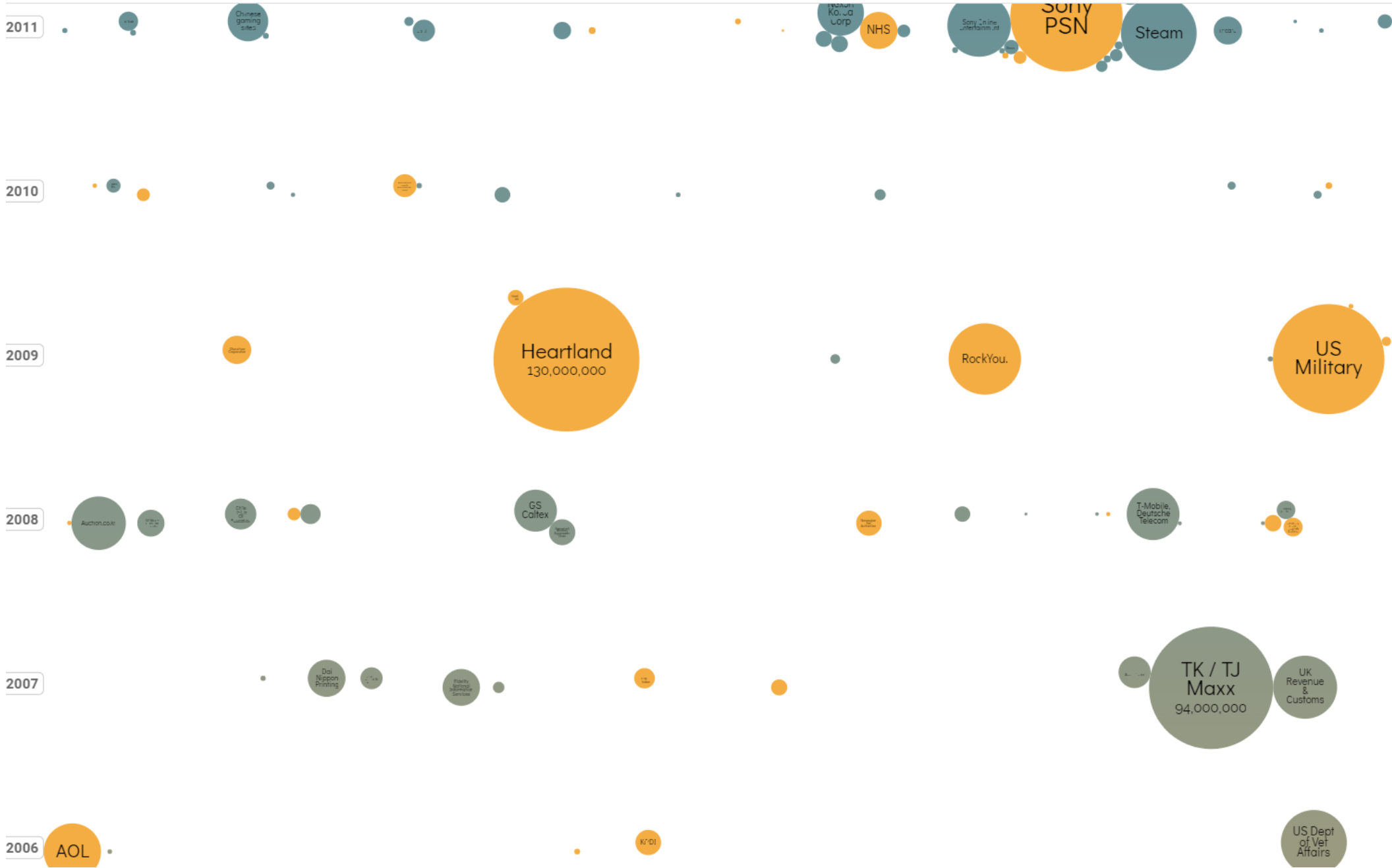
Law around the world

# Cyber Trends

David McCandless & Tom Evans

*Information is beautiful*

Sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others





# Cyber Threat Landscape

- According to the World Economic Forum, cybersecurity is in the **top 10 most serious risks** for companies for the next decade as it impact:
  - **Operations**
  - **Reputation**
  - **Finances**
  - **Legal Obligations**
- Boards and Senior Leadership Teams are focused on **building cyber resiliency**, whereby a victim organization bounces back from a cybersecurity incident
- Numerous cyber threats but key ones to focus on: Ransomware, Data theft, DDoS and Business email compromise (also known as BECs)

## \$6.94 million

The average cost of a cybersecurity breach to businesses in Canada according to IBM

## \$300,000

Average ransomware payment (Canada)

## 42%

Organizations that paid ransom which managed to have their data completely restored (Canada)

## 74%

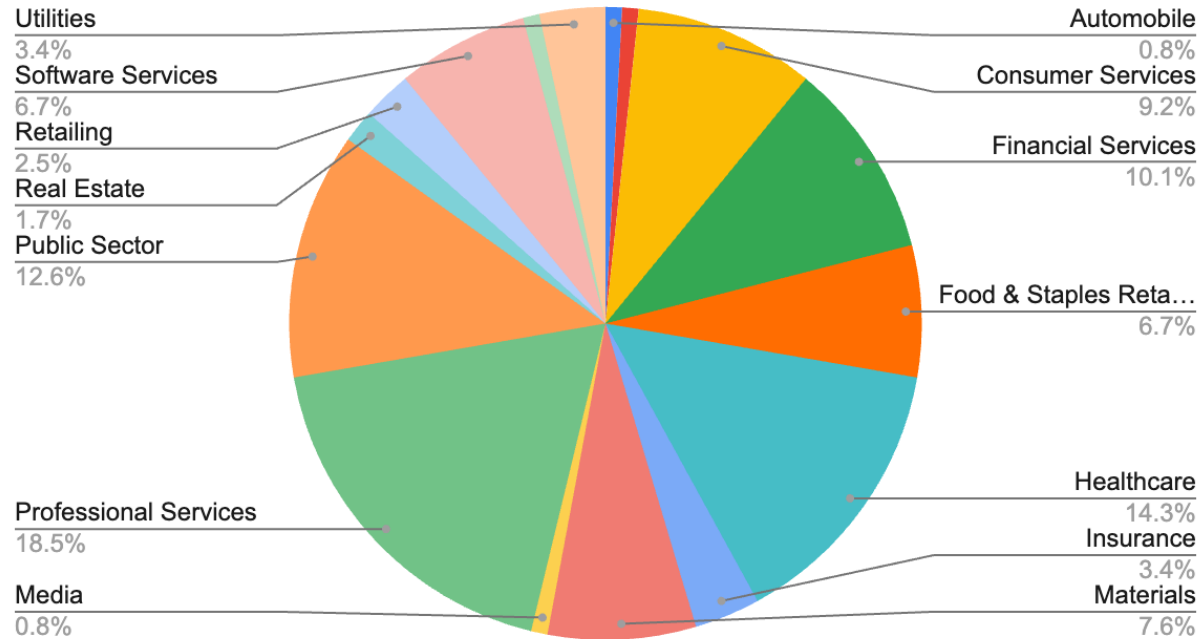
Of incidents in 2022 had human error as a factor, according to Verizon's Data Breach Investigations Report (2023)

## 43%

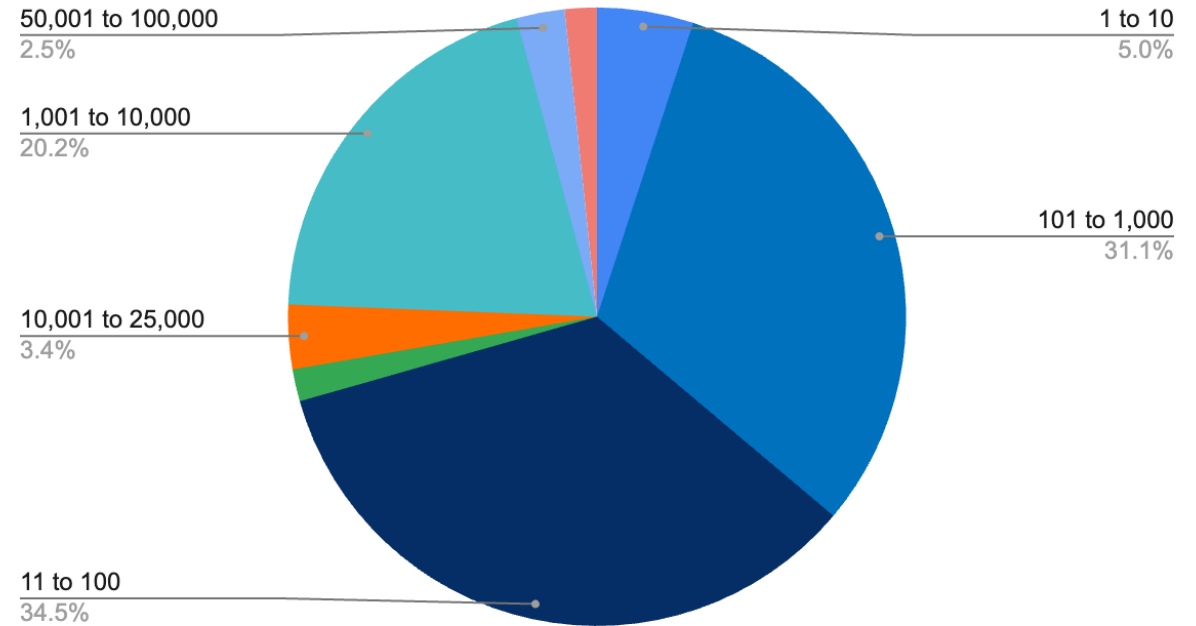
Of worldwide ransomware attacks were targeting **industrial organizations** and infrastructure in North America

# Ransomware Attacks

## Industries Impacted by Ransomware Q2 2024



## Ransomware Impacted Companies by Size (Employee Count)



# Phishing & Social Engineering

**Social Engineering is Responsible for 98% of Cyberattacks:**  
According to IBM, human error is the root cause of 98% of cybersecurity breaches, many of which stem from social engineering tactics.

Phishing attacks increased by a whopping 1,265% in 2023, thanks in part to the growth of generative AI (GenAI), according to "The State of Phishing 2023" report from SlashNext. The Anti-Phishing Working Group (APWG) observed almost 1.3 million phishing attacks in the second quarter of 2023, representing the third-highest quarterly total ever observed by the group.

**Social Engineering Frequency and Losses:**  
Social engineering crimes have escalated, with business email compromise (BEC) schemes becoming 15 times more frequent, leading to average losses of over \$326,000 per incident ([USI Insurance Services](#)).

**Small businesses** are especially vulnerable, experiencing **350% more social engineering attacks** than larger enterprises ([Firewall Times](#)).

In 2023, the **total financial impact** of social engineering attacks globally was estimated at **\$4.2 billion**, projected to rise to **\$4.8 billion** in 2024 ([Sci-Tech Today](#)).

**70% of organizations globally** reported experiencing at least one social engineering attack in 2023, with this figure expected to rise to **75% in 2024** ([Sci-Tech Today](#)).

While 48% of all SMBs have experienced a cyberattack, 43% of them have challenges understanding what security is actually required, according to the Sage Group.

# Cyber Trends and Insurance

a working relationship between its standard and VESIS. You can read more about this in our Appendix B.

So, enjoy the cognitive load we just removed from your (post-mortem) grey matter as we deep dive into specific results and detailed analysis for each pattern.

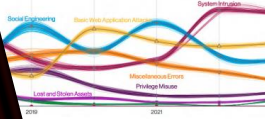
As we have in prior years, here we present our Incident Classification Patterns (patterns) and allow how they have changed over time. Figure 25 shows the patterns over time for incidents, and you can see that Denial of Service is top of the heap, as it has been for several years.

When you contrast this graphic with Figure 26, you can see how different the environment looks when we are focused on those incidents where there was confirmed data loss.

The System Intrusion pattern—with its more complex attacks—has been an overachiever and includes multiple attacks that include ransomware. But we're getting ahead of ourselves. Let's move into the detailed pattern sections for the data.

Basic Web Application Attacks	Denial of Service	Lost and Stolen Assets	Miscellaneous Errors	Privilege Misuse	Social Engineering	System Intrusion	Everything Else
These attacks are against a Web application, and after the initial compromise, they do not have a large number of additional Actions. It is the "get in, get the data and get out" pattern.	These attacks are intended to compromise the availability of networks and systems. This includes both network application layer attacks.	Incidents where an information asset went missing, whether through misplacement or malice, are grouped into this pattern.	Incidents where unintentional actions directly compromise a security attribute of an information asset fall into this pattern. This does not include lost devices, which are with their related.	These incidents are predominantly driven by unapproved or malicious use of legitimate privileges.	This attack involves the psychological compromise of a person that alters their behavior into taking an action impacting confidentiality.	These are complex attacks that leverage malware and hacking to achieve their objectives, including deploying Ransomware.	This "pattern" isn't really a pattern at all. Instead, it covers incidents that don't fit within the orderly confines of its patterns. Like that container where you keep all the electronics you don't own anymore. Just in case.

Table 1. Incident Classification Patterns



NetDiligence

## CYBER CLAIMS STUDY 2023 REPORT



### Perceptions of Risk

Organizations have become increasingly aware of the wide variety of cyber exposures they face, elevating risk management as a priority. This year's findings confirmed that the vast majority of respondents (83 percent) believe cyber risk is a significant concern for their organizations and that steps have been taken to assess their risk. Additionally, 69 percent of respondents have invested in cybersecurity solutions to mitigate their risk, and 60 percent confirmed that risk managers and IT professionals work together to monitor such risk.

Some organizations have also sought help from external parties to address cyber threats. Nearly two-thirds (66 percent) of respondents have partnered with outside firms to bolster their cybersecurity posture. In comparison, 53 percent have expanded cyber stakeholders in their organization to include board members and the IT department. While these are generally positive trends, they closely mirror last year's findings—suggesting some stagnation.

Certain comments from respondents on this topic clarify the challenges companies face today, with one respondent stating their organization had completed none of the provided options to manage their cyber risk and had instead adopted a "closed ostrich" approach.

### Insurance carriers' differences in appetite for cyber exposures and varied approaches to addressing systemic risk in portfolios have likely affected policy consistency, a rising proportion of insurance buyers noted this.

Specifically, more than half (66 percent) of respondents disagreed or completely disagreed that cyber coverage is consistent across insurance carriers, representing an increase of two percentage points from the previous year.

In the scope of managing coverage gaps and overlaps, this year's findings demonstrate that progress may have stalled from prior years. Nearly half (49 percent) of respondents said they are concerned about gaps between their cyber coverage and other insurance products that may also provide such coverage—the same percentage as in 2021, although down from 54 percent in 2020. In addition, 44 percent of respondents said they have noticed overlaps in coverage between their cyber insurance and other insurance products. This is an increase from 2021 (39 percent), yet a decrease from 2020 (48 percent).

Perhaps more concerning is the proportion of respondents who neither agreed nor disagreed with statements regarding cyber coverage gaps (27 percent) or overlaps (30 percent), which remained relatively unchanged from 2021. As mentioned in last year's results, this level of indifference seems particularly high for an issue with potentially severe consequences. Such indifference could have significant financial ramifications among organizations that experience cyber losses and discover they lack sufficient coverage. Amid a challenging cyber insurance market, it's possible that risk managers may be more concerned with simply securing some level of coverage rather than ensuring robust protection for their organizations. But, between this year's findings on policy inconsistency and today's increasingly litigious environment, attention to coverage gaps and overlaps is critical to help prevent major out-of-pocket losses.

## DBIR 2023 Data Breach Investigations Report

### Incident Cost by Revenue Size Claims >= \$1K 2018-2022

Revenue Size	Claims	Minimum	Average	Maximum	Total	% of Total	Rank by Claims	Rank by Cost
Nano-Rev (<\$50M)	3,647	1K	124K	5.2M	452.8M	20%	1	6
Micro-Rev (\$50M–\$300M)	1,430	1K	294K	11.4M	420.5M	19%	3	5
Small-Rev (\$300M–\$2B)	365	3K	995K	17.6M	363.3M	16%	4	4
Mid-Rev (\$2B–\$10B)	95	1K	3.8M	60.0M	362.3M	16%	5	3
Large-Rev (\$10B–\$100B)	34	18K	12.6M	65.8M	428.3M	19%	6	2
Mega-Rev (>\$100B)	3	10.6M	35.2M	55.0M	105.6M	5%	7	1
Unknown	2,326	1K	53K	2.3M	123.6M	5%	2	7

Table 3

Discussions regarding network security posture have become key. Without strong responses to the following types of questions the availability of coverage for most organizations has become challenging:

*Is multi-factor authentication (MFA) implemented for remote network access, e-mail systems, and privileged accounts?*

*Are all remote desktop protocol (RDP) ports closed or placed behind a VPN that is protected by MFA?*

*Is privileged account access limited to those who need access?*

*Do you use at least one e-mail filtration solution, such as, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), or Domain-based Message Authentication, Reporting & Conformance (DMARC)?*

*Do you use a next-gen antivirus solution?*

*Do you use an endpoint detection and response (EDR) solution?*

*Is at least one copy of backups stored off-site or in the cloud?*

*Do you have an Incident Response Plan and do you test it with Table Top Exercises?*

*Do you have a comprehensive employee cybersecurity hygiene training regime?*

\*



## CYBER INSURANCE

# Protect Your Business from Cyber Threats

Cyber insurance provides coverage for financial losses that result from cyber-attacks or data breaches. This includes costs associated with data recovery, legal claims, and regulatory fines.

At Mitchell and Abbott, we offer tailored solutions that address the specific needs of your business, keeping you protected in an increasingly digital landscape.

## PROTECT AGAINST CYBER THREATS

- **Social Engineering Fraud Coverage:** Protects individuals and organizations from financial losses caused by deceptive practices where victims are tricked into transferring money, sensitive data, or other valuable assets to fraudulent parties. These attacks typically involve criminals posing as trusted individuals—such as executives, vendors, or clients—to manipulate victims into taking harmful actions.
- **Data Breach Coverage:** Protects against costs of lost or stolen data, including customer notifications, credit monitoring, and legal fees.
- **Cyber Extortion:** Provides coverage for ransom payments and related costs from ransomware attacks.
- **Regulatory Fines:** Ensures compliance and covers legal defense costs or fines imposed by regulatory bodies after a breach.
- **Third-Party Liability:** Protects against claims from customers or partners affected by your breach.
- **Business Interruption:** Covers lost income and operational expenses due to a cyber-attack or system failure.

## CYBERSECURITY BEST PRACTICES

Understanding and being able to identify potential online fraud techniques is the key to keeping your company safe. Use the following tips to protect your intangible assets and ensure protection against a data breach:

- ✓ Never give sensitive information like social insurance numbers or credit card numbers out over the phone unless you know the person on the other line.
- ✓ Shred all credit reports and other sensitive data before disposal.
- ✓ Annual training on Cyber Security. Educate employees about the potential risks.
- ✓ Always monitor credit reports and other financial data for the company. If you see things that don't belong, investigate.
- ✓ Do not allow employees to write down passwords in the office.
- ✓ Always encrypt sensitive data.
- ✓ Use Multi Factor Authentication for cloud-based services and remote access.
- ✓ Regular back-ups of critical data to a separate location (i.e. offline/disconnected hard drive).
- ✓ Implement loss control measures such as; antivirus software, a firewall, regular software updates.
- ✓ Implement an endpoint detection and response (EDR) solution.
- ✓ If your company doesn't have an IT department, hire an outside company to set up the proper security measures for your computer network.
- ✓ Purchase Cyber Liability Insurance.

"We want to make it easier for you to identify and address any potential cybersecurity gaps at your organization. Cybersecurity experts are here to help you ensure that your business is protected from cyberattacks."

—Victor

Victor is offering a free cyber assessment & consultation (valued at \$397 CAN).

## WHAT CAN YOU EXPECT DURING A CYBER ASSESSMENT CALL?

In 90 minutes or less\*, a cybersecurity expert will:



### 1. Questionnaire

Guide you through a series of questions about your company's cybersecurity operations and practices, including the policies that you currently have in place.



### 2. Scorecard

Provide you with a customized cyber assessment scorecard based on your responses to a series of questions. They'll walk you through your customized cyber assessment scorecard and answer any questions or concerns that you may have.



### 3. Recommendations

Give you recommendations on next steps and the additional cybersecurity service packages available to you. Victor policyholders receive up to 30% off these packages.



### 4. Report

Last, but not least, provide you with a comprehensive cybersecurity report. This detailed formal report will help create the basis for a cybersecurity action plan for your company.

To get started: [Click Here](#) to book your cyber assessment appointment online.

## ABOUT MITCHELL & ABBOTT

Mitchell & Abbott Insurance Brokers is a full-service brokerage firm that has been delivering tailored insurance solutions for businesses, professionals, and individuals for over 100 years. With a client-first approach, we offer a wide range of products, including commercial, personal, and specialty coverages. Our expertise spans industries such as healthcare, construction, manufacturing, hospitality, and professional services. Known for personalized service, competitive pricing, and strong industry partnerships, we also provide exclusive insurance programs tailored to meet specific industry needs.

# Next Steps in Cyber Lifecycle

You are prepared! You have gotten help:



AWARENESS TRAINING



AUDITED YOUR NETWORK SYSTEM



REVIEWED YOUR VENDOR CONTRACTS



SECURED YOUR DATA



PURCHASED YOUR INSURANCE COVERAGE



## NOW WHAT?

# **The Role of Breach Coach and the Investigative Process**

**John Cassell, Partner**

Canadian Co-Head of Information Governance, Privacy and  
Cybersecurity



# Cyber Breach Counsel

- What does a breach counsel do?
  - Guide organizations and individuals through all elements of a data breach incident. Goal is to assist in minimizing risk and damages arising out of the incident.
  - Breach counsel has unique perspective of being involved in all elements of the incident response. Assistance includes:
    - Retaining incident response vendors (forensics, ransom negotiator, communications, restoration, credit monitoring, mailing services);
    - Directing privileged investigation into incident;
    - Advising on legal requirements (reporting/notification);
    - Assisting with incident communication strategy; and
    - Responding to investigations and litigation arising out of incident
- Much of incident response work streams are confidential or subject to legal privilege and largely unknown to external parties.



# Role of External Legal Counsel

Key Steps in the Breach Response Timeline	Coordinate Breach Response	Retain Vendors	Legal Regulatory	Other
	Containment	Digital Forensics	Notifications to Affected Parties	Asserting legal privilege (where appropriate)
	Restoration & Remediation	Crisis Communications	Reports to Regulators	Communications protocols
	Forensics	Data Mining	Business Partners	Coordinating with Law Enforcement
		Credit Monitoring	Litigation / Regulatory Investigations	Cross Border Issues

# How to Approach Ransomware Incidents

In the first  
24 hours

## ✓ Two swim lanes:

- Verify viability of backups and ability to restore without decryptor
- Engage with the threat actor

## ✓ Quickly identify sensitive data and impact if leaked publicly (if exfiltrated)

## ✓ Determine whether any obligations to notify patients, business partners or vendors have been triggered

## ✓ Develop & roll out communication to staff and other stakeholders



DO NOT

## ✗ Engage a vendor without consideration to legal privilege

## ✗ Directly engage with or negotiate with threat actor

## ✗ Put out any statement without legal review

## ✗ Create documents or reports without legal guidance

## ✗ Discuss the incident with individuals or organizations:

- Avoid speculation
- Avoid discussing matters “off the record”

# Containment

- Engagement of incident response and forensic experts by Breach Counsel under privilege
- Direction of privileged forensic investigation
  - Creation of incident response SOW
- Initial Breach counsel considerations during containment phase:
  - Scope of Incident - What systems are impacted?
  - Ransom note? (Do not engage the threat actor!)
  - Evidence of data exfiltration/theft ?
  - Operational Status?
  - Attack vector known?
  - Immediate containment steps possible?



# Forensic Investigation

- Conducted by third party forensic firm at the direction of legal counsel
- Importance of maintaining privilege over investigation and reports
  - Be mindful about relying on existing service agreements – enter into a new statement of work/agreement related to the specific incident at hand
- Scope of forensic investigation typically includes:
  - Root cause of incident
  - Attack vector
  - Data exfiltration / unauthorized access
  - Remediation recommendations (included in separate report)
- Limit sharing of forensic report regarding
  - Requests from auditors, customers, vendors, other third parties
  - Consideration of other avenues to provide responses

# Standalone Cyber Insurance Policies

## First Party

- **Incident Response:** Coverage for an actual or suspected cyber incident for costs related to retaining a “breach coach” and third-party computer expert services to determine the scope of the incident. Notification, credit monitoring, call center and public relations services may also be covered depending on the scope.
- **Network Extortion:** Coverage for extortion monies and associated expenses arising out of a criminal threat to release sensitive information or bring down a network
- **Data Recovery:** Coverage for costs incurred to replace, restore or recollect data which has been corrupted or destroyed as a result of an incident.
- **Business Interruption:** Coverage for loss of income and extra expense arising out of the interruption of network service due to the incident.

## Third Party

- **Cyber, Privacy and Network Security Liability:** Coverage for third party demands following data breach or failure of network security;
- **Payment Card Loss:** contractual liabilities owed to payment card industry firms as a result of a cyber incident;
- **Regulatory fines** and penalties (where legally insurable);
- **Media liability:** Coverage for liability following defamation or infringement online;
- **Defense costs:** Coverage for legal fees to defend against third party claims.



CYBER INSURANCE

# Protect Your Business from Cyber Threats

Cyber insurance provides coverage for financial losses that result from cyber-attacks or data breaches. This includes costs associated with data recovery, legal claims, and regulatory fines.

At Mitchell and Abbott, we offer tailored solutions that address the specific needs of your business, keeping you protected in an increasingly digital landscape.

## PROTECT AGAINST CYBER THREATS

- **Social Engineering Fraud Coverage:** Protects individuals and organizations from financial losses caused by deceptive practices where victims are tricked into transferring money, sensitive data, or other valuable assets to fraudulent parties. These attacks typically involve criminals posing as trusted individuals—such as executives, vendors, or clients—to manipulate victims into taking harmful actions.
- **Data Breach Coverage:** Protects against costs of lost or stolen data, including customer notifications, credit monitoring, and legal fees.
- **Cyber Extortion:** Provides coverage for ransom payments and related costs from ransomware attacks.
- **Regulatory Fines:** Ensures compliance and covers legal defense costs or fines imposed by regulatory bodies after a breach.
- **Third-Party Liability:** Protects against claims from customers or partners affected by your breach.
- **Business Interruption:** Covers lost income and operational expenses due to a cyber-attack or system failure.

## CYBERSECURITY BEST PRACTICES

Understanding and being able to identify potential online fraud techniques is the key to keeping your company safe. Use the following tips to protect your intangible assets and ensure protection against a data breach:

- ✓ Never give sensitive information like social insurance numbers or credit card numbers out over the phone unless you know the person on the other line.
- ✓ Shred all credit reports and other sensitive data before disposal.
- ✓ Annual training on Cyber Security. Educate employees about the potential risks.
- ✓ Always monitor credit reports and other financial data for the company. If you see things that don't belong, investigate.
- ✓ Do not allow employees to write down passwords in the office.
- ✓ Always encrypt sensitive data.
- ✓ Use Multi Factor Authentication for cloud-based services and remote access.
- ✓ Regular back-ups of critical data to a separate location (i.e. offline/disconnected hard drive).
- ✓ Implement loss control measures such as; antivirus software, a firewall, regular software updates.
- ✓ Implement an endpoint detection and response (EDR) solution.
- ✓ If your company doesn't have an IT department, hire an outside company to set up the proper security measures for your computer network.
- ✓ Purchase Cyber Liability Insurance.

## EXCLUSIVE CYBER LIABILITY OFFER FOR MEMBERS OF THE BCACC

	Deductible	Limit of Liability
A.1. Security Liability Coverage, A.2. Privacy Liability Coverage, A.4. Regulatory Proceedings Coverage	\$2,500.00 CAD	\$500,000.00 CAD each Claim \$500,000.00 CAD Aggregate each "Named Insured"
AND		
B.1. Breach Cost Coverage, B.2. Cyber Extortion Coverage, B.3. Digital Asset Replacement Cost Coverage	\$2,500.00 CAD	\$100,000.00 CAD each Claim \$100,000.00 CAD Aggregate each "Named Insured"
AND		
B. 10. Social Engineering Funds Transfer Fraud Event, B. 11. Social Engineering Theft of Funds Held In Trust Coverage, B. 12. Social Engineering Theft of Personal Funds	\$2,500.00 CAD	\$25,000.00 CAD each Claim \$25,000.00 CAD Aggregate each "Named Insured"

Coverage is contingent on the submission of a Warranty Statement which confirms that the following cyber controls are in place:

- Multi factor authentication (MFA) for cloud-based services (such as cloud-based email account access) and for all remote access to your network; or, the business will use Jane, Clinicmaster, Owl Practice or Practice Perfect, with MFA (or2FA) enabled.
- Regular back-ups of critical data to a separate location (such as an offline/disconnected hard drive) that would be unaffected by an issue within your Environment.
- Annual training on Cybersecurity.
- Implement loss control measures such as: Antivirus software, a firewall, and/or regular software updates.

Program aggregate \$10,000,000 each Policy Period for all payments under all Coverages combined for all Subscribers under each certificate.

Annual premium starting as low as \$201.

Higher coverage limits are available upon request.

# Key Takeaways:

- The cyber insurance market continues to mature in response to new threats
- Take advantage of services to help protect your network
- Be familiar with the lifecycle of how a cybersecurity incident is managed – who to call
- Know your insurance coverage and what it can do for you that is unique to your business

# Questions?



NAVACORD®

 MITCHELL & ABBOTT  
INSURANCE BROKERS

 NORTON ROSE FULBRIGHT

BC ASSOCIATION  
of CLINICAL  
COUNSELLORS 