



# Improving Your Organization's Cyber Resilience

Foglers' Bill Hearn & April Gougeon,  
with external experts Patrick Bourk & Jason Kotler  
April 27, 2023



# Outline

- Welcome & Introduction
- Cyber Insurance
- Cyber-Extortion & Ransomware Investigations, Negotiations & Settlements
- Cyber Incident Reporting
- Takeaways
- Questions

# External Expert- Patrick Bourk



**Patrick Bourk, B.A., LL.B., Cyber COPE® Insurance Certification<sup>SM</sup>**  
**Specialty Insurance Consulting**  
**Mobile: 416.302.0886**  
**Email: patrickbourk0@gmail.com**

- In 2007 cyber liability insurance was almost unknown in Canada. After negotiating my first insurance placement for a client it was my belief that data protection and network security would become a growing area of risk for companies. I became a cyber insurance devotee and am now proud to be a thought leader in the cyber insurance and cyber risk field.
- As a former insurance coverage lawyer and specialty insurance broker for the past 20+ years, I have developed a strong and supportive network of cyber specialists in the insurance, legal, incident response and consulting communities.
- Recent positions that I have held include:
  - Equifax, SVP of the Global Breach Services Practice
  - HUB Insurance Brokers, SVP National Cyber Practice Leader
  - Integro Insurance Brokers, Partner and Management Risk Practice Leader
  - Travelers Insurance Company of Canada, Senior Claims Specialist and Coverage Counsel
- I have been involved in: advising insurance companies on their cyber policy wordings and products; connecting breach coach lawyers and IT incident response firms with insurance claims departments; placing insurance coverage and counselling all sizes of companies and professional firms on their cyber insurance needs as well as their pre- and post-breach preparedness.
- I am a frequent speaker at conferences and symposiums focusing on cybersecurity topics both in Canada and the U.S. and I am a member of the NetDiligence Summit Advisory Council.
- I am proud to hold a Cyber COPE Insurance Certificate designation after completing an executive certification in Cybersecurity through Heinz College of Carnegie Mellon University. I am currently a Faculty Advisor to the Program and lecture on cyber insurance for the Heinz College Executive Education, Chief Risk Officer Program.
- I currently offer independent insurance consulting services and I am a consultant for the Insurance Training Center, a global provider of online professional and management liability insurance courses.

# External Expert- Jason Kotler

## ABOUT CYPFER | President's Bio



Recovering Lawyer, circa 2002

- **Jason S.T. Kotler, BA, JD, MBA, CMC** – Jason has significant global experience founding, operating and advising to companies and leading strategic corporate cybersecurity and privacy law initiatives.
- He has held Founder/CXO/Board, Private Equity, Investor and Management Consultant roles in the Cybersecurity, IOT/IIOT, CleanTech, Renewable Energy, Technology and Medical Devices industries.
- Prior to founding CYPFER, was Chief Administrative Officer, Waterton Global Resource Management Private Equity Fund (\$2.5B AUM), a Technology Startup Founder / Professional, a Senior Strategy & Transformation Consultant with Capgemini and he **practiced Privacy, IP, Technology and Corporate Commercial law with McMillan LLP.**
- Jason is a former Board Member of The Atmospheric Fund and is a member of its Investment Committee (\$100M AUM).
- Jason is a member of the Law Society of Ontario, holds an MBA (Deans Honours) from the Richard Ivey School of Business, a **JD from Osgoode Hall Law School**, a Bachelor of Art, Visual Arts (with Distinction) from Western University, and is a Certified Management Consultant (CMC).



# Cyberattacks: On the Rise

Toronto

## Data breach at Toronto health network possibly exposed patient information, OHIP numbers



Leak affects patients at Scarborough Health Network hospitals prior to Feb. 1

CBC News · Posted: May 25, 2022 1:26 PM EDT | Last Updated: May 25, 2022

TECHNOLOGY > CYBERSECURITY | April 12, 2022

## Panasonic confirms cyberattack after Conti leaks data

Electronics giant Panasonic has confirmed that its systems were breached in February after ransomware group Conti leaked files online.

BUSINESS

## Indigo website still down and company likely losing 'millions' after cybersecurity attack last week

Cyber incident on Feb. 8 impacted website and electronic payment system, but stores remain open and company says it is working with experts to investigate and resolve.



By **Clarrie Feinstein** Business Reporter  
Wed., Feb. 15, 2023 · 4 min. read

## Canadian Telecom Firm Telus Reportedly Investigating Breach

A threat actor has leaked data — purportedly, samples of Telus employee payroll data and source code — on a hacker site.

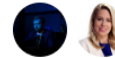


**Jai Vijayan**  
Contributing Writer, Dark Reading

February 24, 2023

CANADA

## Global Affairs Canada suffers 'cyber attack' amid Russia-Ukraine tensions: sources



By **Alex Boutilier** & **Mercedes Stephenson** · Global News  
Posted January 24, 2022 11:45 am · Updated January 24, 2022 9:11 pm

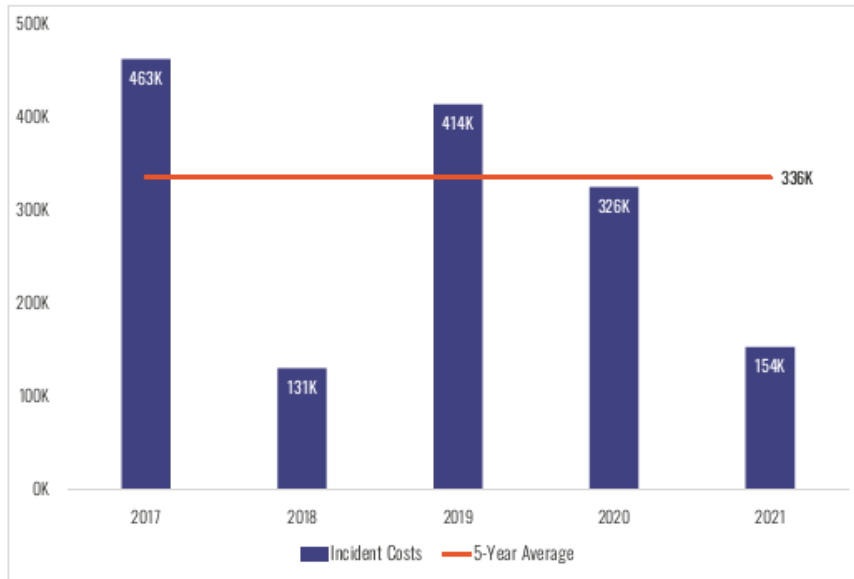
HEALTH

## SickKids reports cybersecurity incident, affecting some phone lines and web pages

By Staff · **The Canadian Press**  
Posted December 20, 2022 9:16 am · Updated December 20, 2022 1:56 pm

# NetDiligence Cyber Claims Study 2022

Average Incident Cost – Canada  
All Revenue Sizes  
(N=267)



Canada  
Top Causes of Loss 2017-2021 – SMEs

| Cause of Loss             | Claims | Average Incident Cost |
|---------------------------|--------|-----------------------|
| Ransomware                | 35     | 563K                  |
| Business Email Compromise | 17     | 181K                  |
| Hacker                    | 11     | 121K                  |
| Staff Mistake             | 7      | 34K                   |
| Wire Transfer Fraud       | 6      | 759K                  |
| Malware/Virus             | 17     | 178K                  |

# Cyber Resilience: A Multifaceted Plan

Cyber Insurance



Cyber Incident Response Plan  
(IRP)



Written Information Security  
Program (WISP)\*

\*Mandatory for public companies and companies in the financial services, health care and telecommunications sectors

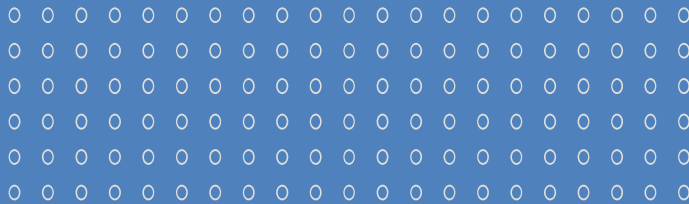




# Cyber Insurance and the State of the Market

Patrick Bourk, *B.A., LL.B.*  
*Specialty Insurance Consulting*

# 1



## The State of the Market: Risks and Challenges

---

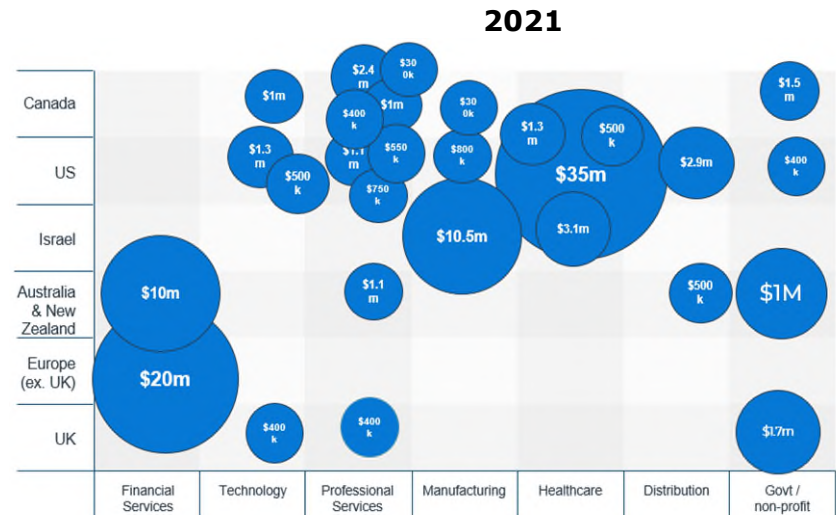
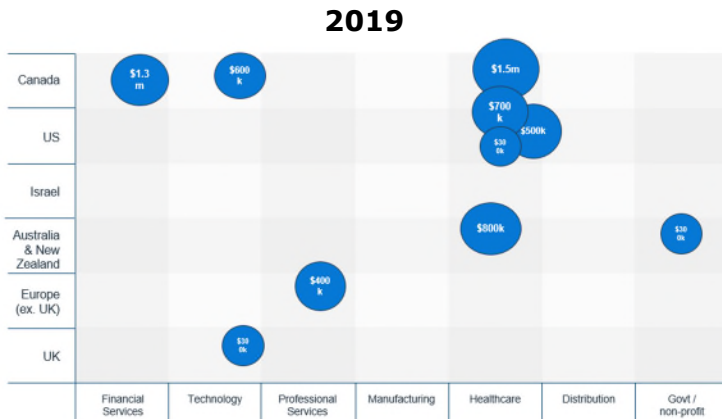


# CYBER RISK IS EVERYWHERE - RECENT 5 YEAR ACTIVITY

Ransomware attacks continue to impact organizations of all size and scope

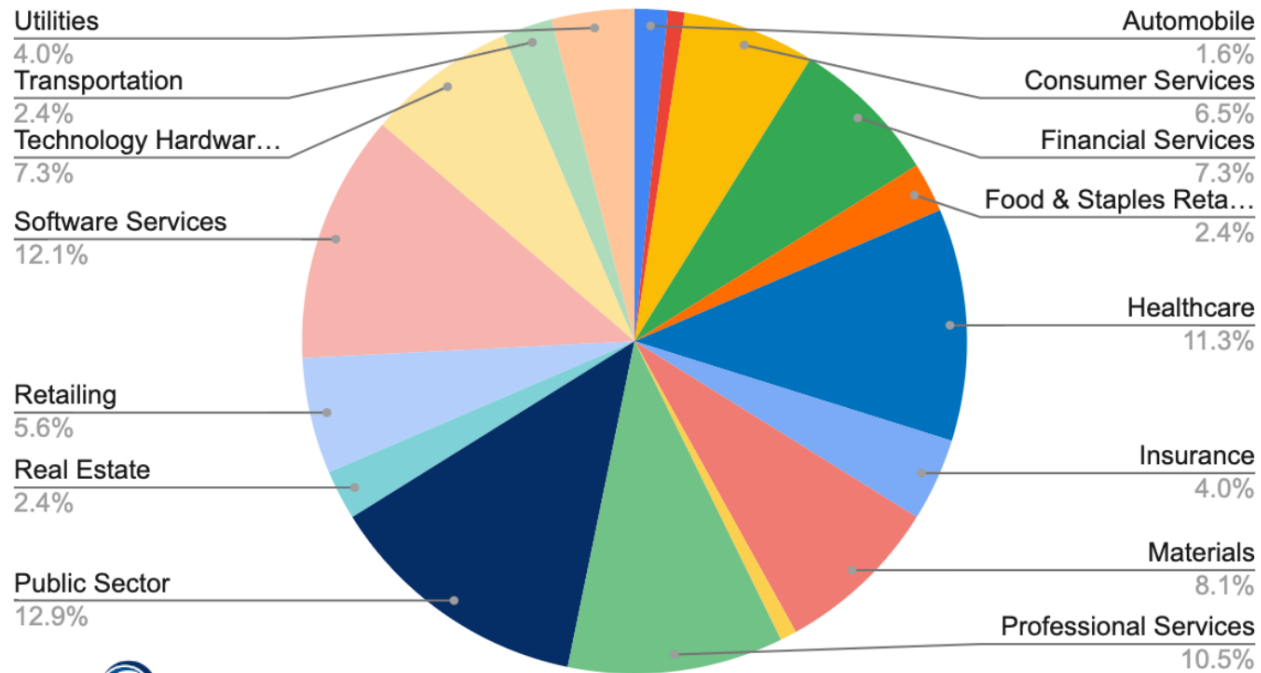
- **86%** of ransomware attacks involved the threat to leak exfiltrated data (as of Q2 2022)\*
- **24** was the average days of downtime for an organization suffering a ransomware attack (as of Q2 2022)\*
- 2022-2023 Ransomware Headlines:
  - Chick-fil-A: (Dec. 2022 – Feb. 2023) **71,000 individuals affected**
  - Sobeys: (Nov. 2022 – Feb. 2023) **\$25M+ expected cost**
  - Indigo: (Feb 2023) **TBD**
  - LCBO: (Jan 2023) **TBD**

**400%** was the percentage increase in the loss ratio in 2020 over 2019 for cyber insurers regulated by OSFI\*\*



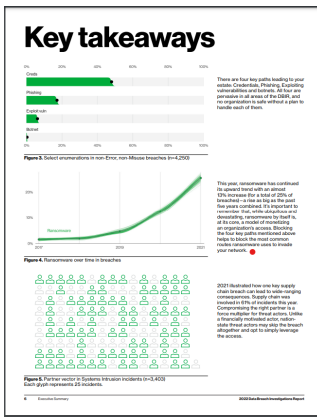
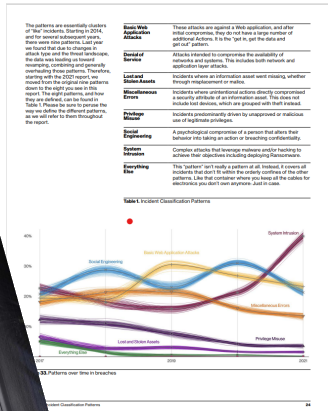
# WHO IS AT RISK?

## Common Industries Targeted by Ransomware Q4 2022



Source: Coveware

# ANNUAL REPORTS FROM NOTED SOURCES



Overview Resources Webinars Sign up Segment reports Archive Contact us

## Know what your business is up against.

# 82%

of breaches involved the Human Element, including Social Attacks, Errors and Misuse.

# 13%

increase in Ransomware breaches — more than in the last 5 years combined.

# 62%

of incidents in the System Intrusion pattern involved threat actors compromising partners.

## Information Security and Cyber Risk Management

October 2022

ZURICH | Advisen

### Perceptions of Risk

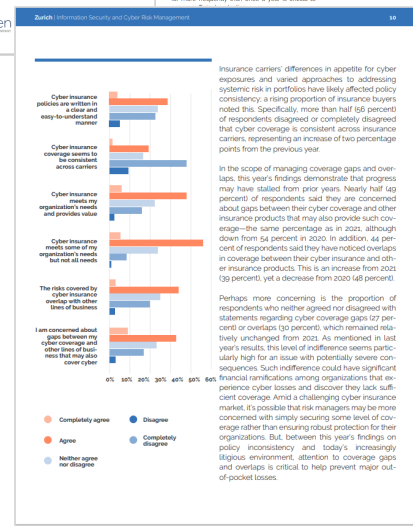
Organizations have become increasingly aware of the wide variety of cyber exposure, they face, elevating risk management as a priority. This year's findings confirmed that the vast majority of respondents (83 percent) believe cyber risk is a significant concern for their organizations and that steps have been taken to assess their risk. Additionally, 56 percent of respondents have invested in cybersecurity solutions to mitigate their risk, and 50 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 (64 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 IT department alike; these are generally positive trends, they classify minor risk, and 50 percent confirmed that risk managers and IT professionals work together to monitor such risk.

Certain comments from respondents on this topic clarify the challenges companies face today, with one respondent stating that their organization had consulted none of the provided options to manage their cyber risk and instead selected a "blind assessment." Another respondent cited a "blind assessment" with IT and cyber risk management together. One respondent identified cybersecurity as an "annual strategy" although this comment suggests that cybersecurity is being viewed as a strategic investment, addressing cyber exposure for more frequently than once a year is critical to

How has your organization's approach to cyber risk management evolved over the years? Please select all that apply.

- Other risk has become a more significant concern for our organization and we have taken steps to assess our risk. **83%**
- We have invested in cybersecurity solutions to mitigate our risk. **56%**
- We have expanded our cyber stakeholders. **53%**
- We have partnered with outside firms to bolster our cybersecurity posture. **64%**
- Risk management and IT professionals work together to monitor such risk. **50%**
- We have involved external parties to address our cyber risk. **64%**
- Other: Please Specify. **8%**

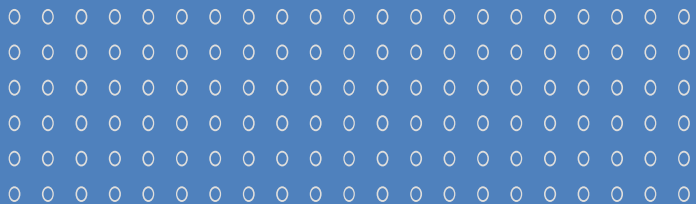




# 2

## Transferring Risk with Insurance

---



# NETWORK SECURITY & PRIVACY LIABILITY INSURANCE

To what extent do traditional insurance policies respond to breaches?

Common insurance policies purchased by most enterprises that may or may not respond to network security or privacy breach situations:

- General Liability
- Business Interruption
- Fidelity (Crime)
- Directors' & Officers' Liability
- Fiduciary Liability

---

Third party insurance coverage versus first party direct loss coverage

---

Pros and Cons of adding Cyber coverage to traditional insurance policies by way of endorsement

---

# EXAMPLE OF HOW TRADITIONAL INSURANCE POLICIES RESPOND TO BREACHES

## LawPRO “Limited Cyber Crime” Coverage

- 3<sup>rd</sup> party coverage only
- As a direct consequence of the performance of Professional Service
- \$250,000 sublimit

### Part V DEFINITIONS

- (a) **ADMINISTRATIVE DISMISSAL** means dismissal of an action for delay (including, without limitation, through breach of an order, direction or timetable), or by reason of abandonment pursuant to Rules 48.14 or 48.15 of the Rules of Civil Procedure, R.R.O. 1990, Regulation 194, as amended or as may be provided in equivalent successor legislation.
- (b) **CANADIAN FINANCIAL INSTITUTION** means a “Canadian financial institution” as defined under the Bank Act, S.C. 1991, c.46, but does not include an entity that is primarily engaged in dealing in securities, including portfolio management and investment counselling.
- (c) **CIRCUMSTANCE(S)** means any circumstances of an alleged, actual, or possible error, omission, or negligent act of which the INSURED becomes aware, which from the perspective of a reasonable LAWYER or LAW FIRM could potentially give rise to a CLAIM hereunder.
- (d) **CIVIL SUIT** means an action, application or arbitration in which a CLAIM
- (h) **CORPORATE EMPLOYER** means a corporation as well as affiliated, controlled and subsidiary companies or other entity of the corporation for which the INSURED is an EMPLOYEE or SECONDED LAWYER, where “affiliated”, “controlled”, and “subsidiary” are as defined under the Securities Act, R.S.O. 1990, c.S.S.
- (i) **COUNTERFEIT CERTIFIED CHEQUE(S) OR COUNTERFEIT BANK DRAFT(S)** means a fake instrument purported to be drawn upon a CANADIAN FINANCIAL INSTITUTION that resembles a certified cheque or bank draft to such an extent that it is reasonably capable of passing for a certified cheque or bank draft, but not a certified cheque or bank draft that has merely been altered and/or signature endorsement forged.
- (j) **CYBERCRIME(S)** means an incursion, intrusion, penetration, impairment, use or attack of a COMPUTER SYSTEM(S) by electronic means by a third party, other than the INSURED or the INSURED’S LAW FIRM.

### Endorsement No. 14 LIMITED CYBERCRIME COVERAGE

This POLICY, subject to all its terms and conditions not in conflict with this endorsement, shall include the following:

#### A. Coverage:

Notwithstanding Part III Exclusion (j), but subject to the SUBLIMIT OF LIABILITY, terms and conditions contained in this endorsement, coverage in accordance with Part I, Coverage A and/or the POLICY, is hereby provided for CLAIM(S) arising out of liability for a CYBERCRIME(S), provided such CYBERCRIME(S) results in:

- (i) the disclosure, destruction, modification, corruption, manipulation, damage, deletion, theft or misuse of any confidential client data which has been entrusted to, received by and held in trust by or on behalf of the INSURED as a direct consequence of the performance of PROFESSIONAL SERVICES; or

- (g) **COMPUTER SYSTEM(S)** means any electronic device, component, network or system, or any protocol, portal, storage device, media, or electronic document, or any computer software, firmware or microcode, or any associated technology which receives, processes, stores, transmits or retrieves data either locally or remotely, or any part thereof, whether stand-alone, interconnected or operating as part of an integrated system or process, for use by or on behalf of the INSURED and/or the INSURED’S LAW FIRM.

- (ii) the misappropriation of money which was entrusted to, received by and held in trust by or on behalf of the INSURED as a direct consequence of the performance of PROFESSIONAL SERVICES.

#### B. SUBLIMIT OF LIABILITY:

The amount of coverage provided with respect to this endorsement shall be subject to a SUBLIMIT OF LIABILITY of \$250,000 per CLAIM and in the aggregate per POLICY PERIOD for the INSURED. This SUBLIMIT OF LIABILITY is included within the LIMIT OF LIABILITY and AGGREGATE LIMIT OF LIABILITY OF THE INSURER, as set out in ITEMS 5 and 6 of the Declarations. The total limit of the INSURER’S liability pursuant to this endorsement, for each CLAIM, regardless of the number of INSUREDS who may be in a LAW FIRM, shall be \$250,000 per POLICY PERIOD for each LAW FIRM.



# NETWORK SECURITY & PRIVACY LIABILITY INSURANCE

## Privacy Liability:

Covers loss arising out of the organization's failure to protect sensitive personal or corporate information in any format. Can also be enhanced to provide coverage for regulatory proceedings brought by a government agency alleging the violation of any federal, state, or foreign identity theft or privacy protection legislation.

---

## Network Security Liability:

Covers any liability of the organization arising out of the failure of network security, including unauthorized access or unauthorized use of corporate systems, a Denial-of-Service attack, or transmission of malicious code.

---

## Internet Media Liability:

Covers infringement of copyright or trademark, invasion of privacy, libel, slander, plagiarism, or negligence by the organization from the content on its' internet website

---

## NETWORK SECURITY & PRIVACY LIABILITY INSURANCE: *FIRST PARTY EXPENSES*

### Data Breach Expenses

- **Legal Expenses:** Coverage to retain “breach coach” lawyer to manage a breach incident
  - **Forensic Expenses:** Coverage to retain third party computer forensics services to determine the scope of a Network Security failure
  - **Notification Expenses:** Coverage to notify customers of sensitive personal information breach
  - **Crisis Management Expenses:** Coverage to obtain legal, public relations or crisis management services
  - **Credit Monitoring Expenses:** Covers the cost of credit monitoring, credit freezing or fraud alert services
- 

**Network Extortion:** Covers extortion monies and associated expenses arising out of a criminal threat to release sensitive information or bring down a network unless consideration is made.

---

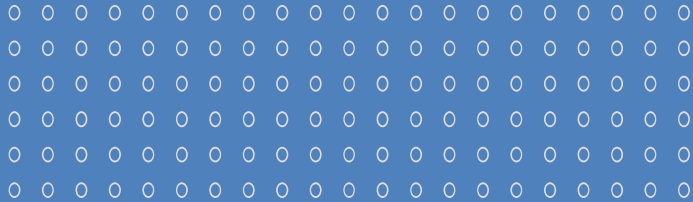
**Digital Asset Loss:** Covers costs incurred to replace, restore or recollect data which has been corrupted or destroyed as a result of a network security failure.

---

**Business Interruption Loss:** Covers loss of income and extra expense arising out of the interruption of network service due to an attack on the insured’s network.

---

# 3



## Getting Coverage in the Current Market

---





# The 5 “Levers” of the Cyber Insurance Market

## Claims

- Overall claims frequency and severity remains high
- Insureds taking a “DIY” approach to incident response is having a devastating effect.

## Premium & Retentions

- Pricing increases are relative. Depending on specific factors you should expect anywhere from 30% to 400% increases
- Retentions on renewals are at least double
- It’s not about cost, it is about coverage!

## Capacity & Attachments

- Insurers are reluctant to provide more than \$5M limits
- Excess is preferred over primary and attachment points are very high
- Underwriters have met budgets for 2021 and it is safer to “put pens down” rather than risk deploying capacity
- “Inverted” towers and “By Part Pricing” are becoming common

## Coverage Terms

- Serious restrictions on ransomware coverage
- Sub-limits and co-insurance clauses are more common
- Targeted coverage exclusions including: restrictions related to SolarWinds, MS Exchange Server, poor patch management, lack of MFA, etc.

## Underwriting Scrutiny

- Underwriters will insure only ‘Best in Class’ risks
- Full Applications and Supplemental Ransomware Applications are mandatory
- Almost all insurers use scanning technologies in their underwriting process
- Best to make use of in-house cyber risk engineers at insurance companies



## EXPECT A RIGOROUS UNDERWRITING PROCESS

Discussions regarding network security posture will be key. Without strong responses to the following types of questions the availability of coverage (*or insurability*) may be in doubt:

1. Is **multi-factor authentication** (*MFA*) implemented for remote network access, e-mail systems, and privileged accounts?
2. Are all remote desktop protocol (*RDP*) **ports closed** or placed behind a VPN that is protected by MFA?
3. Is privileged **account access limited** to those who need access?
4. 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*)?
5. Do you use a **next-gen antivirus** solution?
6. Do you use an **endpoint detection and response** (*EDR*) solution?
7. Is at least one copy of **backups stored off-site** or in the cloud?
8. Do you have an **Incident Response Plan**, and do you test it with Tabletop Exercises?
9. Do you have a comprehensive **employee cybersecurity hygiene training** regime?

# PREPARATION FOR PLACEMENTS AND RENEWALS

Tell all your friends

- Know your risk profile and how the market is changing
- 

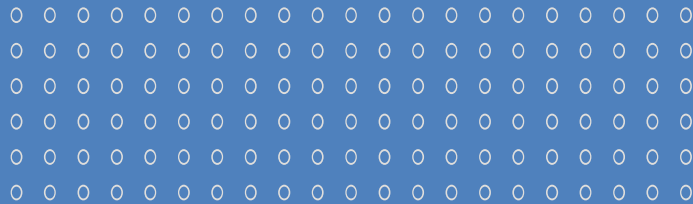
Start as soon as possible

- Placements and renewals will take more time
  - Expect a fulsome application and supplemental questionnaires
  - Network security weaknesses will be punished!
- 

Scrutiny is yearlong and loss prevention is becoming key

- Insurers are relying on scanning technologies
  - Employee Hygiene Training
  - Pen Testing
  - Incident Response Planning and Tabletop Exercises
-

# 4



## Aligning Risk Transfer with Breach Response Planning

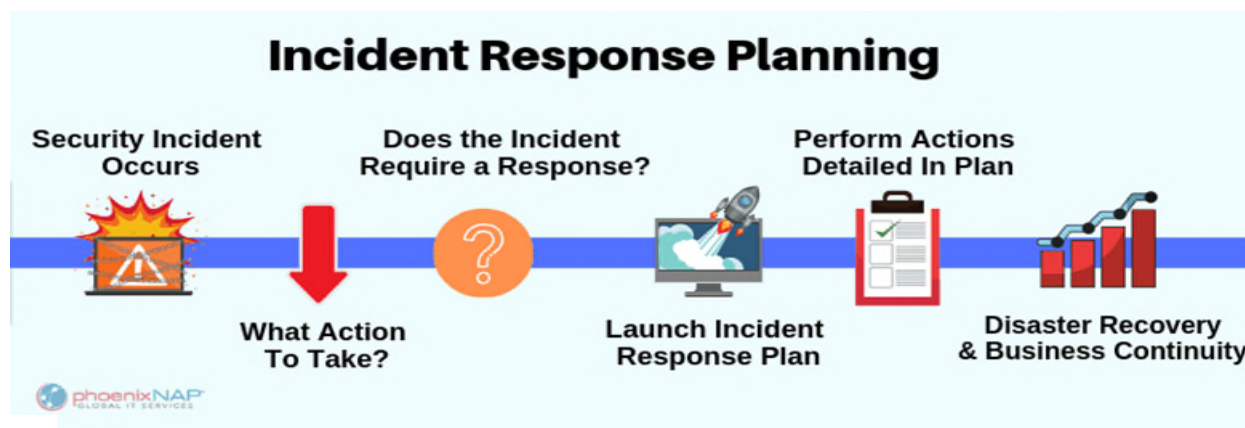
---



# PRE-BREACH PREPAREDNESS

## It's time for Incident Response Planning

- What is a Cyber Incident Response Plan?
  - A comprehensive plan for addressing network security and/or privacy liability threats and attacks. The plan provides a kind of roadmap or “playbook” with guidance on steps to be taken (i.e. who to call, what to do, when to do it, etc.) and how best to document them from the time of the suspected breach to post-incident response closure



Source: <https://phoenixnap.com>



# Cyber-Extortion & Ransomware Investigations, Negotiations & Settlements

Jason Kotler, *BA, JD, MBA, CMC*  
*President, CYPFER*



# CYPFER | Cyber-Extortion Advisory



## CYPFER

Website: [www.CYPFER.com](http://www.CYPFER.com)

HQ: Toronto, Ontario, Canada

Founded: October 2019

Associate Partner:

**NO MORE RANSOM!**

[www.nomoreransom.org](http://www.nomoreransom.org)

- CYPFER Corp. ("CYPFER") is a global, market-leading Cybersecurity Advisory firm, based in Toronto, Canada, with technical expertise in cybersecurity breaches and cyber-attacks, cyber-extortion and ransomware investigations, negotiations, cryptocurrency sourcing and settlements, emergency cyber-attack incident first-response, and post-breach recovery and remediation.
- **With over 4,000 Ransomware Matters Negotiated**, our Team comprises of leaders from the IT Security, Legal, Forensics, Law Enforcement, Finance, Technology and Operations fields, and has worked for both public and private companies, at various growth stages, across diverse industries
- CYPFER's seasoned and expert ER Team is razor-focused on helping organizations of all sizes and targeted high-profile individuals respond and recover from Cyber-Attacks and Cyber-Extortion.
- We specialize in conducting complex threat intelligence operations and engagement with cyber-attackers ("Threat Actors"), including investigations, communications, negotiations and where required, cyber-settlements, in response to cyber-attacks, cyber-extortion, and ransomware incidents.





# RANSOMWARE | Ransom Note, Chat Room Examples



**Your network was compromised.**

**Important Files on your network was downloaded and encrypted.**  
We used an asymmetric cipher to encrypt your files. Meaning the only way to decrypt them is to have a **Private Key**.  
Our custom **Decrypt App** is bundled with your **Private Key**.  
In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live Chat**.  
Act quickly to get a discount!

Decrypt App Price

You have **4 days, 09:22:09** until:

- **Decrypt App** special discount period will be discontinued.
- Discount price is available until **12/14/21, 3:41 AM**

Discount Price: **\$3000000**  
Full Price: **\$3500000**

Status

Awaiting payment of **\$3000000** to one of the following wallets:

|         |  |                               |
|---------|--|-------------------------------|
| Bitcoin |  | \$3450000 (?) = 71.533725 BTC |
| Monero  |  | \$3000000 = 15495.867769 XMR  |

[Instructions](#)   [Live Chat](#)   [Trial Decrypt](#)   [Intermediary](#)

I wish to pay with  
Bitcoin




# CYBER-EXTORTION



HOME AUCTION NEWS ABOUT CONTACT US

800 601 2017



**Welcome to the Karakurt hacking team website. You can browse and download the files that were leaked. Read our news. Learn more about us and on how we operate.**

Our lair is divided into 3 stages\rooms\levels call it what you want. The deeper you get the worse is your situation!

## vol.4 Autumn Data Leak Digest

27 NOV 2021, 15:10:00



**D**ear visitors, customers & journalists. Here is 4th volume of our victims that either stopped negotiations or simply ignored our welcoming letter.

Jones Studio Inc. - [jonesstudioinc.com](http://jonesstudioinc.com) - Architecture/Design  
Five Star Products, Inc. - [fivestarproducts.com](http://fivestarproducts.com) - Industrial  
RI Analytical Laboratories Inc - [rianalytical.com](http://rianalytical.com) - Environmental Services  
Contech TopSystems AG - [contech.com](http://contech.com) - Technology  
Petro-Serve USA - [petroserviceusa.com](http://petroserviceusa.com) - Energy  
Valley Realty - [valleyreality.com](http://valleyreality.com) - Real Estate  
PACE Worldwide - [paceworldwide.com](http://paceworldwide.com) - Industrial

So, as you all can see our variety of victims is unpredictable. Every company can be under attack. Some cases will be as big as their future consequences because of ignoring our message. At the moment we have 3 big data leaks that will be posted separately containing some interesting insight information.

In the next post we are going to choose one of those: [SPREADSHIRT.COM](http://SPREADSHIRT.COM), [INSUREON.COM](http://INSUREON.COM) or [BASSPRO-CABELLAS.COM](http://BASSPRO-CABELLAS.COM). You can help us by sending your votes via contact form. Let us choose their destiny together...

Please, stay tuned & follow our updates. Our roller coaster is speeding.

### RECENT POSTS



vol.3 Autumn Data Leak Digest



vol.2 Autumn Data Leak Digest



vol.1 Autumn Data Leak Digest



ALL RIGHTS RESERVED. DESIGNED BY SANDRA BULLOCK

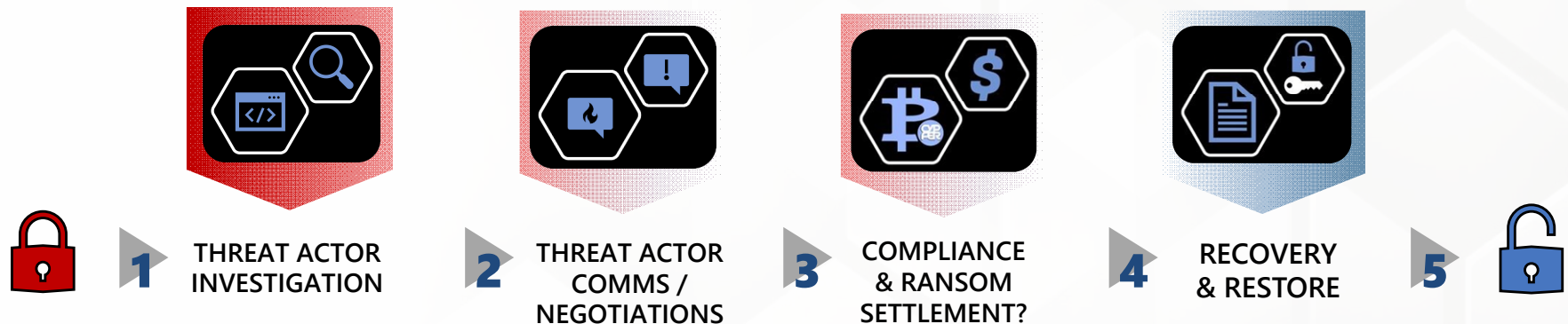
We thought for a long time what to write on this page. Since you're here - you've got the point by now, right? You probably think that we are nothing more than another team of online scammers trying to make money. In part, this is probably true, but for us the situation looks different. So how are we different in our opinion? We strongly condemn the low threshold of knowledge required now to implement attacks on commercial networks, hacking turns into a routine work, frameworks have simplified the process to trivial button presses. For our part, we try to approach our work as creatively as possible, improving various techniques and deeply immersing ourselves in the study of products related to modern information security tools. If you've been the victim of a hack and data theft, don't be in a rush to blame your security team, it just wasn't their day. The budgets that you spend on the purchase of protective equipment and software can only complicate our work, they can never completely protect you, but we, for our part, love complex tasks very much.

Now a few words on the case. We do not try to harm your processes, delete your data, destroy your business, at least until you yourself give us a reason. We never attack the same target twice. We always adhere to the agreements we have concluded. We do not bargain, never bargain, never bargain at all. The reason is simple - spending considerable time researching the obtained data, including financial indicators, we always know how much you are able to pay so that you do not have to delay salaries or cancel any projects. We know how long it will take for you. Don't try to deceive us. The final storage points for your data are disconnected from the Internet, so you won't be able to localize them and deny us access to them.

**Sofisticated. Evasive. Deep. Persistent.**

## Transparent Investigations, Negotiations and Payment Settlement Process

- CYPFER provides Clients a comprehensive upfront engagement plan and only proceed upon direction.
- Upon further analysis of the situation, Ransomware/Threat Actor Group and Client's situation, we:
  - Engage with Threat Actors to discover their demands and investigate what was locked and/or stolen;
  - Develop negotiations objectives and strategy with Clients, Incident Response Team and Breach Counsel;
  - Negotiate with the Threat Actors to try and reduce the ransom ask, buy time for recovery;
  - Manage the exchange and payment settlement process (MSB / KYC / AML / OFAC COMPLIANCE); and
  - Work to recover the decryption key(s) to unlock encrypted data and to recover, delete and suppress stolen data

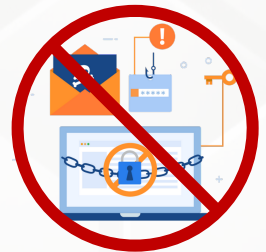


## LEARNINGS:

- **Threat Actors are innovating and changing the rules of engagement**
- **Increase in “Double Extortions”** – Threat Actors exfiltrate data prior to encryption and threaten to expose the data if ransom is not paid
  - *Due to increase in exfiltration events, increase in “breaches” requiring notification*
  - *Continued complex data mining & manual review necessary to determine notification obligations*
  - *Failure to notify might equal penalties and further regulatory action*
- **Rise in “Triple Extortions”** – DDOS and Repeat Attacks
- **Rise in Class Action Litigation**
- **Increase in complexity of Compliance, Regulatory requirements; reduction of notification timelines**

## TAKEAWAYS:

- Regularly test and validate backups; ensure Immutable
- Continue to be Cyber-Vigilante; conduct System Audits/Penn Tests / User Training
- HIDE Cyber-Insurance Policy + Incident Response Plan – Keep offline with Advisors
- Policy of Least Permissions; Conduct Data Audits & Security; Segregate Data
- Archive / Deletion of “No Man’s Land” data on Share Drives





# Cyber Incident Reporting

April Gougeon

*Fogler, Rubinoff LLP*



# Mandatory Breach Reporting Under PIPEDA

- Two main takeaways:
  1. Organizations may need to report data breaches to regulators and individuals in certain circumstances - organizations must determine whether they've hit the reporting threshold
  2. Organizations need to keep records of all breaches

# When to Report a Breach?

## Who to report to?

- Affected individuals
- The Office of the Privacy Commissioner of Canada (OPC)
- Orgs that can help mitigate or reduce risk of harm
- Reporting is “as soon as feasible” - there are certain notification requirements and reporting forms

## When do organizations need to report a data breach?

- When it is “reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual”
- Known as the “RROSH” standard

# WHAT IS SIGNIFICANT HARM?

Humiliation

Damage to  
reputation

Damage to  
relationships

Loss of  
professional  
opportunities

Loss of business  
opportunities

Loss of  
employment

Financial loss

Identity theft

Negative effects  
on credit record

Damage to  
property

Loss of property

Bodily harm

# When is there a REAL RISK of significant harm?

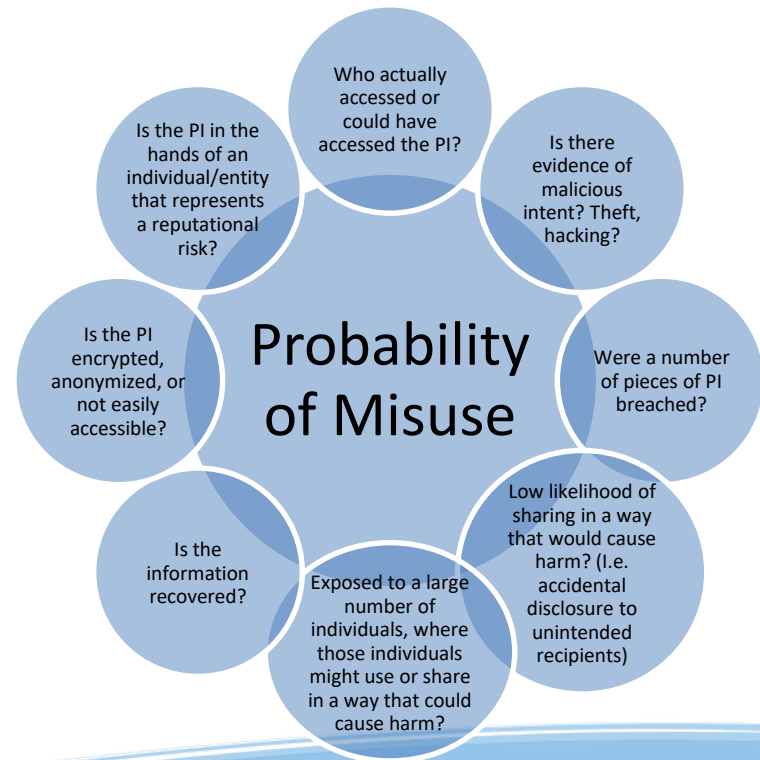
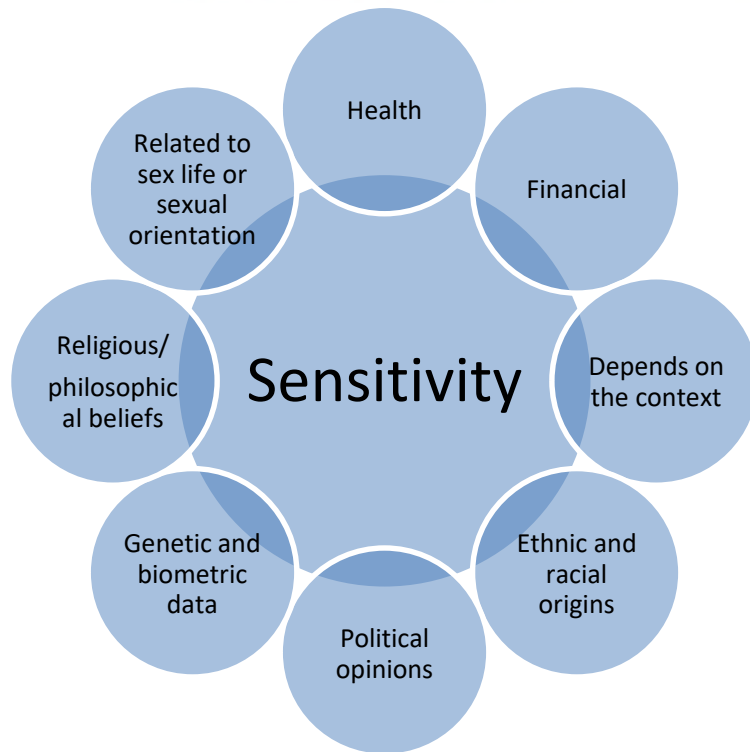
## Real risk of significant harm — factors

(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include

(a) the sensitivity of the personal information involved in the breach;

(b) the probability that the personal information has been, is being or will be misused; and

(c) any other prescribed factor.



\* Examples are not exhaustive – taken from [OPC Guidance](#) & previous findings

# Mandatory Breach Record Keeping Requirements

## Records

**10.3 (1)** An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control.

## Provision to Commissioner

**(2)** An organization shall, on request, provide the Commissioner with access to, or a copy of, a record.

- All breaches of security safeguards need to be recorded
  - OPC can request a copy of breach records
- Offense of up to \$100,000 to knowingly contravene a) not reporting a RROSH breach to the OPC and b) the mandatory record keeping requirement
- Bill C-27 - AMPs and offence provisions - fines of up to 5% of gross annual turnover or \$25 mil

# Takeaways

- Cyber incident- *not if but when and how*
- Cyber resilience
- Cyber insurance
- Ransomware
- Mandatory breach record-keeping and reporting
- Information security program
- Incident response plan
- As with a privacy management program, don't be overwhelmed: *start where you are*

# Recent Fogler Publications on Privacy and Cyber Law

- [2023 Chambers Guide to Privacy and Data Protection, Canada Chapter, April 2023](#)
- [The Litigation Consequences of Cyber Security Breaches, April 2023](#)
- [Why All Businesses Should Have Privacy Management Programs, March, 2023](#)
- [What's Ahead in 2023 for Privacy and Cyber Security Law, January 2023](#)

# Questions





# Thank You

Patrick Bourk  
Independent Consultant  
E: [patrickbourk0@gmail.com](mailto:patrickbourk0@gmail.com)  
P: 416.302.0886

April Gougeon  
Fogler, Rubinoff, LLP  
E: [agougeon@foglers.com](mailto:agougeon@foglers.com)  
P: 416.365.3744

Jason Kotler  
CYPFER Corp.  
E: [Jkotler@CYPER.com](mailto:Jkotler@CYPER.com)  
P: 647.497.7916

Bill Hearn  
Fogler, Rubinoff, LLP  
E: [bhearn@foglers.com](mailto:bhearn@foglers.com)  
P: 647.632.7893