Marsh

Cyber Claims Process and best practices to manage a Cyber incident

Marsh Canada Limited |
May 5, 2023
Declan Friel, Client Executive, Toronto |

1. Update on the Cyber Insurance Market
2. Brief discussion of the critical cyber coverages for organizations
3. Analysis of recent cyber claims and the critical steps clients need to take following a cyber attack
4. Importance of having an incident response plan
5. Discussion

Agenda

Cyber Market Overview

What's driving market changes?

Cyber Market Executive Summary

Stable market with evolving controls-based underwriting

- **Market Dynamics:** Rate increases are stabilizing; the underwriting process continues to go deep on cybersecurity controls. Coverage scrutiny remains.
- **Risk Environment:** Focus is on catastrophic risk, dynamic privacy regulations, and continued threat of ransomware.
- **Client preparation:** Demonstrate strong cybersecurity hygiene; align key stakeholders for a smoother process as well as decisions on cyber risk treatment.
- **Looking Forward:** We are optimistic about a stabilizing market. As carriers start to see sufficiently priced programs and improved cyber risk profiles, we expect minimal increases to become more common.

Cyber insurance

- Stand alone policies are generally divided into two types of coverage:
  - **Expense coverages** (known as First Party Coverage), which cover costs the business incurs in dealing with a breach.
  - **Third party coverage** – liability to others arising from the breach.
- Most of the cyber claims in the past few years have triggered the expense coverages rather than the liability coverages.

Cyber coverage parts

First party coverage with claims examples

	Description	Covered costs	Claims examples
First Party cover 1st Party Insurance coverage: direct loss and out of pocket expense incurred by insured			
Business income / extra expense	Interruption or suspension of computer systems due to a network security breach. Coverage may be added to include system failure and can extend to contingent businesses.	• Loss of Income • Costs in excess of normal operating expenses required to restore systems • Forensic expenses • Dependent business interruption	• Malware gets into the computerized factory controllers causing the line to cease operating. IT forensics must be performed to restore system operations. • During routine network patching duties, an IT employee accidentally crashes the critical IT infrastructure causing operational disruption when the IT systems are inaccessible. • A supplier you depend for delivery of your end service to customers suffers a cyber event that prevents them from delivering critical parts/services to you. You sustain a business income loss.
Data asset protection	Costs to restore, recreate, or replace electronic data and other digital / intangible assets that are corrupted or destroyed.	• Restoration of corrupted data • Vendor costs to recreate lost data	• After a cyber event that impairs your IT (or OT) network, costs are incurred to hire an IT forensics firm to determine whether the information can be restored. The data is recreated and restored.
Event management / breach response	Costs associated with a ransomware event, regardless of whether or not a ransom demand is paid.	• Forensics • Notification • Credit Monitoring • Call Center • Public Relations	• You suffer a data breach and incur costs ranging from IT forensic analysis, legal advice, costs to notify affected parties, credit monitoring for affected parties, and public relations assistance to help restore public trust in your firm.
Cyber extortion	Costs associated with a ransomware event, regardless of whether or not a ransom demand is paid.	• Negotiation & ransom payments • Forensics • Investigation	• Your employee unwittingly clicks a link in a phishing email resulting in ransomware locking out your ability to utilize business critical technology until a ransom demand is paid (or you're able to restore your network from back-ups).

Note: Additional 1st party coverage like Reputational Harm , Bricking and full supply chain contingent interruption may be available.

Cyber coverage parts

Third party coverage with claims examples

	Description	Covered costs	Claims examples
Third Party cover 3rd Party insurance coverage: defense and liability costs due to alleged harm caused to others by the insured.			
Privacy / network security liability	Failure to prevent unauthorized access / disclosure of personally identifiable or confidential information; Failure of system security to prevent or mitigate a computer attack.	• Liability and defense • Bank lawsuits • Consumer lawsuits	• A breach of your computer network leads to loss of sensitive customer information. Customers file suit against you for the failure to protect their private data. • Your network security fails to prevent a self-propagating malware from being transmitted from your network to a third party. You are sued for financial damages incurred by 3rd parties, like banks that incurred costs to re-issue bank cards to impacted individuals.
Privacy regulatory defense costs & PCI fines & penalties	Investigations and related fines or penalties assessed by Regulators or for violation of PCI data security standards	• Liability and defense • PCI / PHI / regulatory fines and penalties • Prep costs to testify before regulators	• A data breach leads to an investigation by a regulator such as the Office Of Civil Rights (OCR) for a breach of sensitive healthcare information leading to a HIPAA violation • A EU data protection authority investigates a potential GDPR violation. .
Media liability	Including but not limited to: libel, slander, product disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, etc.	• Liability and defense	• You are sued by a competitor when your CEO posts disparaging comments about the competitor on a social media site.

Cyber crime coverages

- **Social Engineering Fraud:** The intentional misleading of your organization by means of a dishonest statement or misrepresentation of a material that results in the voluntary transfer of funds by an employee to a third party. After ransomware the second most common form of cyber attack.

- **Electronic Theft and Computer Fraud:** This is the transfer, alteration or theft of data. It also includes fraudulent data entry into the system (e.g. electronically adding a vendor / invoice) with the intent to defraud that results in your money being transferred or lost.

- These coverages are typically sub limited ($250K) and many insurers are no longer insuring them.

- Full limits can be obtained under a Crime Policy.

Example of Canadian cyber claims that we have experienced

- **Retail Client –** hackers extracted customer credit card data from stores in the US. Total claim was approx. $3M including PCI fines and penalties.
- **Healthcare – Social Engineering Fraud** – cyber criminal (pretended to be from a major Canadian Bank) phoned the controller to inform that their bank account details had changed. This was followed by an email with the new account details. Controller wired 3 payments totalling $500K which was of course never recovered.
- **Healthcare – Ransomware attack** on Labour Day weekend. Shut down the entire system for a 4,000 employee organization. Eventually able to restore systems but Ministry of Health would not allow them to reconnect to their systems for 5 months until they were satisfied they were secure. Eventual loss $1.5M.
- **Not for Profit Charity** – hackers attacked their fund raising website in December. Website was shut down for several weeks during their maximum fund raising period. Revenue loss/ BI claim was settled at $1M.
- **Municipalities** – two separate attacks on this year, clients discovered an attempt to infiltrate data from one of it's servers. No PII was taken but forensics and legal costs were over $200K
- **Healthcare - Hospital** – hackers targeted a hospital with a ransomware attack forcing it to take systems offline and direct healthcare services to other facilities. Ultimately paid a ransom of approximately $1M.

Why are cyber claims different?

- A Cyber attack has the ability to shut down the entire network infrastructure in a municipality.
- It can have an immediate effect on the population in the municipality – i.e. cannot pay taxes, obtain information, apply for building permits etc.
- Healthcare – it can result in contacting thousands of patients that their PHI has been stolen or worse shut down hospitals as occurred in the UK during the WannaCry ransomware attack.
- Unlike most typical claims, senior management will be involved immediately and if you are not prepared, these can be very stressful situations.

Cyber incident response

- The initial steps taken to respond determine a successful, smoother outcome.
- Have a printed sheet of claims contact information as part of their incident response plan. Reason to print is that in the event of a cyber attack, you may not have access to your system.
- Our preference is to contact the insurer/broker and the breach coach (typically insurer will provide a panel of several law firms). Breach coach is a lawyer whose role is to manage the process of the claim.
- Ensure that insurers have provided permission before hiring vendors.
- Client should not use their own lawyer as breach coach. There are very few lawyers that have the experience and technical knowledge to deal with a complex cyber claim.

Claims process

Recommended best practices

Early on…

- **Consult with insurer prior** to hiring a forensic investigation firm directly.
  - Insurers have **preferred rates** with a panel of firms and will not pay the difference when client retains their own firm. They have very low tolerance on exceptions to this**.**
- Retain an approved **breach coach** who will hire forensics to investigate, repair and get the network back up.

- If **PHI/PII** has been compromised, breach coach may hire a company to notify affected individuals and set up a call center to deal with inquiries.
- Also, a **PR** firm may need to be retained for internal and external communication purposes.

Party	Role
Insurer	Coverage under policy
Coverage counsel	Insurer's lawyer advising on what's covered under the policy
Broker	Placed policy and business' advocate
Breach counsel	Advising business on management and response to breach
Forensics	Firm work (at direction of breach coach) on containment, restoration and forensics
Public relations	Firm working (at direction of breach coach) on communications.
Credit monitoring	Firm providing credit monitoring services
Mailing & Call center	Firm offering mailing and call center service (usually for large size breaches)
Others	May be considered by Insurer on a case-by-case basis

Claims process

Recommended best practices (cont.)

Breach coach…

- Ensures that the investigation is set up to maintain appropriate **legal privilege**.
- Is insured's representative with respect to engagement with regulators.
- directs the notification of potentially affected individuals and vets public statements with respect to the breach.

General comment: A cyber attack can create tremendous stress and tension within the organization and the breach coach can provide support during a time of crisis.

Ransom payment

- If there is a ransom demand, need to engage with the Insurer early to determine course (pay or not pay and why).
  - Insurer will want to understand why a payment is required (e.g., need for a decryptor, return/deletion of highly sensitive data, etc.).
- Ransom negotiations needs to be done via third-party vendor retained by breach coach.
- Prior to a ransom payment being made, need to obtain a "clear" sanctions check.

Cyber claim protocol: AIG

CYBER INCIDENT RESPONSE TIMELINE: WHAT TO DO IN THE EVENT OF A CYBER INCIDENT

STEP ONE
CYBER INCIDENT OCCURS

- An actual or reasonably suspected cyber incident takes place

STEP TWO:
CALL CYBER BREACH COACH AND OBTAIN GUIDANCE

- Call the AIG cyber breach hotline at:

  1-800-292-7345

- Contact Marsh cyber insurance broker

NOTE:

- Contacting the breach hotline **DOES NOT** satisfy the claim notification requirements under the AIG policy

STEP THREE:
PROVIDE FORMAL NOTICE

- Provide AIG with written notice of any claim or circumstances which may reasonably give rise to a claim **as soon as practicable** after any personnel in the office of any member of the control group first becomes aware of the Claim; or any first party event commences or, is discovered
- Notice can be provided to AIG via mail or email as follows:

By Mail:
AIG Insurance Company of Canada Canadian Head Office
120 Bremner Boulevard,
Suite 2200, Toronto, Ontario,
Canada M5J 0A8

mailto:
financialclaimsCA@aig.com

- In addition to providing notice to the insurer, report claims to Marsh via the following applicable zone email. Please note that reporting claims to Marsh does not constitute notice under the policy.

Toronto	Toronto.claims@marshcanadaclaims.com
Vancouver	Vancouver.claims@marshcanadaclaims.com
Calgary	Calgary.claims@marshcanadaclaims.com
Winnipeg	Winnipeg.claims@marshcanadaclaims.com
Montreal	Montreal.claims@marshcanadaclaims.com

STEP FOUR:
COORDINATE A RESPONSE

- After notification, AIG and the CyberEdge claims team will continue to collaborate with your firm throughout the investigation and response process

NOTE:

- Policyholders have the option of requesting their own firms prior to binding. All are subject to review and approval by AIG

VENDOR LIST:

LEGAL (Breach Coach)

Blakes
- Sunny Handa
- 1-833-564-0163
- breach@blakes.com

Norton Rose Fulbright
- Imran Ahmad
- 1 (416) 202-6708
- imran.ahmad@nortonrosefulbright.com

Bennett Jones
- Ruth Promislow
- promislowr@bennettjones.com
- Barry Reiter
- 416-777-6500
- reiterb@bennettjones.com

Langlois
- Jean-François De Rico
- 1 (418) 650-7923
- jean-francois.derico@langlois.ca

Osler Hoskins
- Adam Kardash
- 1 (416) 862-4703
- akardash@osler.com

FORENSICS

- Cytelligence
- Deloitte
- K2 Intelligence
- Kroll
- Kivu Consulting
- Mandiant
- KPMG

NOTIFICATION & MONITORING

- TransUnion

PUBLIC RELATIONS

- Levick
- Edelman
- Fleischmann Hillard Highroad

Summary

Recommendations

1 Know

Conduct a “**situational awareness**” exercise to specifically determine the most critical cyber risks that can adversely impact your business.

2 Plan

Have detailed **plans**, **protocols** and **playbooks** on how to effectively response to a cybersecurity incident.

Everyone in the organization should know what their role is and how it fits into the bigger picture.

3 Team

Have all **key vendors** lined up **before** an incident so as to ensure quick and methodical response.

4 Test

Regularly **test your cyber readiness** through simulations.

Establish a budget to conduct regular pen tests, security assessments, etc.

5 Constantly Review

Hackers are constantly changing tactics.

Make sure to **review and adjust** your preparation and response strategy regularly.

Questions?