

The Mining Industry Faces Cyber-Risk too!

May 29, 2019

Agenda

- Introduction
- World Economic Forum Global Risk Survey Results
- Cyber Risk in the Mining Industry
- Legislative Changes
- The Evolution of Cyber Risk
- The Wonderful World of Cyber Insurance
- The Marsh Approach to Cyber Insurance
- Questions

World Economic Forum Global Risk Report Results



The Global Risk Perception Survey draws on the views of the WEF's global community of multi-sector stakeholders

Respondents

- Number: 916
- Sectors:
 - Government
 - Business
 - International organisation
 - Academia
 - Non-governmental organisation
- Geographies (97 countries total)
 - North America
 - Europe
 - Middle East and North Africa
 - Sub-Saharan Africa
 - Eurasia
 - South Asia
 - East Asia and the Pacific
 - Latin America and the Caribbean

Survey questions

Assessment of global risks and trends

- *In 2019, do you think the risks associated with various current issues will increase or decrease compared to 2018?*
- *How likely is each risk to occur globally within the next 10 years, and what would be the estimated impact globally if the risk were to occur?*
- *What are the most strongly connected global risks?*
- *What are the most important trends that will shape global development in the next 10 years?*
- *What are the global risks most strongly driven by each of the trends identified above?*

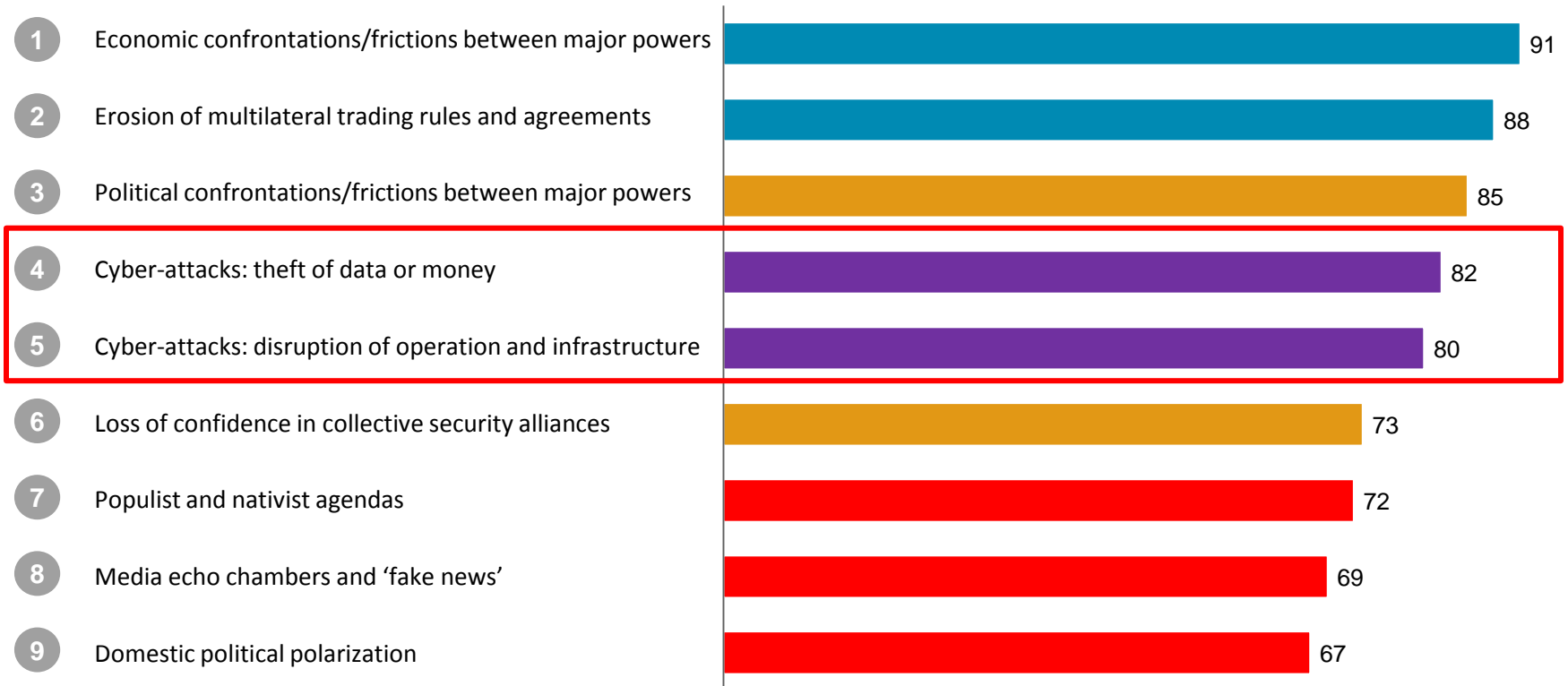
Note: Global Risk Perception Survey conducted in Q3 2018; The overall survey response total of 885 is taken from the total number of people who provided answers to section 2 of the survey

Source: World Economic Forum, *Global Risks Report 2019*

More than two thirds of respondents expect certain economic, geopolitical and technological risks to get worse in 2019

Global and regional risks expected to increase (either 'somewhat' or 'significantly'), all regions (2018–2019)

Risk (in order of % increase)



■ Economic ■ Environmental ■ Geopolitical ■ Societal ■ Technological

Note: Global Risk Perceptions Survey (916 worldwide responses to this question). Respondents were asked to predict how risks would change in 2018, in relation to seven key global issues
Source: World Economic Forum, *Global Risks Report 2019*

10-YEAR PERSPECTIVE ON GLOBAL RISKS: MULTI-SECTOR STAKEHOLDER SURVEY



In recent years, environmental, technological, and geopolitical threats have come to supplant economic risks as issues of greatest concern

Evolving Global Risk Landscape (2009–2019)

Top 5 Global Risks in terms of likelihood

■ Economic
 ■ Environmental
 ■ Geopolitical
 ■ Societal
 ■ Technological

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Asset price collapse	Asset price collapse	Storms and cyclones	Income disparity	Income disparity	Income disparity	Interstate conflict	Involuntary migration	Extreme weather	Extreme weather	Extreme weather
Slowing Chinese economy	Slowing Chinese economy	Flooding	Fiscal imbalances	Fiscal imbalances	Extreme weather	Extreme weather	Extreme weather	Involuntary migration	Natural catastrophes	Climate change mitigation and adaptation failure
Chronic disease	Chronic disease	Corruption	Greenhouse gas emissions	Greenhouse gas emissions	Unemployment/under-employment	National governance failures	Weak climate change response	Natural catastrophe	Cyberattacks	Natural catastrophes
Global governance gaps	Fiscal crises	Biodiversity loss	Cyber attacks	Water supply crises	Climate change	State collapse	Interstate conflict	Terrorist attack	Data fraud	Data fraud
Retrenchment from globalisation	Global governance gaps	Climate change	Water supply crises	Aging population	Cyberattacks	High unemployment	Natural catastrophes	Data fraud	Climate change adaptation failure	Cyberattacks

Top 5 Global Risks in terms of impact

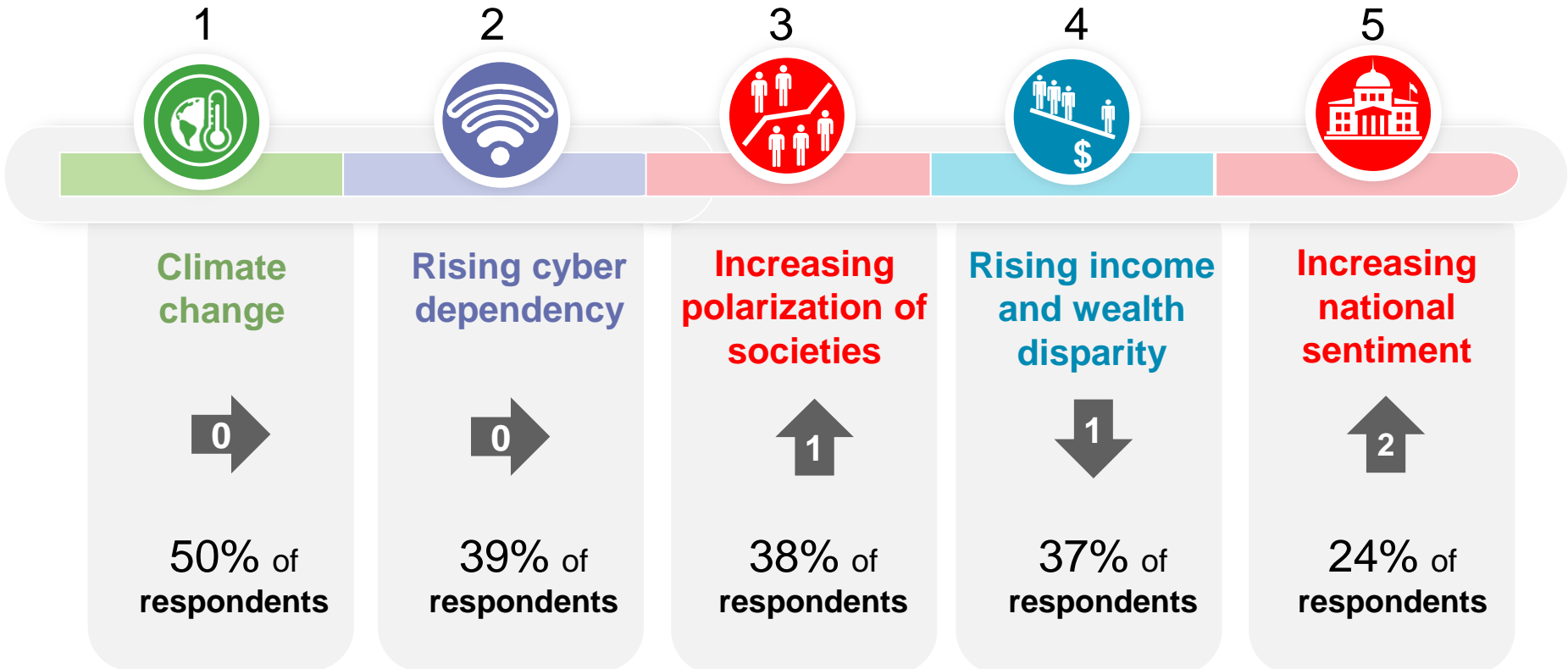
2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Asset price collapse	Asset price collapse	Fiscal crises	Systematic financial failure	Systematic financial failure	Fiscal crises	Water crises	Weak climate change response	WMDs	WMDs	WMDs
Retrenchment from globalisation	Retrenchment from globalisation	Climate change	Water supply crises	Water supply crises	Climate change	Infectious diseases	WMDs	Extreme weather	Extreme weather	Climate change mitigation and adaptation failure
Oil and gas price spike	Oil price spike	Geopolitical conflict	Food crises	Fiscal imbalances	Water crises	WMDs	Water crises	Natural catastrophes	Natural catastrophes	Extreme weather
Chronic disease	Chronic disease	Asset price collapse	Fiscal imbalances	WMDs	Unemployment/under-employment	Interstate conflict	Involuntary migration	Water crises	Climate change adaptation failure	Water crises
Fiscal crises	Fiscal crises	Extreme energy price volatility	Volatility in energy and agricultural prices	Weak climate change response	Critical ICT systems breakdown	Weak climate change response	Energy price shock	Weak climate change response	Water crises	Natural catastrophes

Source: World Economic Forum, *Global Risks Report 2019*

25 September 2019

Climate change, rising cyber dependency and increasing polarization of societies are expected to shape global development in the next 10 years

Top trends shaping global development in the next 10 years



↑ # Number of positions moved since 2017 # % Number of respondents selecting trend

■ Economic ■ Environmental ■ Geopolitical ■ Societal ■ Technological

Note: Global Risk Perceptions Survey (749 responses worldwide): Respondents were asked to identify three trends that will shape global development in the next 10 years.

Source: World Economic Forum, *Global Risks Report 2019*

CYBER RISK IN THE MINING INDUSTRY



Cyber Risk in the Mining Industry

RISKS

- ▶ **RELIANCE ON TECHNOLOGY:** Remote operations and automated equipment are connected through network infrastructure IT systems, increasing dependency on the internet, creating an access vulnerability
- ▶ **INDUSTRIAL CONTROL SYSTEMS:** Enables efficient production processes to reduce costs and increase output through highly integrated and automated industrial control systems
- ▶ **LOSS OF EXPLORATION DATA, MINING RIGHTS AND TITLE AND RESOURCE DEFINITION:** Exploration data includes valuable geological data that has taken a considerable time and investment to acquire, and is a core component of a mining company's value. Loss of this data – or loss of access to it – therefore has the potential to cause significant financial loss, including cost of reinstatement

CYBER EVENTS IMPACTING MINING COMPANIES

HACKTIVISM

An Australian mining company's website was defaced and access blocked as part of a campaign against the opening of a processing plant overseas

DATA BREACHES

The world's largest platinum producer experienced a security breach on their website resulting in leaked sensitive data online including PII, credentials and investor information.

INDUSTRIAL CONTROL ATTACKS

A large miner was hit by a cyber attack which was detected by accident when examining the reliability of a piece of equipment in its supply chain. The miner discovered software coding for the equipment had been changed with an unauthorized amendment

BUSINESS INTERRUPTION

The world's largest state-owned oil and gas supplier, experienced an attack intended to halt their supply of crude oil and gas which resulted in more than 30,000 hard drives and 2,000 servers being destroyed ultimately forcing I.T. systems to be disconnected from the internet for two weeks.

DEPENDENT BUSINESS INTERRUPTION

Attackers using the Marai botnet to target a DNS provider - the largest DDoS attack ever recorded, degrading cloud services and websites.

Cyber Risk in the Mining Industry: What should we be asking?

BUSINESS INTERRUPTION

- If an attacker were to disable a business application, a production facility or a critical vendor, how long would it take you to recover?
- How much would it cost you? How would you measure the cost?

EXPOSURE TO THIRD PARTIES

- How do you ensure your vendors' security standards are appropriate?
- What would you do if a key supplier or key customer had a data breach?
- How do you mitigate your exposure via contract?

BREACH RESPONSE

- What type and how much sensitive information are you responsible for?
- If you learned today that your network was compromised, what would you do?
- Do you have a dedicated business continuity team?
 - Do you test the plan in a tabletop exercise? When was the last time you did?
 - Is the risk management team part of the plan?
- Who would you call to investigate a data breach?
 - What law firm would you use? Do they have breach response experts?

STEP ONE CYBER INCIDENT OCCURS



STEP TWO: CALL CYBER BREACH COACH AND OBTAIN GUIDANCE



STEP THREE: COORDINATE A RESPONSE



Mining – Claims Examples

GoldCorp ⁽¹⁾

Incident Date: April 2016

Canadian gold-mining firm Goldcorp suffered a major data breach when hackers leaked 14.8GBs of data where employee PII and financial data was released.

Detour Gold Corp.⁽²⁾

Incident Date: April and May 2015

Canadian gold mining company, Detour Gold Corp. was hacked resulting in 100GBs+ worth of stolen data being released

AngloAmerican⁽³⁾

Incident Date: May 2013

The world's largest platinum producer AngloAmerican experienced a security breach on their website resulting in leaked sensitive data online including PII, credentials and investor information.

Nautilus Minerals and Marine Assets Corporation⁽⁴⁾

Incident Date: February 2015

Canada's Nautilus Minerals company and Dubai-based marine solutions company Marine Assets Corporation (MAC) were the victims of a cyber scam that resulted in Nautilus paying a \$10M deposit intended for MAC into an unknown bank account.

Potash Corporation⁽⁵⁾

Incident Dates: October and November 2011

In an attempt to gain information on bid information about BHP Billiton Ltd's ultimately unsuccessful takeover bid for Potash Corporation, hackers attacked the secure networks of several law firms and computers of the Government of Canada's Finance Department and Treasury Board.

Sources:

(1) <https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf>

(2) <https://www.theglobeandmail.com/report-on-business/industry-news/energy-and-resources/small-canadian-gold-firm-suffers-computer-hack/article25083416/>

(3) <https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf>

(4) http://www.miningweekly.com/article/nautilus-minerals-the-victim-of-a-cyber-scam-prepays-10m-to-wrong-account-2015-02-02/rep_id:3650 and <https://documents.trendmicro.com/assets/wp/wp-cyber-threats-to-the-mining-industry.pdf>

(5) <https://www.theglobeandmail.com/technology/tech-news/hackers-linked-to-china-sought-potash-deal-details-consultant/article534297/>

Business Interruption Claims Examples (Not Mining Specific)

Baku-Tbilisi-Ceyhan Pipeline (Owned by BP)⁽¹⁾

Incident Date: August 2008

Hackers were able to gain access to the operational controls of the Baku-Tbilisi-Ceyhan Pipeline where they were able to increase the pressure in the pipeline without setting off alarms resulting in an explosion. Beyond damaging the pipeline, the attack cost BP, the State Oil Fund of the Republic of Azerbaijan, and others millions of dollars, and also caused thousands of barrels of oil to spill close to a water aquifer.

Unnamed German Steel Mill⁽²⁾

Incident Date: 2014

A German Steel Mill was the victim of a spear-phishing attack which allowed attackers to gain access to their office network causing outages of production networks and entire production machines. The outages ultimately resulted in a blast furnace not being appropriately shut down causing significant damage to the plant.

Unnamed Oil Tanker⁽³⁾

Incident Date: 2003

Cyber attackers were able to gain access to the SCADA network of an oil tanker resulting in an 8 hour shutdown.

Saudi Arabian Oil Company (ARAMCO)⁽⁴⁾

Incident Date: August 2012

The world's largest state-owned oil and gas supplier, experienced an attack intended to halt their supply of crude oil and gas which resulted in more than 30,000 hard drives and 2,000 servers being destroyed ultimately forcing I.T. systems to be disconnected from the internet for two weeks.

Kyivoblenergo⁽⁵⁾

Incident Dates: 2014

Malware called BlackEnergy was used to gain access to Ukrainian Kyivoblenergo, a regional electricity distribution company to gain remote access to SCADA systems and remotely switch substations off, leaving 225,000 without electricity for three hours.

Sources:

- (1) <https://arstechnica.com/information-technology/2014/12/hack-said-to-cause-fiery-pipeline-blast-could-rewrite-history-of-cyberwar/>
- (2) <https://www.sentryo.net/cyberattack-on-a-german-steel-mill/>
- (3) http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf
- (4) <https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>
- (5) https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

LEGISLATIVE CHANGES



Digital Privacy Act (Amendments to PIPEDA): Mandatory Breach Notification for Canadian Organizations



WHAT IT IS:

- Regulation requiring organizations to manage and protect personal data
- A combination of statutory provisions in PIPEDA and a set of regulations which address matters such as breach reporting, the content of notices and breach record keeping
- Came into effect November 1, 2018



WHO IT APPLIES TO:

Organizations that:

- Operate in Canada; and
- Collect or store personal information



WHAT'S REQUIRED:

Mandatory Notification:

- Mandatory notification to affected individuals and to the Office of the Privacy Commissioner of Canada about data breaches where it is reasonable to believe that the breach creates a “real risk of significant harm” to the individual

Mandatory Record Keeping For All Breaches:

- Organizations are required to keep and maintain a record of every breach of safeguards involving personal information under their control. In addition, upon request, organizations must provide the Commissioner with such records. The Commissioner may publish information from such records if it would be in the public interest

Heightened Consent Requirement:

- A new requirement regarding consent states that consent is valid only if it is reasonable to expect that the affected individual would understand that “nature, purpose and consequences” of the collection, use or disclosure of personal information to which they are consenting.

General Data Protection Regulation (GDPR): A Paradigm Shift in Privacy Regulation



WHAT IT IS:

- Regulation requiring organizations that operate in the European Union (EU) or collect/ process personal data from EU residents to manage and protect personal data
- Strengthens privacy rights of individuals in EU: right to information, information rectification, erasure, data portability
- Came into effect May 25, 2018



WHO IT APPLIES TO:

Organizations that:

- Collect data from EU residents
- Processes data on EU residents



WHAT'S REQUIRED:



DATA PROTECTION

- Companies must take measures to ensure a level of security appropriate to the risk, such as encryption



PENALTIES

- Up to 20 million euro or 4% of revenue, whichever is greater



PRIVACY RIGHTS

- Provides a “right to erasure,” and other personal rights
- Requires the EU resident to affirmatively agree to data processing



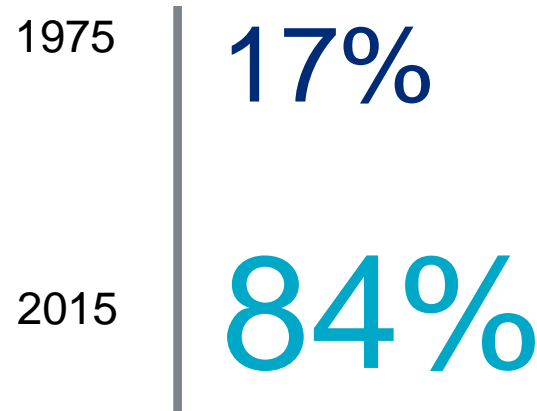
BREACH NOTIFICATION

- Notify competent data authority within 72 hours of becoming aware
- Notice to individuals “without undue delay” when the breach is likely to result in a high risk to the rights and freedoms of natural persons

THE EVOLUTION OF CYBER RISK



Percent of S&P 500 Companies' Market Value Tied To Intangible Assets ⁽¹⁾



(1) Intangible Asser Market Value Study, 2017, Ocean Tomo, LLC

Intangible assets are making up a greater proportion of company value

The insurance industry must task itself with producing products and broader solutions to transfer this risk. As the underlying risk changes, so must the risk industry

Overview of Cyber Risk and Cyber Insurance Coverage: Cost of a Data Breach

The Per Capita Cost Of Data Breach By Country Or Region

\$202 Canadian **Average**
Cost Of A Data Breach Per Capita

\$148 Global **Average Cost**
Of A Data Breach Per Capita

The Average Total Cost Of A Data Breach

\$4,740,000 Canadian **Total**
Average Cost Of A Data Breach

\$3,860,000 Global **Total**
Average Cost Of A Data Breach

The Average Number Of Breached Records By Country Or Region

22,275 Canadian **Average Number Of Breached Records**

24,615 Global **Average Number Of Breached Records**

Source: (1) "2018 Cost of Data Breach Study: Canada"; Ponemon Institute

197 Days

Mean Time To **Identify** A Data Breach

“Companies that identified a breach in less than 100 days **saved more than \$1,000,000** as compared to those that took more than 100 days.”

“Companies that **contained** a breach in less than 30 days **saved more than \$1,000,000** as compared to those that took more than 30 days.”

69 Days

Mean Time To **Contain** A Data Breach

“The **Faster** A Data Breach Can Be Identified And Contained, The **Lower** The Costs.”

Source: (1) “2018 Cost of Data Breach Study: Canada”; Ponemon Institute

Managing Cyber Risk: Prepare, Protect and Respond



Third party risk

Cyber risks posed by third-party suppliers, vendors and other impacts throughout the supply chain

Cyber risk management

A robust cyber risk management framework based on understanding and protecting core assets and optimizing recourses. This can include employee training, a data asset classification policy and segregation of duties and acceptable use policies.

Response plans

Response plans alongside robust cyber risk mitigation programs to ensure resilience, as well as operational and reputation recovery

Cyber insurance

The role of cyber insurance and how can it be an important component of a cyber risk management framework to support response and recovery

THE WONDERFUL WORLD OF CYBER INSURANCE








Overview of Cyber Risk and Cyber Insurance Coverage: Where Are The Gaps?

Insurers are responding to evolving cyber threats and costs by providing expanded standalone coverage options for organizations

TRADITIONAL INSURANCE

As organizations assess their cyber insurance coverage options, it is important to understand how cyber incidents may be covered in existing policies

	Property
	Casualty
	Crime
	Errors & omissions
	Kidnap and ransom

Management teams should work with insurance brokers to conduct a comprehensive gap analysis








Insurers are increasingly excluding cyber coverage under existing policies



This places a growing focus on the need and value of standalone policies

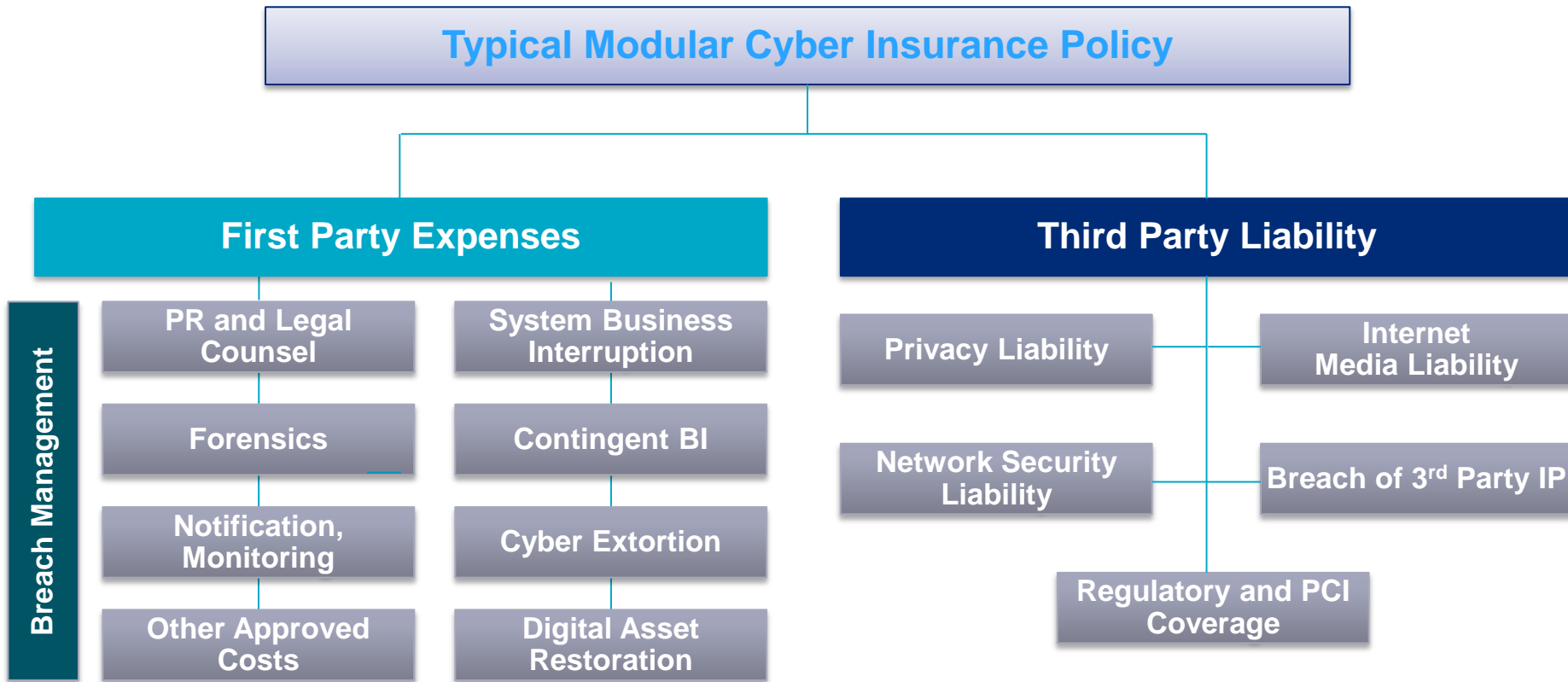
STANDALONE CYBER INSURANCE¹

Expanded coverage options are being provided for business interruption, extortion, and costs associated with response and recovery

	Data confidentiality
	Operational technology malfunction
	Network outage
	Inadvertent disruption of 3 rd party system
	Deletion or corruption of data
	Encryption of data
	Cyber Fraud/Theft

Management should undertake a detailed analysis of their digital assets, exposures and overall cyber risk appetite

1. Refer to the appendix for further details on cyber insurance policies
Source: MMC/ WCD; Cyber Risk Management – Response and Recovery (2018)



Provides coverage for the insured's own financial loss arising from a cyber event, often referred to as a network security or privacy event



Business Interruption (BI) / Extra Expense

Business interruption coverage reimburses the insured for loss of profits and increased operating costs the insured incurs due to an interruption or suspension of their computer system or business operations resulting from a network security event. Cyber business interruption is structured similarly to traditional business interruption coverage under a property insurance policy, however, the coverage trigger under a cyber policy is a non-physical peril as opposed to a physical peril such as fire, explosion, windstorm etc.

A broadened coverage trigger to the business interruption coverage section known as "system failure" can be added to respond to the loss of profits and increased operating costs the insured incurs as a result of any unintentional or unplanned outage or failure of a computer system.

Application of Coverage:

- *Malware infects the insured's computer network resulting in a network security event which causes the computer system to be inoperable for three weeks. As a result, the insured suffers loss of profits and incurs significant expenses to operate a work around.*



Contingent Business Interruption (CBI)

Contingent business interruption coverage reimburses the insured for loss of profits and increased operating costs resulting from an interruption of regular business activities caused by a network security event or system failure on the network of a third party firm the insured depends on to provide information technology (IT) services. Coverage can be broadened to include non IT providers.

Application of Coverage:

- *Malware infects the computer network resulting in a network security event of a third party's computer network that the insured relies on to provide business process services (such as payroll) causing the third party network to be inoperable for three months. As a result, the insured suffers loss of profits.*



Digital Asset Replacement

The digital asset replacement coverage reimburses the insured for expenses incurred to restore, recreate, or recollect data on the insured's computer system that is corrupted or destroyed as a result of a network security or privacy event.

Application of Coverage:

- *Wiper Malware erases data on all of the insured's computer network stations and as a result, the insured incurs significant costs to restore the data.*



Incident Response Costs / Event Management

Incident response coverage (sometimes referred to as the event management coverage section) reimburses the insured for expenses incurred in responding to a network security or privacy event including:

- Expenses incurred to hire a lawyer to obtain legal advice in relation to the network security or privacy event.
- Expenses incurred to hire a IT security forensics specialist to determine the cause of the privacy event.
- Expenses associated with having to notify individuals affected by an actual or suspected network security or privacy event.
- Expenses incurred to set up a call centre and credit monitoring services for individuals affected by the network security or privacy event.

The incident response coverage section is one of the most important aspects of coverage, as it provides the insured with access to the appropriate experts to assist in the management of a network security or privacy event.

Application of Coverage:

- *A network security event takes place on the insured's computer system and as a result, the insured must hire a computer forensics expert to determine how the network security event occurred.*



Cyber Extortion

Cyber extortion coverage reimburses the insured for extortion expenses incurred in responding to a network security or privacy event such as a threat actor threatening to expose or destroy an insured's data in an attempt to extort money, securities, tangible or intangible property from the insured.

Cyber extortion coverage reimburses the insured for costs including:

- Expenses to hire a qualified consultant to advise the insured on the appropriate response to a network security or privacy event including the negotiation and investigation to determine the cause.
- The cost of the ransom payment demanded (including cryptocurrencies).
- Expenses incurred to obtain bitcoin or cryptocurrency to be surrendered as payment to terminate a network security or privacy event.

Application of Coverage:

- *The insured's computer system is infected with ransomware that encrypts critical data causing a network security event. As a result, the insured is forced to pay an extortion demand to the threat actor to unlock the encryption..*

Cyber Risk: Common Insuring Agreements | Third Party Coverages

Provides coverage for liability actions and costs to defend a claim against the insured for financial loss caused to others arising out of a network security or privacy event



Privacy Liability

Privacy liability coverage indemnifies the insured for liability and defense costs arising out of the insured's failure to prevent unauthorized access, theft or disclosure of protected information in the insured's care custody or control. This coverage also extends to the failure of others whom the insured entrusted protected information.

Application of Coverage:

- *A lawsuit brought against the insured by customers who's private information (such as personal health information (PHI) and personally identifiable information (PII)) was compromised.*



Network Security Liability

Network security liability coverage indemnifies the insured for liability and defense costs arising out of the insured's failure to prevent unauthorized access, unauthorized use, physical theft, introduction of malicious code or denial of service attack upon the insured's or a third parties' computer system.

Application of Coverage:

- *A lawsuit against the insured brought by a trading partner who suffered economic damage because the insured failed to protect their computer network from a network security or privacy event.*
- *A lawsuit against the insured brought by a trading partner alleging that malware entered their system from a connection with the insured's computer networks.*



Media Liability

Media liability coverage indemnifies the insured for liability and defense costs incurred as a result of dissemination or publishing of media content on its website that results in the libel, slander, plagiarism, piracy, misappropriation, infringement, in the insured's creation or dissemination of media content.

Application of Coverage:

- *A lawsuit brought against the insured by their competitor alleging defamation and slander arising from statements made on the insured's website.*



Privacy Regulatory Defense Costs

Privacy regulatory defense costs coverage indemnifies the insured for defense costs, fines or penalties that a regulatory body assessed against the insured as a result of suffering a network security or privacy event.

Application of Coverage:

- *A regulatory investigation of the insured by the provincial or federal Office of the Privacy Commissioner (OPC) following a network security or privacy event.*

It is important to note that first party expense coverage is generally written on a Discovery basis, while third party liability coverage is written on a Claims Made basis

Cyber Risk: Common Exclusions

Some Common Exclusions in a Cyber Policy

Exclusion	Losses Not Covered	Applicable Exceptions and Considerations
Power Outage & Infrastructure Exclusions	<ul style="list-style-type: none"> Excludes coverage arising from any mechanical or electrical failures of infrastructure including any electrical power interruption, surge, brownout or blackout 	<ul style="list-style-type: none"> An exception to the exclusion applies for a mechanical or electrical failure under the insured's direct operational control as a result of a network security event
Prior Knowledge Exclusion	<ul style="list-style-type: none"> Excludes coverage for claims where a control group member (i.e. C-Suite) was aware of, or could of reasonably foreseen, that such incident which occurred prior to policy inception would lead to a claim during the policy period. 	<ul style="list-style-type: none"> Prior knowledge of incidents which would give rise to a claim under the policy (not system vulnerabilities) must be disclosed up front as insurance policies are good faith contracts
Conduct Exclusion	<ul style="list-style-type: none"> Excludes coverage for any fraudulent, dishonest, criminal, malicious or intentional acts committed by certain insureds, i.e. the Control Group (e.g. CEO, CFO, CIO, CISO, etc.) 	<ul style="list-style-type: none"> Cannot insure criminal activity or behavior Coverage for defense costs to defend claims against the insured applies until a final non-appealable adjudication is made Coverage for the entity applies in the event a "rogue" employee's intentional conduct results in a network security or privacy event
Bodily Injury/Property Damage Exclusion	<ul style="list-style-type: none"> Excludes coverage for bodily injury and property damage 	<ul style="list-style-type: none"> An exception to the bodily injury exclusion applies to mental anguish and emotional distress resulting from a privacy event Coverage for bodily injury and/or property damage can be negotiated under a cyber policy, where appropriate
War Exclusion	<ul style="list-style-type: none"> Excludes coverage for war as it is an uninsurable risk 	<ul style="list-style-type: none"> An exception to the war exclusion applies to cyber terrorism
Insured vs. Insured Exclusion	<ul style="list-style-type: none"> Excludes coverage for claims made by or on behalf of, any insured against any other insured 	<ul style="list-style-type: none"> Generally, an insured cannot sue another insured under the policy and profit from insurance proceeds An exception to this exclusion applies for claims made by an insured person in their capacity as the insured's customer or employee as a result of a privacy event
Contractual Liability (Breach of Contract) Exclusion	<ul style="list-style-type: none"> Excludes coverage for contractual liability or any breach of contract, warranty, guarantee or promise, including any liability of others assumed by the insured 	<ul style="list-style-type: none"> An exception to the exclusion applies for contractual liability claims as it relates to an obligation to comply with payment card industry security standards under a contract, and the protection of confidential information

Cyber Crime Coverages: Social Engineering Fraud

Cyber Crime Coverages Available Under a Cyber Policy

Social Engineering Fraud

Provides coverage to the insured for loss of funds that are voluntarily transferred to an unintended third party by means of “fraudulent instructions” from a third party by committing any phishing or social engineering attack against an employee or senior executive officer.

The key distinction between social engineering versus funds transfer fraud coverage is that social engineering coverage involves a good faith/voluntary transfer, whereas funds transfer fraud coverage applies to involuntary transfers of funds, usually by means of hacking.

*Limits applicable to social engineering fraud under a cyber policy may be less than the limits offered by an insurer under a crime policy

Example

CFO at a mining company receives an email appearing to be from the company’s treasurer, requesting transfer of \$500K from X Bank to Y Bank to cover an outstanding check. As a result, the CFO wire transfers \$500K to Y Bank and instead, the \$500K ends up in the bank account of a threat actor who impersonated the treasurer.

Funds Transfer Fraud

Provides coverage to the insured due to a third party committing any:

- Unauthorized electronic transfer of funds from their bank
- Theft of money from their bank by electronic means
- Theft of money from the insured’s corporate credit card by electronic means

Example

A hacker infiltrates a brokerage firm’s computer system, using it to electronically transfer \$5M to their bank in the Caribbean. By the time the brokerage firm realizes what has happened, the hacker has withdrawn the funds from their bank and escaped with the \$5M in cash.

Theft of Funds Held In Escrow / In Trust

*Please note that this coverage is not currently offered by all insurers

Provides coverage to the insured as a direct result of the insured having to reimburse any third party for theft, committed by a fraudulent third party by electronic means, of their money or other financial assets from a bank account held by the insured on their behalf.

Example

A law firm’s computer system experienced a breach resulting in the fraudulent transfer of \$500K from their account that they held in escrow on behalf of one of their largest clients.

Theft of Personal Funds

*Please note that this coverage is not currently offered by all insurers

Provides coverage to reimburse a senior executive officer for personal financial loss as a result of a third party compromising the insured’s network security which results in:

- Theft of money from a personal bank account of a senior executive
- Identity theft of a senior executive as a result of a privacy breach suffered by the insured

Example

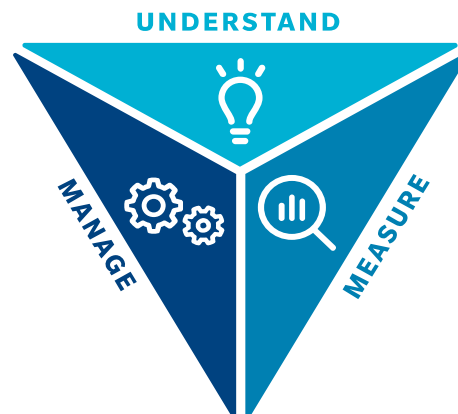
A senior executive officer’s bank account was fraudulently accessed by a third party as a result of their company’s network security being compromised. As a result, the senior executive suffered a loss of \$50K from their personal bank account which was covered by the cyber policy.

THE MARSH APPROACH



Key Takeaways: Marsh's Approach to Cyber Risk Management

- **UNDERSTAND** your security and privacy risk management policies and procedures are the most important and first line of defense
- **MEASURE** and quantify the security and privacy exposures that are most relevant to your organization
- Determine which security and privacy exposures/risks your organization is comfortable accepting and which exposures/risks your organization may consider transferring through insurance
- Analyze your organization's current portfolio of insurance products to see if you already have some from of security and privacy coverage
- If, after considering the items above, your organization feels that cyber insurance would be helpful as a second line of defense in **MANAGING** your cyber risk, reach out to your broker to discuss further





For further information, please contact your local Marsh office
or visit our web site at: marsh.com

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are intended solely for the entity identified as the recipient herein (“you”). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

Copyright © 2019 Marsh Canada Limited and its licensors. All rights reserved. www.marsh.ca | www.marsh.com 170501vg