HUB

Cyber Security:

Legal Update, Risk Management and Insurance Perspective

Association of Managers in Canadian College University and Student Centres

National Conference

Calgary – May 28th, 2019

Patrick Bourk, HUB International Insurance Brokers

Principal, National Cyber Practice Leader

Office: 416.619.8097 | Mobile: 416.302.0886 | patrick.bourk@hubinternational.com

CYBER RISK – IT IS EVERYWHERE

- **Not a day goes by without another story …**

April 2019: According to the NetDiligence Cyber Claims Study 2018 (released April 2019) which analyzes claims information provided by insurance company participants, the range of cost per record lost between 2013-2017 was between $0.01 and $1.6M! The average cost per lost record was $5,233 and the median was $43. The average total breach cost in 2017 was $603,700.

CrowdStrike 2019 Global Threat Report: CrowdStrike's Falcon platform deploys endpoint agents on customer machines in over 176 countries and captured more than 240 billion events every 24 hours in 2018. In 2017 that number was 90.1 billion. Events are happening all the time!

- **Details of damage:**

N **No Business Sector is too small:** NetDiligence Cyber Claims Study 2018 noted that of the 1201 claims reviewed from 2013-2017 by business sector, Professional Service firms had the highest number (20%) followed by Healthcare (17%) , Financial Services (12%) and Retail (12%). CFC Underwriting reports that 90% of claims affect businesses with less than $50M in revenues. For smaller sized organizations the impact of a breach can often be far more devastating.

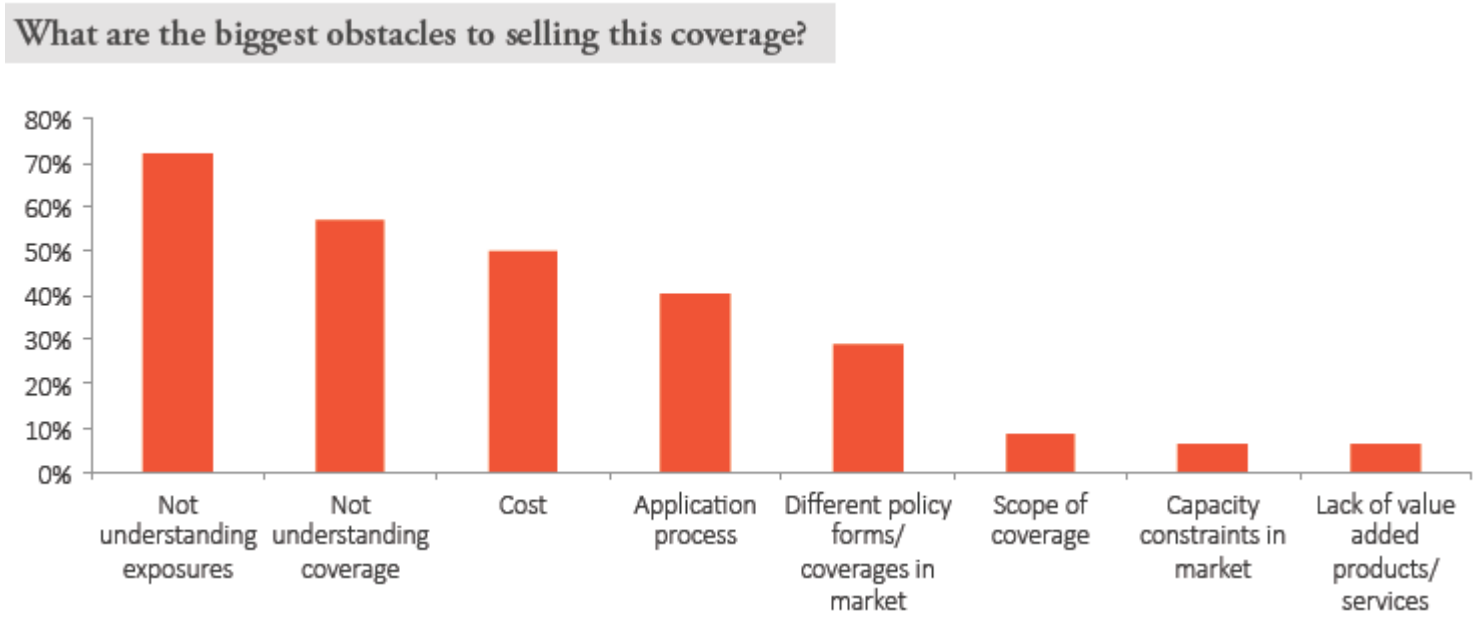
N **Knock-on Effect:** The proliferation of ransomware attacks can lockdown systems such that business cannot be conducted which in turn leads to the greater exposure of business interruption loss.

N **City of Atlanta:** The City entered into emergency contracts worth $2.7 million to help restore the city's computer network in the days following their cyber attack of March 22nd, 2018. Despite hiring outside security and crisis management consultants departments remained hobbled for weeks. The ransomware demand was for $52,000.

CYBER RISK – PERCEPTIONS & REALITIES

THE CLIENT

- **It's an "IT Thing" and so Cyber must be an untranslatable kind of coverage that can't be understood and is therefore TERRIFYING!**
  - It is NOT just an IT matter and the coverage, although very customizable and nuanced, is capable of translation!
- **Board Members and Senior Management are now interested and are asking questions**
  - As the topic "du jour" management teams have an obligation to educate themselves. As for buying it ….



Source: Advisen Survey of Cyber Insurance Market Trends 2016

CYBER RISK – PERCEPTIONS & REALITIES

- **5 REASONS CLIENTS DON'T BUY CYBER LIABILITY INSURANCE**
  - Our Director of IT assures us that our systems are 100% secure
  - We don't hold any health information or sensitive data and therefore our exposure is minimal
  - Our firm is too small to be considered a target (we are not Target, or Home Depot or Equifax)
  - We outsource everything to 3rd parties and/or rely on others for protecting data and therefore carry none of the liabilities
  - We would rather invest in our technology systems than insurance

NETWORK SECURITY & PRIVACY LIABILITY INSURANCE

What has recent case law highlighted?

- **Unprecedented litigation activity and class certifications**
  - *Jones v. Tsige* – The tort of "intrusion upon seclusion" – turned the tap from trickle to flood
  - Plaintiffs are finding creative damage mechanisms (*Evans v. Scotia*) and are testing them in the class action forum
- **Breach incidents giving rise to collateral damage**
  - Directors, officers and management teams are now being held to account
  - "Business to business" claims on the rise – consumers as victims seek compensation from banks who bring suit against the original corporate victim
- **Legislative landscape – change has arrived**
  - The courts have been creating the framework for response requirements rather than the legislation but … *Bill S-4 passed into law June 18th, 2015, Regulations were published April 18th, 2018 and …*
    - ***NOVEMBER 1st, 2018*** – Mandatory notice and reporting where there is a "real risk of significant harm to the individual"
    - Mandatory record keeping for ALL breaches – Expect the 'breach log' to be a target

NETWORK SECURITY & PRIVACY LIABILITY INSURANCE

The "three pillars" of breach exposure

- **Ransomware/Cyber Extortion**
  - Significant increase in reported claims since 2016 and affecting every industry sector
  - Since 2016 a noticeable increase in targeted ransomware variants – identifying specific businesses and their likelihood of making payment
- **External intrusions targeting specific confidential information**
  - Organizations with networks of affiliated organizations make for prime targets since network integration is rare and systems are often inconsistently monitored and/or updated. If more than 5-10 linked institutions, then malware is often customized given the size of opportunity for hackers
  - Foundations typically hold extremely valuable non-PII information – sensitive financial and donor information
- **Phishing attacks**
  - Theft of money but equally concerning are attacks that deny access to corporate network systems
  - Seemingly innocuous businesses can be "locked down" for days causing huge delays and resulting in significant business interruption/extra expense losses

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)**
  - **Professional Liability**
  - **Directors' & Officers' 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

NETWORK SECURITY & PRIVACY LIABILITY INSURANCE

Third Party Liability

- **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 trade mark, 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:*** Covers expenses to retain "breach coach" lawyer to advise and guide the process of managing a breach incident
  - ✓ ***Forensic Expenses:*** Covers expenses to retain third party computer forensics services to determine the scope of a failure of Network Security
  - ✓ ***Notification Expenses:*** Covers expenses to notify customers whose sensitive personal information has been breached.
  - ✓ ***Crisis Management Expenses:*** Covers expenses to obtain legal, public relations or crisis management services to restore the company's reputation.
  - ✓ ***Credit Monitoring Expenses:*** Covers the cost of credit monitoring, credit freezing or fraud alert service expenses for breaches of true identity data.
- **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.

NETWORK SECURITY & PRIVACY LIABILITY INSURANCE

There are nuances to cyber risks that are coverage-specific

- **Social Engineering and Social Engineering Fraud:**
  - ✓ The art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques
  - ✓ Social Engineering Fraud coverage as a coverage enhancement that refers to "phishing" attacks that involve MONEY!
    - Cyberliability insurance = protection of DATA
    - Crime insurance = protection of MONEY
- **Lessons learned:**
  - ✓ **REVIEW YOUR COVERAGE!**
    - Is your crime coverage enhanced with social engineering fraud coverage?
    - If not, can your cyberliability insurer provide social engineering fraud coverage?
    - Distinguish between 'computer funds transfer' coverage and 'social engineering fraud' coverage
    - Are your limits and deductibles appropriate in order take advantage of the coverage?
    - Watch for subjectivities, i.e. voice confirmation in advance of transfer

NETWORK SECURITY & PRIVACY LIABILITY INSURANCE

What do underwriters look for in their risk assessment?

- **Your Information:**
  - ✓ Type of information an organization is responsible for and the number of records
  - ✓ All about Planning: Incident Response Plans, Disaster Recovery Plans, Business Continuity Plans, Responsive and protective IT security procedures
- **Your people**
  - ✓ Controls in place to set expectations for employees as far as their awareness and responsibility for dealing with sensitive information
  - ✓ Governance: How engaged is the executive management and leadership? Network Security and privacy issues are no longer an IT issue. They are a governance issue
- **Information Security**
  - ✓ Do you understand what all kinds of data you control and why?
  - ✓ Due diligence internally and with outside service providers for data protection
  - ✓ Safeguards for personally identifiable information, especially healthcare and credit cards
- **Your Vendors**
  - ✓ Do you ensure 3rd Party providers are meeting both regulatory and contractual obligations related to information security

PRESENTER

Patrick Bourk

Principal, National Cyber Practice Leader, HUB International Insurance Brokers

As an insurance coverage expert, Patrick provides technical expertise in the analysis, placement and negotiation of various management risk insurance coverages including professional liability, crime and directors' & officers' liability insurance but with an emphasis on cyber liability insurance. In addition to negotiating terms and placing coverage Patrick's cyber liability insurance practice also includes advising clients on how best to align breach response planning with insurance and risk mitigation solutions.

A graduate of Windsor Law School in 1997, Patrick began his career as an associate lawyer with a commercial litigation focus. After moving to Toronto to work for a national law firm, he joined the Legal and Claims Department of London Guarantee Insurance Company, specializing in directors' and officers' coverage, technology and miscellaneous professional liability, employment practice liability, and fidelity coverage. Prior to joining HUB, Patrick was a Claims Lawyer for the Financial and Professional Services Group at Travelers Insurance Company and its predecessor companies.

Patrick is a licensed lawyer and Member of the Law Society of Upper Canada, a Member of International Association of Privacy Professionals (IAPP), and has been a part-time instructor at both Sheridan College and Humber College, where he has taught courses on law for business managers. He has authored several publications in the areas of specialty insurance coverage and cyber liability and has been a frequent speaker at conferences and symposiums focusing on cyber liability insurance both in Canada and the U.S. Patrick also holds a Cyber COPE Insurance Certificate designation after completing an executive certification in Cybersecurity through Heinz College of Carnegie Mellon University.

HUB

QUESTIONS ?