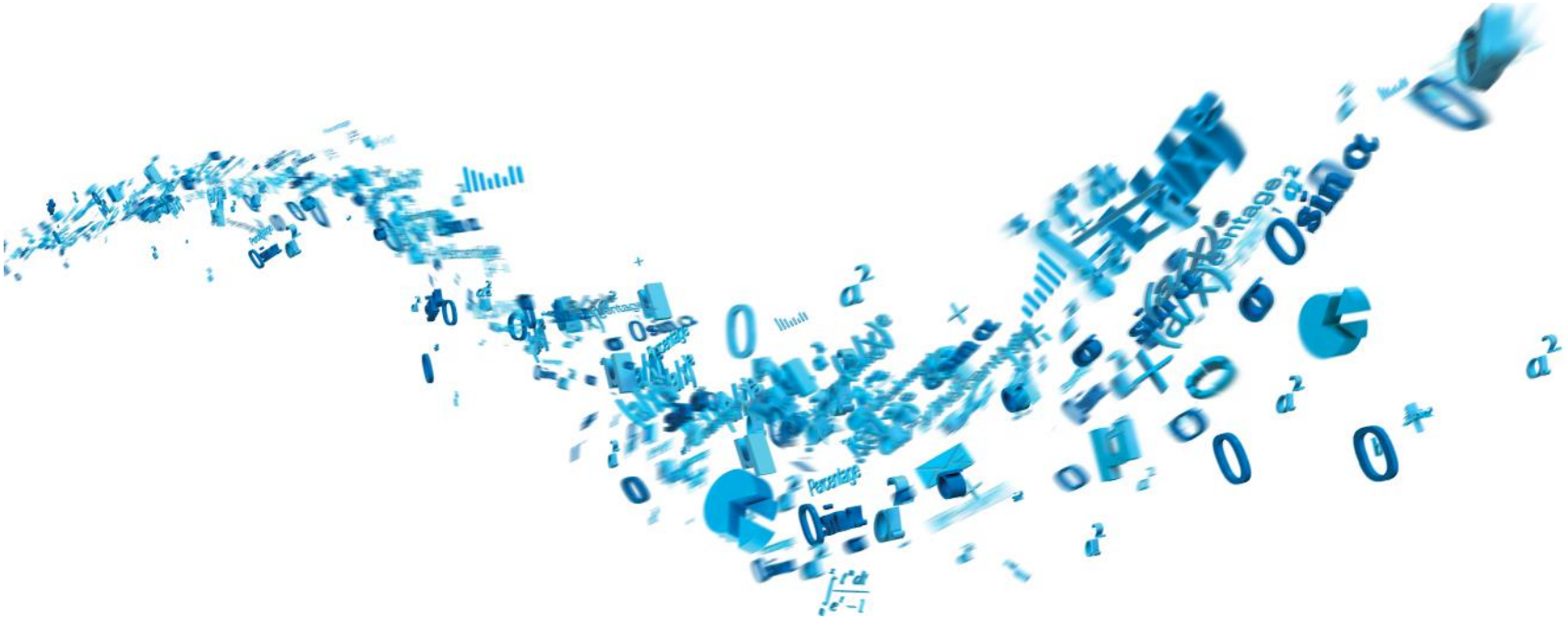


Davidson & Company
CFO Series XIII: Cybersecurity
Network, Data Security & Privacy Liability Insurance

Prepared by Aon Risk Solutions
Aon Cyber and Privacy Practice (ACAPP)

Empower Results®

‘Cyber’ Risk Factors

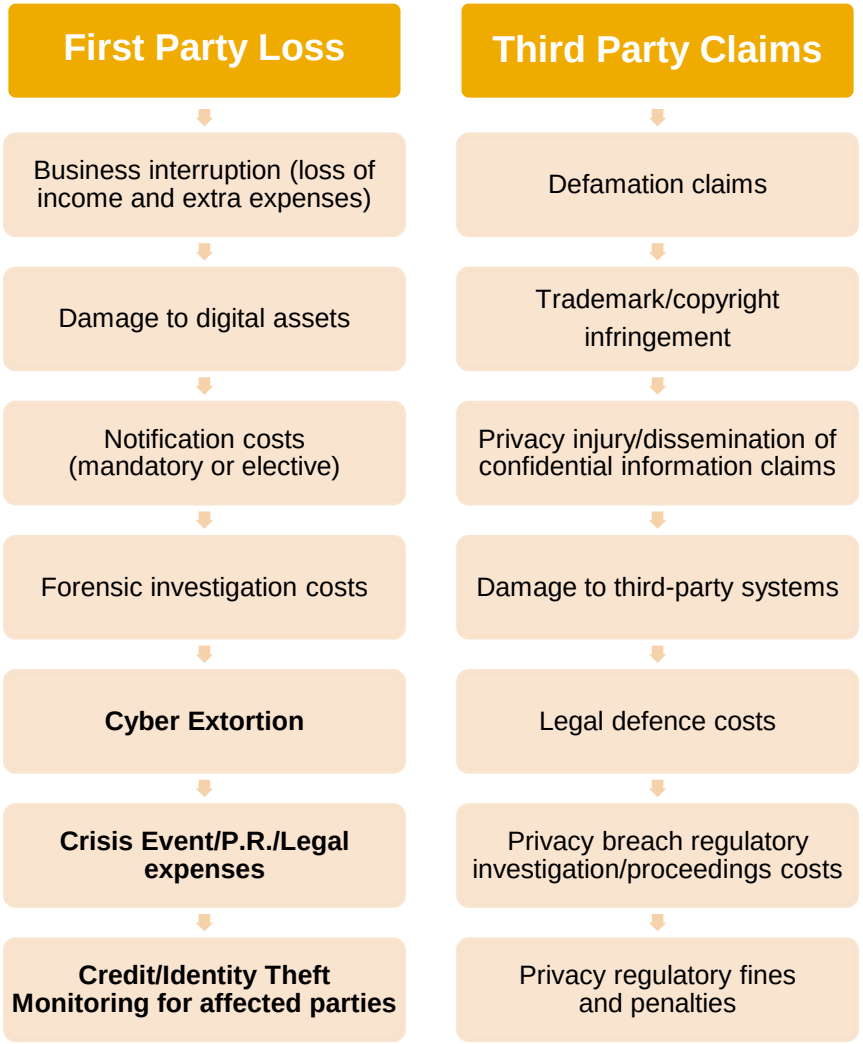
- A high degree of dependency on electronic processes and computer networks
- Large volumes of private personal and/or confidential corporate information collected, maintained, disseminated or stored (clients, employees, business partners, contractors)
- Potential vulnerability to reputational harm
- Employees; potential for human error and/or malicious acts
- Increasing business-related online and social media activity
- Exposure to vicarious liability relating to third party service providers, business partners, vendors
- Subject to regulatory statutes/oversight in Canada, U.S. and other jurisdictions
- PCI (Plastic Card Industry) fines and assessments
- Potential for cyber-related Property & Business Interruption loss
- Vulnerability to cyber-extortion
- Critical Infrastructure / Industrial Control Systems potentially at risk from a cyber-event

To Insure, or to Self-Insure Cyber Risk?

There are many factors to consider in answering this question, among them:

- Your organization's level of risk tolerance/appetite for retaining risk
- The extent of in-house resources available to establish and execute Incident Response Plans (Risk Management, Legal, Compliance, Information Security, I.T.)
- The volume of private records your organization holds, and the potential cost of notification to and credit/identity theft monitoring services for affected customers, employees or business partners
- Your industry's attractiveness as a 'target'
- The extent to which your organization might be exposed to liability or loss arising out of the use of third-party service providers
- Your organization's potential exposure to infrastructure damage / business interruption losses arising from a cyber-event (this is an 'evolving' area where insurance response is concerned)

What Does a “Cyber Risk” Policy Look Like?



Why Aren't 'Traditional' Insurance Policies Enough?

- Property insurance policies cover "tangible property" – which data isn't
- Business Interruption cover responds only when insured property has been physically damaged by an insured peril
- General liability policies speak to bodily injury/property damage risk, and do not contemplate claims brought by employees
- Crime/Employee Dishonesty policies have no "liability" component
- D&O Liability policies ***might*** partially respond depending on circumstance, but much depends on the nature and target of the allegations
- Professional Liability policies ***might*** partially respond, but will only address third-party loss arising from allegations of professional negligence
- Conventional insurance policies contain terrorism exclusions
- K&R policies don't provide fulsome (or any) coverage for cyber-extortion
- None of these policies address first-party expenses; forensic investigation costs, notification/credit monitoring costs, legal/crisis response/public relations expenses, privacy regulatory investigation costs/penalties, cyber-related business interruption, damage to digital assets

Privacy Risk Exposures

Customer/Employee Data

- Credit/debit card information
- Bank account information
- Credit reports
- Employee medical records
- Social Insurance numbers
- Personnel files
- Student transcripts
- Payroll Information
- Motor vehicle abstracts
- Mortgage insurance records
- Employment contracts

Corporate Information

- Client/investor lists
- Compliance reports and data
- Litigation records
- Merger/acquisition plans
- Marketing/advertising plans
- Corporate contracts
- New product development plans
- Security assessments
- Network architecture details
- Business continuity plans
- Restructuring/hiring/lay-off plans

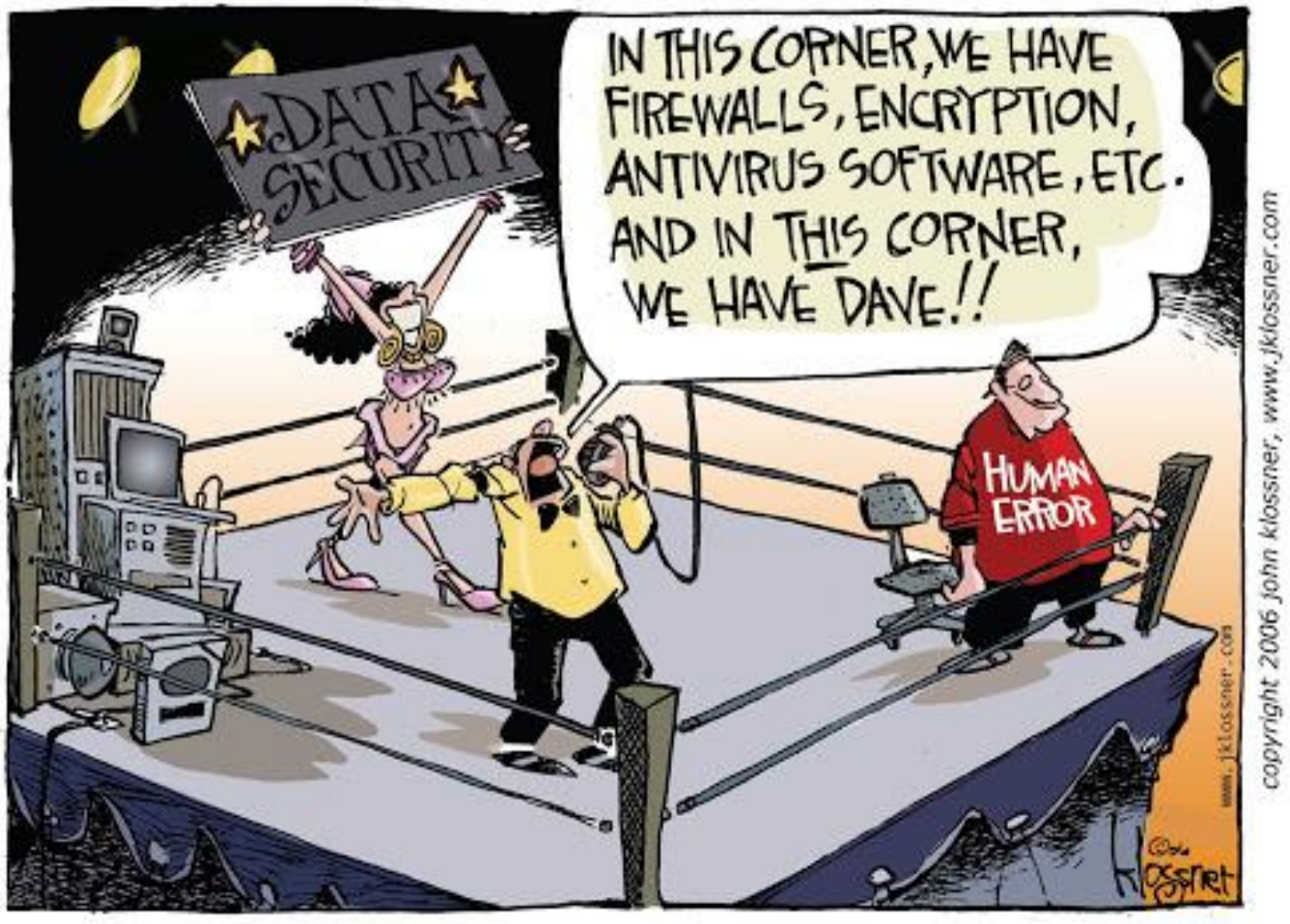
Can’t We ‘Transfer’ Cyber-risk to External Service Providers?

- Third-party service providers (e.g. payment processors, cloud storage providers, I.T. consulting firms) typically contractually limit their liability, and they rarely indemnify their customers; this can result in significant exposure to their customer in terms of potential financial and reputational loss
- In limited circumstances where contractual indemnities are forthcoming, the service provider’s ability to honour the indemnity should be assessed; many do not carry Professional Liability/Cyber-risk insurance themselves, and/or are unlikely to have the financial resources to fulfill their indemnity obligations
- You can contractually request that service providers carry Technology Errors & Omissions/Cyber-risk coverage, but their policy(s) are highly unlikely to directly address your organization’s legal costs or third-party/first-party damages
- Where protection of brand reputation is concerned, reliance on a third party contractor’s resources and decisions would be undesirable for most organizations

Won't Our I.T./Information Security Controls Protect Us?

- Not all Privacy/Data and Media/Content risk exposures relate to hacking or electronic exploits
- The majority of privacy breach and network security incidents are attributable to employees, not to outsiders
- Human error is a huge risk; lost paper files/laptops/USB sticks, misdirected emails, falling for phishing attempts
- Loss arising from the actions of rogue employees (whether acting alone or in collusion with outsiders) is a significant risk exposure, particularly if that employee(s) is familiar with your organization's systems and controls
- The bad guys on the outside keep getting smarter, particularly where cyber-extortion is concerned

Dave


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
JKlossner
copyright 2006 John klossner, www.jklossner.com

Cyber-risk Coverage Checklist

Cyber-risk policy offerings and wordings vary greatly from insurer to insurer. A few things to look for when reviewing your existing policy or 'shopping' for coverage:

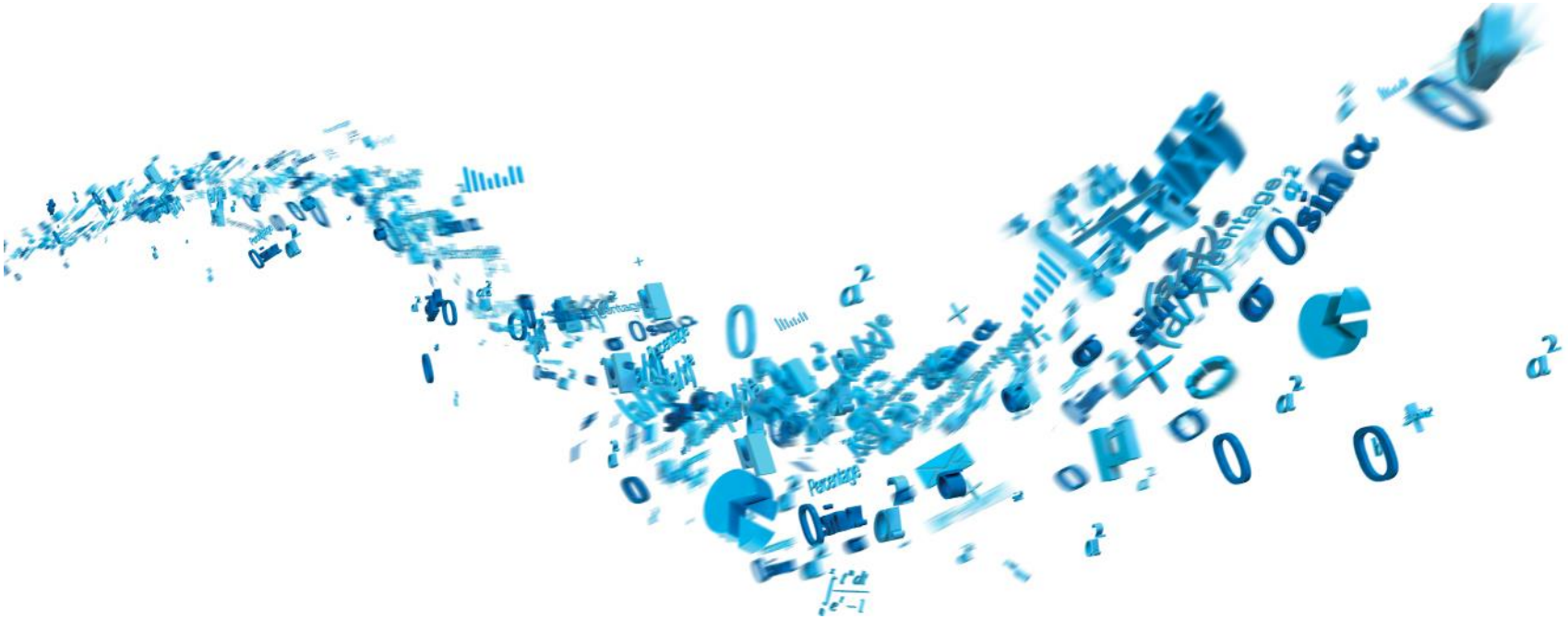
- Does the 'Crisis Response' coverage module response to voluntary notification to affected parties, or only to notification mandated by legislation/statute?
- Is there a Retroactive Date on your policy? This can be problematic in the context of a persistent threat that was undetected at the time of binding cover.
- Are there sub-limits associated with certain sections of your policy? With some isolated exceptions, full policy limits should be provided across all insuring agreements.
- Does the Media/Content Injury coverage module restrict cover to 'website' content only, or has it been expanded to include all modes of information dissemination – including social media?
- Is there clear, affirmative cover for vicarious liability arising from your organization's use of external service providers?
- Does the policy clearly detail incident response reporting coordinates?

For More Information…

Sandy Treleaven
Vice President
Aon Risk Solutions
Financial Institutions & Cyber Practice
t +1.604.443.3365
sandy.treleaven@aon.ca
https://www.aoncyberdiagnostic.com

Andrew Russell
Senior Vice President
Aon Risk Solutions |
Vancouver Branch, Mining Practice Leader
t +1.604.443.2425
andrew.russell1@aon.ca

Tim Snyders
Vice President and Account Executive
Aon Risk Solutions
t +1.604.443.3388
tim.snyders@aon.ca



Questions/Thank you

Empower Results®