SURVIVING A CYBER INCIDENT

DRIE Spring 2017 Symposium
March 9, 2017
Presented by: Greg Markell

RIDGE GLOBAL

DISCLAIMER

This presentation contains general information only and is not intended to provide an overview of coverages. The information is not intended to constitute legal or other professional advice. Please refer to insurer's policy wordings for actual terms, conditions, exclusions and limitations on coverage that may apply.

Section 1:

THE THREAT LANDSCAPE

INDUSTRY TRENDS

- Proliferation of ransomware demands
- IoT devices designed for functionality, not necessarily security
- Disruption as opposed to deletion
- No longer just ‘intangible’ loss
- Politically motivated hacking becoming “par for the course”

Section 2:

INSURANCE INDUSTRY TRENDS

INDUSTRY TRENDS

- Most incidents occur as a result of either a hacker, or employee
- Small businesses struggling with prevalence of ransomware and extortion demands
- Contractual language evolving. Minimum insurance requirements being embedded within contractual language
- Many businesses outsourcing critical functions/storage to third parties
- Confusion in insurance on divide between money/securities loss, and data loss

Section 3:

COMMON INSURANCE SOLUTIONS

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 arising from the breach

EXPENSE COVERAGES

Notification Costs: The costs associated with letting all those affected by the breach know that it has occurred. This would include costs such as: mailing campaigns, credit monitoring, call centres to handle questions, etc..
Forensic Investigative Costs: The costs associated with hiring a professional third party to determine where, when, and how the breach occurred; also, to ensure that no future problems occur as a result of that particular system issue.
Business Interruption: Lost income as a result of the breach during the period of restoration.
Crisis Management Expenses: The costs incurred in hiring a professional team to help prevent reputational harm to your business. This could include a PR team, lawyer to draft a press release, etc.
Data Restoration: The cost to restore the network and data to the point it was at before the event occurred. This can include both hardware and software replacement.
Cyber Extortion: Costs associated with an attack or threat against the company, when there is a demand for compensation to stop the attack.
Regulatory Proceedings Coverage: Coverage to provide for costs associated with being called in front of a civil, administrative, or regulatory proceeding.

LIABILITY COVERAGES

Network Security Liability: Covers damages and claims expenses associated with the unauthorized access to, degradation of, or disruption to the insured's network through the use of malware, denial of service attacks, phishing, etc. causing loss.
Privacy Liability: Covers the disclosure, use, access, destruction, or modification of personal protected Information.
Internet Media Liability: Liability resulting from allegations of: infringement of privacy, defamation, disparagement, piracy, copyright infringement, etc. related to content displayed electronically eg., a blog.

Section 4:

THE “OH NO” MOMENT

REPORTING

- When a breach (or suspected breach) happens, who makes the call?
  - What level of management does it need to get to in order to have to notify the insurer?
- What duties does the organization have?
- Who do you call first?
- When do you get outside counsel involved?
- What does the triage process look like?

CLAIMS TRIAGE

- Always call outside counsel first
- Report to the insurer(s)
- Involve forensics immediately
- Liaise with public relations and outside counsel – careful crafting of reputational preservation material going to the public… no admission of liability!
- Remediation experts involved
- Consistent updates to the insurer(s)/TPA’s

Section 5:

WHAT CAN WE DO?

GOVERNANCE

- Make it a governance issue – not an IT problem
- Focus must be on resiliency
- Disclosure to shareholders/stakeholders
- Compliance, while expensive, is a *minimum*
- Holistically… people, processes, technology

PRE-BREACH

- Assess what information your organization has
- Examine controls in place
- Develop a plan
- Assign responsibilities in advance
- Identify key stakeholders.
  - Internal and external
- Practice the plan
- Contract review – what are the responsibilities that both suppliers and vendors have?
  - Create annual checklists. Manage the process diligently

POST-BREACH

- Follow the plan
- If no plan exists, rely on the experts
- DO NOT sit on the issue
- Don’t try and fix it yourself

Section 6:

A NEW HORIZON

LEGISLATION

- Digital Privacy Act passed in June 2015
- Mandatory notification to OPC coming into effect
- “Real risk of significant harm”
- The incident log and implications from a third party liability perspective?
- Cost considerations for organizations
- CSA Staff Notices: 11-332 and 51-347

THANK YOU

Greg Markell
President & CEO
Ridge Canada Cyber Solutions
647-643-4737
gmarkell@ridgecanada.com