HUB

Transferring your Cyber Risk Through Insurance

Declan Friel HUB International

Presenter Disclosure

- **Presenters:**
- Declan Friel, HUB International;
- Kathryn Frelick, Miller Thomson;
- Vanessa Foreman, Hamilton FHT

- **Relationships with commercial interests:**
  - **Not Applicable**

Disclosure of Commercial Support

- **This program has not received financial or in-kind commercial support.**
- **In support of this program, there are no potential conflicts of interest**

Recent Trends In Cyber/Privacy Breaches

- Increasing number of class action lawsuits as a result of privacy breaches
- Ransomware (Eg.WannaCry) attacks are increasing and it is only a matter of time before FHT's may be affected
- Most incidents occur as a result of a hacker, or employee
- Small organizations are at increasing risk of a cyber event that could severely impact their operation

Why Cyber Insurance?

- Current legislation is mandating organizations to take steps to notify affected individuals in event of a breach.
- Defence costs for liability lawsuits could be significant.
- Cyber/privacy breach insurance is a relatively inexpensive means of ensuring the significant costs from a privacy/cyber breach are covered
- Gives you access to industry experts to mitigate and manage the event

Ransomware

- Ransomware is a type of malware that prevents you from using your computer or accessing certain files unless you pay a ransom.
- WannaCry was a recent example that effectively shut down the operation of NHS hospitals in the UK.
- Buffalo hospital spent $5 million on new hardware, software and services to recover its data and protect itself from future intrusions.
- Ontario Privacy Commissioner has issued a guideline that ransomware attack constitutes stolen information if PHI was not encrypted or de-identified.

Coverage for Physicians

- CMPA published an article in July stating its members are reporting an increasing number of ransomware attacks
- CMPA will defend physicians against lawsuits associated with privacy breaches
- It is unlikely that the CMPA will pay for the potential expenses associated with a cyber breach
- As the physicians are considered HICs w.r.t. the EMR in the FHT, they need to consider a means to transfer this risk

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
- Important to obtain a policy that has sufficient limits for both coverages.

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.

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.

Expense Coverages

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.

Business Interruption: Lost income as a result of the breach during the period of restoration

Liability Coverages

- **Privacy Liability:** Covers the disclosure, use, access, destruction, or modification of personal protected Information.
- **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.
- **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.

Claims Process

- Organization should have a list of the critical people at insurer/broker to contact in event of suspected breach
- First call should be to the insurers & Breach Coach (legal counsel appointed by insurer and typically named in policy)
- Breach coach directs the investigation of the breach, retains expert assistance and ensures the process benefits from appropriate privilege protections

Claims Process

- The Breach Coach directs the notification of potentially affected persons and will vet public statements with respect to the breach
- Breach Coach will involve forensics immediately
- Breach coach also acts as insured's representative with respect to engagement with the regulator
- Bottom line is that Breach Coach relieves a tremendous level of stress on organization during a time of crisis.

Security Best Practices for Cyber Risk

- Security culture & awareness - opening malicious emails; weak passwords
- Threat assessment and vulnerability testing
- Network security – encryption and dual authentication
- Mobile device security
- Data breach readiness plan

Summary

- Cyber insurance should be seriously considered as a means to manage the significant costs from a privacy/cyber breach are covered.
- Ensure your coverages are adequate for the size of your organization.
- Have a cyber readiness plan and practice it.
- Develop an incident response plan of vendors through your insurance policy