CYBER LIABILITY AND DATA BREACH INSURANCE FOR THE TECHNICALLY CHALLENGED: EVERYTHING YOU WANT TO KNOW BUT WERE AFRAID TO ASK

Panelists:
Judi Cranberg, Froedtert Health
Lynn Sessions, Baker Hostetler
Jason Warmbir, Willis Group
Moderator:
Heather Fields, Reinhart Boerner Van Deuren s.c.

Discussion Overview

- Cyber Event Hypothetical
- Understanding Cyberliability Coverage
  - Types of Insurance
  - Common Policy Limits
  - Other Considerations
- Risk Management Perspective
- Legal Counsel Perspective
- Role of Board and Senior Leadership

Cyber Event Hypothetical

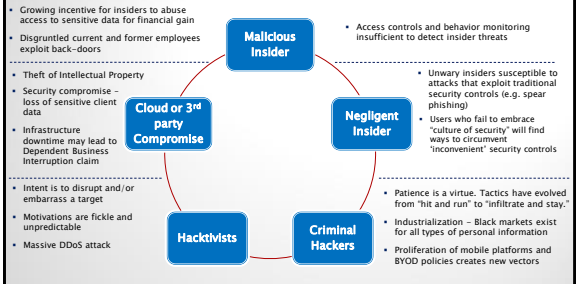
At 6pm on Friday, July 3rd, an information technology employee at a health system reports unusual server activity associated with malware and data exfiltration has been detected. The malware may have gained access to a file server containing PHI via a phishing email on a physician workstation.

DO YOU HAVE INSURANCE COVERAGE FOR THIS?

Cyber Insurance Markets

- Over 60 insurers writing coverage – a very robust market
- Substantial claims paid without insurers withdrawing from market
- Recognized underwriting standards
- Estimated $1B premium volume moving to $5B

Sources of Potential Data Breaches



- Growing incentive for insiders to abuse access to sensitive data for financial gain
- Disgruntled current and former employees exploit back-doors
- Access controls and behavior monitoring insufficient to detect insider threats
- Theft of Intellectual Property
- Security compromise – loss of sensitive client data
- Infrastructure downtime may lead to Dependent Business Interruption claim
- Unwary insiders susceptible to attacks that exploit traditional security controls (e.g. spear phishing)
- Users who fail to embrace "culture of security" will find ways to circumvent 'inconvenient' security controls
- Intent is to disrupt and/or embarrass a target
- Motivations are fickle and unpredictable
- Massive DDoS attack
- Patience is a virtue. Tactics have evolved from "hit and run" to "infiltrate and stay."
- Industrialization – Black markets exist for all types of personal information
- Proliferation of mobile platforms and BYOD policies creates new vectors

Insurance Considerations

- Identify the cyber exposures the company faces and what the plan to address these risks is?
- What coverage gaps exist in traditional insurance policies that would not respond to a cyber event? (i.e. Cyber Business Interruption vs. Property Business Interruption)
- What is the potential loss of net income/profit of an operating system (i.e. facility or plant) that would be incurred if our network were to be shutdown due to a cyber event?

Available Coverage to Address Cyber Gaps

- **Event Response Services**
  - Covers expenses incurred in responding to adverse publicity or media attention arising from a claim covered in the policy and other required response costs including:
    - Privacy breach-related "Duty to Notify" costs
    - Costs to procure credit monitoring services on behalf of customers
    - Call center costs
    - Legal costs from responding to a breach
    - Response coaching costs
    - Forensic costs
    - IT Security response costs
    - Public Relations service costs

Available Coverage to Address Cyber Gaps

- **Business Interruption & Extra Expenses**
  - Covers lost online and offline income when loss is caused by security breach or errors plus expenses of avoiding such a loss
- **Dependent Business Interruption**
  - Covers lost online and office income when loss is caused by a third party's network security failure or error

Available Coverage to Address Cyber Gaps

- **Network Security Liability**
  - Covers claims arising from an inability to use or access your network, infection of others' networks, information damage to other networks, inability of others to rely upon the accuracy, validity or integrity of their information residing on your network
- **Electronic Theft (select carriers)**
  - Covers for theft via a network of money, securities, goods, services and intangible property (e.g., intellectual property

Additional Coverage to Address Cyber Gaps

- **Content Injury Liability (media)**
  - Defamation, disparagement, copyright, trademark, publicity rights and content errors, etc. Covers computer readable content and can be expanded to all media
- **Data Restoration / Digital Assets**
  - Covers costs to recreate or restore network to pre-loss conditions. Attacks covered include those instigated by employees
- **Network Extortion**
  - Pays credible extortionist demands and response costs to demands for money against threats to release private information or bring down a network

CYBERLIABILITY INSURANCE: RISK MANAGEMENT CONSIDERATIONS AND ROLE OF RISK MANAGER

CYBERLIABILITY INSURANCE: LEGAL CONSIDERATIONS AND ROLE OF LEGAL COUNSEL

CYBERLIABILITY INSURANCE: ROLE OF BOARD AND SENIOR LEADERS