NEW WORLD OF

CYBER INSURANCE

September 28, 2021

Marc Galindo

www.usi.com

THE USI ONE ADVANTAGE®

USI at a Glance

Leading Brokerage & Consulting Firm

Largest privately-held broker of U.S. business

"America's Best Large Employers"

Two Years in a Row!

Forbes Magazine, 2018 & 2019

The USI ONE Advantage® delivers superior client solutions with financial impact

500,000+

clients served

$2 *Over* **BILLION** IN Revenue

8,000+ employees

~200 Local offices

Servicing local, national, and international needs.

150+ Years of brokerage experience

through our acquired agencies

PROPERTY & CASUALTY ▪ EMPLOYEE BENEFITS ▪ PERSONAL RISK ▪ PROGRAMS ▪ RETIREMENT CONSULTING

Misconceptions About Cyber Insurance

- Nothing is covered ("claims get rejected 95% of the time")
- I'm not in a high-risk industry (e.g. healthcare, financial services, retail, education or municipalities)
- My company is too small for the criminals to target
- I do not take credit cards -or- we pay a 3rd party to process our credit card transactions
- I know our controls are inadequate, so nobody will cover us anyhow

What is "Cyber Insurance?"

Part One: 1st Party Insuring Agreements

1st Party Insuring Agreements

- Cyber Extortion
  - Reimbursement for payment of ransom and related extortion forensics costs as a direct result of a credible extortion threat
- Breach Response and Crisis Management
  - Covers costs incurred to respond to a data breach (forensics, notification, monitoring)
- Business Interruption
  - Reimbursement for lost net income and associated extra expenses resulting from the total or partial interruption of a company's computer system via a:
    - cyber attack/security breach or
    - system failure (unexpected outage)
- Dependent Business Interruption
  - The same as Business Interruption, but for net income lost due to a cyber attack/security breach or a system failure of a vendor (dependent business)
- Data Restoration
  - Reimbursement for costs associated with restoring or recreating non-physical assets, such as data that are corrupted or otherwise destroyed via a cyber attack

What is "Cyber Insurance?"

Part Two: 3rd Party Insuring Agreements

3rd Party Insuring Agreements

- Security and Network Privacy Liability
  - Coverage for liabilities resulting from a failure to protect or unlawful disclosure of both online and offline confidential information, virus attacks, denial of service attacks and transmission of malicious code
- Privacy Regulatory Defense and Penalties
  - Coverage for defense costs and fines/penalties for violations of privacy regulations
- Media Liability
  - Coverage for both online and offline media content, including claims alleging copyright/trademark infringement, libel/slander and personal injury
- Payment Card Industry Data Security Standards (PCI DSS)
  - Reimbursement for costs associated with monetary charges, assessments, fines and/or penalties levied by a payment card association or acquiring bank resulting from non-compliance with PCI DSS

Added Benefits of "Cyber Insurance"

Pre-Breach Services

Pre-Breach Services

- Insurers provide value-added services to their cyber policyholders
  - These “pre-breach services” serve to mitigate the risk of cyber events, which benefits both the insurers and the insured
  - Offerings vary from insurer to insurer
  - Some insurers offer “free” services, while others provide access/introductions to vetted vendors, often at preferred rates. Examples of pre-breach services include:
    - Vulnerability scans
    - Phishing simulations and employee training
    - Tabletop exercises and assistance in developing incident response plans
- These services are not guaranteed to eliminate the risk
  - They help by identifying vulnerabilities and providing resources to address them
  - If you have a cyber event/breach/litigation, having coverage in place provides comfort that you have a partner standing by ready to respond

The Cyber Insurance Market

The Cyber Insurance Market

Market Dynamics

- Carriers in the market
  - There are over 100 policy forms available, but there are major players
- Claims on the rise
  - Ransomware has seen the greatest uptick; all industries & sizes at risk
  - Both frequency and severity have increased exponentially in the last two years
- Rate increases are here
  - Because claims are on the rise, insurers are re-evaluating their books of business and realizing premiums are inadequate

- How to Obtain Coverage
  - ✓ Contact your broker
    - Cyber expertise
    - Claims expertise
  - ✓ Complete submission materials
    - Application
    - List of outsource service providers
    - Supplementary info, as needed
  - ✓ Understand your options
    - Limits, retentions, term & conditions
    - Pre-breach offerings
  - ✓ Know who to call during a claim

"TOP 5" CYBER UNDERWRITING FOCUS AREAS in 2021

1. **MULTIFACTOR AUTHENTICATION***
   - What are the specifics on how widely it is utilized?
     - Privileged accounts, back-ups, remote access require MFA for the entire network?
     - All local and remote access for administrative and privileged users at a minimum?
   - Compensating factors in place where it's not being utilized **are no longer accepted** and we/USI will need to seek additional detail from client
2. **END POINT DETECTION AND RESPONSE (EDR) & EXTENDED DETECTION AND RESPONSE (XDR):**
   - In place? Utilized on entire network – if not, why not?
   - Vendors used – Sentinel One? Carbon Black? Other?
3. **24/7 NETWORK MONITORING AND SECURITY OPERATIONS CENTER (SOC):**
   - In place? How is it being done? Internal or external (through an IT Managed Service Provider, e.g.)? 24/7 monitoring of all logs and reports?
4. **NETWORK BACK-UPS:**
   - Type? Immutable? Does it require MFA to access?
   - Location - off site? Co-location? Air-gapped?
   - Frequency - how often are back-ups made?
   - Testing - is this done?
5. **NETWORK SEGMENTATION:**
   - Critical systems segmentation in place?
   - EoL (End of Life) / EoS (End of Support) update?
   - Process for monitoring and preventing lateral movement?
   - Patching and patching cadence? Especially for critical risks?

***What is Multi-Factor Authentication (MFA)?**

Multi-factor authentication (MFA) is a security control that requires users to verify their identities by providing multiple pieces of evidence before gaining access to a device or application.

What Are the Different Authentication Factors?

- Knowledge—the user provides information only he/she knows, like a password or answers to challenge questions
- Possession—the user supplies an item he/she has, like a one-time password
- Inherence—the user relies on a characteristic unique to who he is, such as a fingerprint, retina scan, or voice recognition

Two-Factor Authentication vs. Multi-Factor Authentication (2FA vs. MFA)

- Two-factor authentication (2FA) always utilizes two of the factors to verify the user's identity.
- Multi-factor authentication (MFA) could involve two of the factors or it could involve all three.

Source: IBM

Items requested if Cyber coverage currently in place – IN ADDITION TO APPLICATIONS:

- Current cyber policy including all endorsements and most recent application/supplements
- Copy of most recent audited financials with notes (at a minimum revenue size is needed)
- Copy of organizational structure with ownership (most recent)

Items requested if cyber coverage NOT currently in place:

- Understanding of which cyber threat(s) does client believe pose the largest financial/operational impact to the organization
- Cyber preparedness plan (DRP/IRP)
- Most recent audited financials

USI