October 28, 2021

Cyber Insurance

THE USI ONE ADVANTAGE®

www.usi.com

USI®

Why are we talking about insurance?

Why is it Important

- More frequent cyber events, impacting all organizations
- More severe cyber events – costly lawsuits, fines/penalties and event response costs
- Organizations have limited expertise to deal effectively with a cyber event
- Ransomware – A Tale of Three Cities

City	Initial Demand	Final Estimated Costs to City
City in Georgia	$55,000	$17M
City in Maryland	$76,000	$18M
City in Florida	$485,000	$10K

Building a Solution

Privacy & Network Coverage

Building Block #1	Building Block #2	Building Block #3
Liability Costs	**Compliance/Corrective Costs**	**Direct Costs**
Trigger: Liability costs when someone sues you or makes a demand as a result to	**Trigger:** Costs associated with loss containment and regulating authorities	**Trigger:** Direct costs to your business as a result of a security failure/system failure
Coverage Included: ▪ Privacy Liability ▪ Network Security Liability ▪ Media Liability	**Coverage Included:** ▪ Notification Costs ▪ Privacy Regulatory Costs ▪ Payment Card Industry/ Data Security Standards	**Coverage Included:** ▪ Cyber Extortion ▪ Network Interruption/ Extra Expense ▪ Contingent Network Interruption/Extra Expense ▪ Data Reconstruction ▪ Bricking Coverage ▪ Voluntary Shutdown ▪ Reputational Harm BI/EE ▪ Social Engineering

Disclaimer: *The hypothetical claims scenarios contained herein are for illustration purposes only and should not be relied upon as governing any specific facts or circumstances. Actual claims are governed by your specific policy terms, conditions, limits, and exclusions and are subject to individual claims review by applicable insurer representatives.*

Typical Cyber Exclusions

Exclusions include but are not limited to:

- Coverage best addressed in another insurance policy
- Policyholder decides not to assume identified risk controls just because;
  - Policyholder decides not to complete a contract just because
- Certain actions against public policy and consumer protection laws i.e. :
  - FTC Federal Trade Commission
  - DMCA (Digital Millennium Copyright Acts
  - ERISA (Employee Retirement Income Security Act)
  - SEC (U.S. Securities and Exchange Commission)
- Prior Knowledge of prior acts…the building is burning and now we need insurance. The intent is of course to protect the entity against unforeseen events
- Dishonest, Criminal Acts
  - The intent is to protect the entity against the acts of rogue or uninformed employees.
- Infrastructure, Act of War and Nuclear
- Coverage best addressed in specific policies, i.e.
  - Patent Infringement

Top 4 Cyber Threats

DATA BREACH

Protected or confidential data has been viewed, stolen, or used by an unauthorized individual.

In public sector data breach costs increased from an average total cost of $1.08MM in 2020 to $1.93MM in 2021. This has resulted in a 78.7% YOY increase.

via IBM YE 2021 study

BUSINESS INTERRUPTION

Attack that directly or indirectly causes business interruption or network degradation, incl. recovery costs.

The negative impacts of these events are obvious to the organizations and individuals involved and can include massive costs to recover. The Baltimore ransomware attack crippled government systems for months, disrupting everything from water billing to real estate transactions. A separate attack caused the county's school system to shut down for 115,000 students. The interruption impacted student academic performance, lesson plans, and communication between teachers, students and parents.

CYBER EXTORTION

Cyber attack or threat of an attack against an organization coupled with a demand or request for money or other actions to avert or stop the attack.

Based on available data, most public entities are not paying ransoms. In 2020, 26.7% of public entities refused to pay the ransom, while 12.7% did pay, and the median ransom amount in 2020 was $389,000. In 2019, the city of Baltimore chose not to pay a $75,000 ransom demand, and the city spent over $18 million on recovery. New Orleans, after refusing to pay their ransom during an attack in December 2019, spent about $7 million on recovery.

SOCIAL ENGINEERING

"Business Email Scam" or "Phishing" uses deception to manipulate individuals into divulging confidential or financial information.

Social Engineering scam losses jumped on average to $75,000 per successful attempt in 2019 (YoY jump from approx. $17k in 2018). Remote workforces may be more susceptible to this type of attack. Email, SMS texting attacks ("smishing") and even phone calls with a live person ("vishing") are attack vectors.

2020 stats are showing average Social engineering estimates of $80,000-$130,000 depending on the study.

https://pdf.ic3.gov/2019_IC3Report.pdf

Loss Scenario 1: “Smartphone Lost!”

A medical malpractice defense attorney forgets an unencrypted Smartphone in an airport restaurant. It is never recovered. It is late at night on a weekend and the Smartphone is not remotely wiped for 2 days. The attorney has 8,000 emails and some contain protected health information.

Source: The Chubb Corporation

Loss Scenario 2: "The Cyber I.D. Thief"

On a "black hat" website, Myra learns how to write an SQL Injection script that allows her to gain access to a law firm's databases through their website.

She is able to access and download over the Internet names, addresses and Social Security numbers of 1,500 of the firm's clients.

As required under State breach notification laws, the firm notifies their affected clients, incurring $250,000 in notification and related crisis management expenses.

Source: The Chubb Corporation

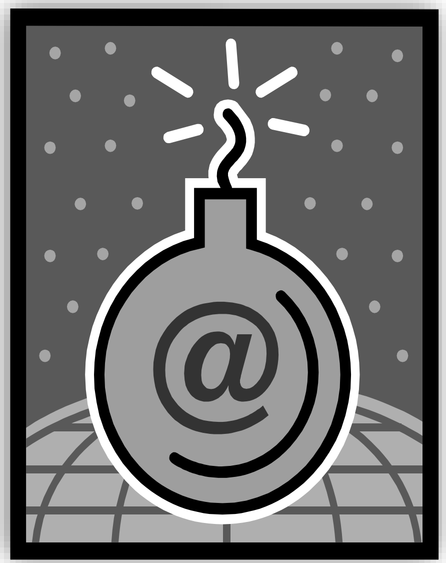
Loss Scenario 3: “The Oops Factor”

Rodney, in Personnel, is rushing to get a spreadsheet containing the names, addresses, and Social Security numbers of 250 job applicants to a background screening firm.

Attaching the sheet to an e-mail, he then inserts the name of his contact in “To:”, not realizing that what he has inserted is his bowling league contact list.

He hits Enter – and sends the list of prospective employees to the correct contact – and 30 other people outside the organization.

Source: The Chubb Corporation



Loss Scenario 4: "The Inside Job"

Prior to dismissal for cause, a disgruntled system administrator installed a logic bomb into the firm's computer system. Some time after departure, the logic bomb began systematically corrupting critical data.

The firm identified the root cause and quickly quarantined the corrupted data. However, it took several months to restore the data and resume normal business operations.

Source: The Chubb Corporation

Loss Scenario 5: “Social Engineering – You Better Think Twice”

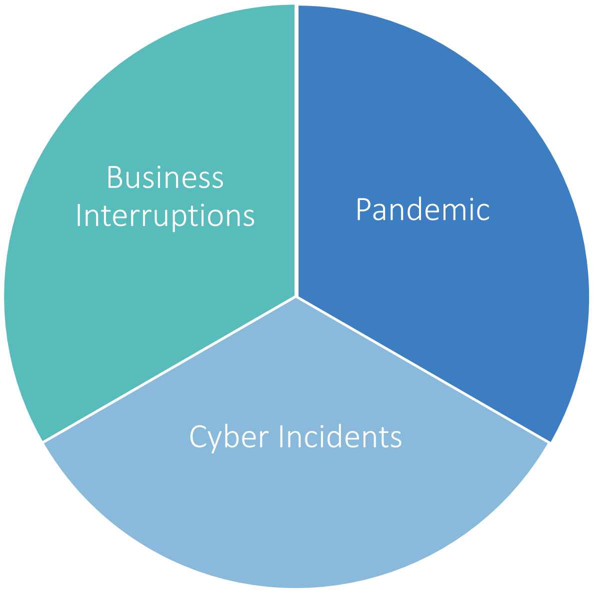
In connection with a recent closing of one residential real estate transaction, hackers infiltrated the seller’s systems and caused a fraudulent email to be sent to the buyer’s lawyers, including modified wire transfer instructions that would have sent funds to a third-party account controlled by the hackers.

Source: The Chubb Corporation

State of the State

Cyber Realities

COVID Trifecta



- Record Increase in Ransomware Activity
- Record increase in the severity levels of ransomware event
- Deeper focus on information security controls
- Renewed focus on aggregate event initiated by vendor supply chain incident
- Increase in regulations and regulatory oversight
- Reputation Harm

Cyber Market Update

National Market Update – Aggregate- and Rate Forecast	
Product Line/Market Update*	Q 42021
Network Security & Privacy (Cyber)	40% to 50% pristine submission / +50%- +100% for less pristine
Technology/MPL Network Security	40% to 50% pristine submission / +50%- +100% for less pristine

- Increased Ransomware Activity
- Increased Excess Rates
- Aggregation Exposures
- Privacy Regulatory Changes
- Premium and SIR Changes
- Additional Underwriting Requirements – Technical Underwriting
  - Scans – Implications & Use

Ransomware Classification Scheme

- Best in Class
- Above Average
- Average
- Below Average

Insulation of Insurers

- Exclusion
- Coinsurance
- Sublimit/Retention
- Specific Event Exclusion

Insurers are at least laser-focused on insured controls like:

- Record Count
- **Multi-factor authentication (MFA) controls**
  - **Remote Access**
  - **Privilege Accounts**
  - **Email Accounts**
- Patch management processes/ cadence
- **Backup procedures**
  - **Encryption**
  - **Air gapped**
  - **Immutable**
- Presence and use of endpoint detection and response (EDR),
- Open Remote Desktop Protocol (RDP)
- Vendor Management IT controls
- Phishing Training

CONFIDENTIAL AND PROPRIETARY: This document and the information contained herein is confidential and proprietary information of USI Insurance Services, LLC ("USI"). Recipient agrees not to copy, reproduce or distribute this document, in whole or in part, without the prior written consent of USI. Estimates are illustrative given data limitation, may not be cumulative and are subject to change based on carrier underwriting. —

Cyber Market Update

- **Cyber Insurer Appetite Changes**
  - Insurers experienced a spike in ransomware events during 2020 and also experienced a massive increase in the dollar impact of these events. While ransomware affects all industries, insurers are managing their exposures (reducing the deployed capacity or increasing the overall SIR) in certain hard-hit industry verticals, including:
    - Municipalities
    - Manufacturers
    - Educational institutions
    - Professional services firms (i.e., law firms)
    - Public officials/entities

“TOP 7” 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?
6. **PRIVILEGED ACCESS MANAGEMENT**
   - in use and product?
7. **ARE ALL DOMAIN ADMINISTRATOR ASSIGNMENT REVIEWED REGULARLY?**

NEXT STEPS

If you currently purchase Cyber Insurance

- Have your current policy reviewed by an insurance professional with expertise in Cyber Liability insurance. There is no standardized policy so coverage can differ a great deal between insurers
- Take advantage of the pre-loss consulting services and put a plan in place ahead of a loss
- Review underwriting requirements with your broker well ahead of renewal

If you do not currently purchase Cyber Insurance:

- Start the process now; underwriters are very strict so it may take time to put in place the controls insurers require
- Make sure you are working with an organization that has a specialization
- Start thinking of a public relations response if you have a loss without Cyber Liability insurance in place

USI®

CONFIDENTIAL AND PROPRIETARY: This document and the information contained herein is confidential and proprietary information of USI Insurance Services, LLC (“USI”). Recipient agrees not to copy, reproduce or distribute this document, in whole or in part, without the prior written consent of USI. Estimates are illustrative given data limitation, may not be cumulative and are subject to change based on carrier underwriting.