



LEMME

INSURANCE BROKERS & CONSULTANTS

A DIVISION OF EPIC

# Managing Cyber Risk: A 360° View

June 2022

[EPICBROKERS.COM](https://epicbrokers.com)

# AGENDA



- I. Current Risk Environment
- II. Managing Cyber Risk
- III. Cyber Insurance Market
- IV. Questions

# Current Risk Environment

---



# Escalating and Evolving Risk

---

## 5G Revolution

- Greater power to *connect* internet devices;
- Artificial Intelligence: although it helps us, allows us to be more efficient, it feeds into cyber crime

## Lingering Global Pandemic

- Changing Workplace
- Lack of Certainty and Stability

## Cyber Criminal Cartels

- Increasing collaboration within criminal underworld – formation of cartels

## Ransomware 3.0

- Double, Triple, Quadruple Extortion



# Ransomware

84% of US Organization have experienced **phishing** or **ransomware** attack in the past 12 months

Average **Ransom Payment** has increased **82%** between 2020-2021  
\*\*\*today average is **\$570,000**




# Managing Cyber Risk

---

# Commitment to Network Security & Data Privacy

---

A circular inset image on the right side of the slide. It shows a person standing on a rocky, mountainous peak with their arms raised in a 'V' shape, signifying achievement or triumph. The background is a vast, cloudy sky. The image is semi-transparent, allowing the text to be overlaid.

When you're committed to  
something, you accept no  
excuses – only results.

Ken Blanchard

# 360° View: Managing Cyber Risk



**Legal  
and  
Compliance**

**Business  
Continuity**

**Leadership  
and  
Governance**

**Human  
Factor**

**Operations  
and  
Technology**



# Legal and Compliance

## Attentiveness to Privacy Regulatory Landscape

Rapidly Evolving Domestic and International Regs

- Regulatory Fines/Penalties
- Private Right of Action – Trending but contentious point

## Sensitivity to Risk of Civil Liability

Civil Actions by Clients/Employees/Bus Partners

- Failure to Protect Data/Corporate Info
- Theft of Funds: SEF; Client/EE Accounts
- Wrongful Collection of Data



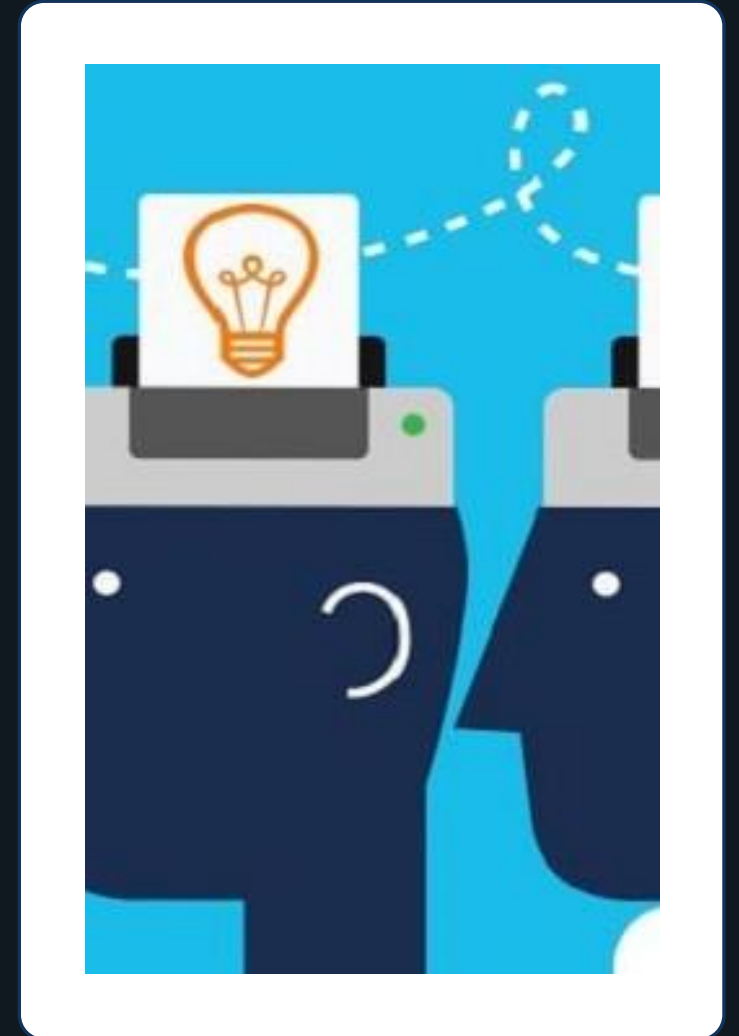
# Human Factor

## Training and Awareness

- Formal training should be *engaging*

## Create a *Culture* of Security

- Take advantage of teachable moments
- ***Demystify*** security by using everyday language
- Create a sense of understanding and belonging – security belongs to everyone
- Communicate the risks in a way that everyone understands
- Provide ***non-threatening***, convenient ways for employees to report suspicions





# Business Continuity





# The First 72 Hours

---

How you handle the **first 72 hours** after an attack is detected are critical.

Once you reach out and engage the threat actor, the **proverbial clock starts** ticking.

Missteps within the first **72 hours** can have a significant impact on the overall cost of the event – from both a **financial and reputational** standpoint.





# Are you Prepared to Respond?

## **Create Separate Incident Response Playbooks**

- Extortion, ransomware, SEF, data breach, invoice manipulation, dependent business attack...

## **Practice/Stress-Test Your Plan**

- Conduct Table Top Exercises

## **Incident Response & Recovery Information Packets for all Team Members**

- These should be **HARD** copy documents!

## **Incorporate insurance and other contract requirements into you Incident Response Plan**

- Reporting requirements

# Understand your Recovery Timeline



Understand and ***continually re-evaluate*** your Recovery Timeline

- How long will it take to recover substantially? Fully?
- Consider the impact of severity and nature of the incident on your recovery time
- What factors will/could have a ***significant*** impact on your recovery time?

# Consider Your Position on Ransom

---

Under what circumstances would you pay? Under what circumstances would you NOT pay?

- Network Encryption + Data Exfiltration?
- Data Exfiltration alone?
- Threats to auction high-profile client data?
- Threats to auction Senior Executives data?

Consider the implications of a “**no pay**” position:

- Practical/Financial/Reputational/Legal



# Ransom Payment Considerations

**Practical Considerations:** Will paying get your network/data back?

- Does the attacker's track record suggest it will provide a workable decryption key? (There is no guarantee)
- Will paying incentivize *future* attacks?

**Financial Considerations:** Is paying the ransom the most *efficient and cost-effective* means to recover versus restoring from backups?

- 2019 Attack on **City of Baltimore**: Mayor refused to pay Ransom Demand of \$760K; Cost of Rebuilding the systems cost \$18M +

**Reputational Considerations:**

- How will paying the ransom be *perceived* by clients, employees, business partners etc.

**Legal Considerations:** Is paying legal?

- Legality of paying a ransom varies from country to country
- Insurability issues – OFAC; AXA XL-France





# Operations and Technology

- (1) MFA implemented (privileged access, remote access, remote cloud-based apps/O365)
- (2) Network segregation/segmentation
- (3) Regular data backups (less than quarterly)
- (4) Backups stored in more than one location
- (5) Disabled administrative privileges on endpoints
- (6) Security awareness training for employees
- (7) Anti-malware implemented
- (8) Strong password controls
- (9) Sender Policy Framework (SPF) implemented
- (10) Endpoint Detection and Response (EDR) implemented
- (11) 24/7 Security Operation Center (SOC) engaged
- (12) Security info/event management (SIEM) platform implemented
- (13) End of Life hard/software segmented/air gapped from network



*These are the basic controls that underwriters **EXPECT** to see – today*

*Keep in mind, underwriting requirements are **dynamic** and **vary** based on market*

# **Leadership: Culture/Commitment to Security**

- Network Security must be a strategic part of business operation: Requires investment of time and money
- Culture of C-Level Engagement: True and Sincere Commitment to Network Security and Data Privacy

# Cyber Insurance Market

---



# What You Need to Know about the Cyber Market

## **RATE, RATE and MORE RATE: Increasing Premiums**

Firms are experiencing premium **increases** at renewal of 50%+. In many instances, the increase is in the double digits – 100%+. Having strong network security and data privacy controls is an **expectation**, not a basis for a discounted premium.

## **SKIN IN THE GAME: Increasing Retentions Connected to Revenue**

Underwriters are using retentions and deductibles as a way of spreading or sharing the risk with the Insured. Often, the Retention is set based on the annual revenue of the company.

## **BACKING AWAY ON LIMITS: Decreased Capacity**

Maximum limit, today, is \$5,000,000 on primary layer – most markets.

## **EXIT STAGE LEFT: Carrier Exiting the Market**

We are starting to see carriers **exit** the market entirely.

## **NOT AS HUNGRY: Changing Underwriting Appetite**

In the past, carrier appetite was insatiable. Today, carriers are reevaluating their appetites, including classifying more industry verticals as “high risk”.



# What You Need to Know about the Cyber Market

## **MFA, MFA, MFA: Enhanced Underwriting**

Underwriters now “expect” to see certain network controls in place; or NO quote.

## **JUST SAY NO: Declinations More Frequent**

Underwriters are engaging in comprehensive, technical and strategic underwriting that results in more declinations. They are not afraid to “just say no”

## **PERFECT STORM: Market Saturation**

Most cyber insurance brokers are conducting full marketing exercises + demand for cyber insurance has increased = Markets are flooded with applications.

## **TIGHTEN THE BELT: Coverage Tightening**

Most cyber insurers now impose co-insurance and/or sub-limits on coverage for ransomware attacks which extends to all areas of the cyber policy that are triggered by the attack.

## **PRESSURE: Cyber First Responders Under Pressure**

The increase in frequency and severity of claim activity is also taking its toll on cyber first responders: claims professionals, breach coaches, cyber extortion negotiators, computer forensic vendors, public relations (PR) firms...

# Best Practice Tips

- 1. Strive for a Culture/Commitment to Network Security and Data Privacy**
  - ✓ Invest the time and money!
  - ✓ Security Leaders need a seat at the C-Suite Table
- 2. Consider your position on Ransomware IN ADVANCE of an attack**
  - ✓ Continue the conversation regularly
- 3. Stay focused on the Privacy Regulatory Environment**
  - ✓ Increased enforcement is on the horizon



# Questions?

---