MARSH & McLENNAN AGENCY

WORLD CLASS. LOCAL TOUCH.

Cyber Security – The Complex & Inevitable Exposure

NRASP - July 15, 2020

Dan Hanson, CPCU

SVP Management Liability and Client Experience

Marsh & McLennan Agency

Mario Paez, RPLU, MBA, CIPP/US

Director, Cyber & Technology E&O

Marsh & McLennan Agency

Disclaimer

- *This presentation and content is not meant to be considered professional legal advice.*

- *The presenter is not a licensed attorney and all information obtained from this presentation should be considered for informational purposes only.*

- *You should consult with a licensed privacy counsel for any decisions surrounding your corporate privacy initiatives, incident response plan or data breach response methodology.*

Agenda

- Cyber Risk Statistics
- Why Might you Be a Target
- Emerging Threat Trends
- Risk Management Techniques
- What to do Once a Data Event has Occurred
- Why Insurance Coverage is Recommended and Things to Look for in the Policy
- Q&A

Covid Related Cyber Threats & Stats

- FBI and U.S. Secret Service have recently issued alerts for the growing threats on Business Email Compromise and Malicious Email Attacks.
- Ransomware attacks jumped 148 percent in March from the previous month (VMWare)
- Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600% (KnowBe4)
- Ransomware demands have continually increased over the past year due to increased sophistication of attacks (such as infiltrating critical systems and backups) with multi-million dollar demands becoming more common.
- Increase of 33% from Q4 2019 to Q1 with average demand being over $111,000 (Coveware)
- The majority of SMBs (83%) said they do feel prepared for a ransomware attack. Forty-six percent of SMBs have been targeted by ransomware, 73% have paid the ransom (Infrascale)
- Cloud-based cyber-attacks by external actors on businesses went up by 630% between January to April 2020.
- During May, a total of 108 data breaches exposed 841,529 sensitive records and 68,298,815 non-sensitive records.
- Around 16 billion records have been exposed so far this year. According to researchers, 8.4 billion were exposed in the first quarter of 2020 alone, a 273% increase from the first half of 2019 which saw only 4.1 billion exposed.
- Average estimated probability of a successful breach for organizations in the US is 45% (ESI Thoughtlab June Report)

Statistics

NetDiligence Cyber Claims Study 2019 (+2k claims analyzed)

- Small to Medium Sized Enterprises (SMEs) (less than $2B in revenue) accounted for 96% of claims reported
- **SME Average Expenses Paid:**
  - Breach Expenses: $178k
  - Crisis Services: $112k
  - Legal Expenses: $181k
  - Business Interruption: $343k
  - Per-Record Costs: $234 per record
- **SME Cause of Loss and average:**
  - Social Engineering: $107k
  - Ransomware: $150k
  - Hacker: $337k
  - Business Email Compromise: $156k

**Source: NetDiligence Cyber Claims Study 2019*

Statistics

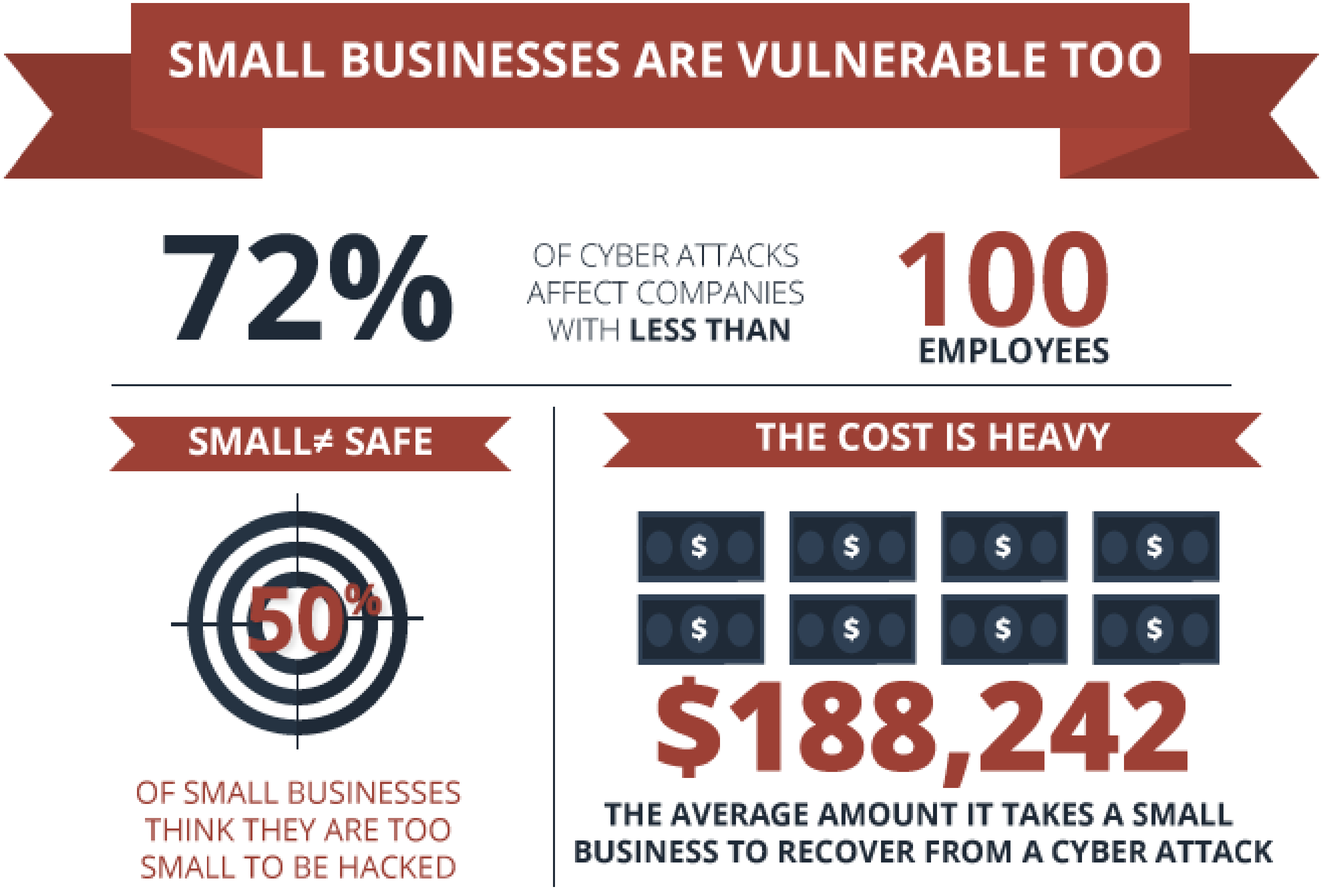
NetDiligence Cyber Claims Study 2019 (+2k claims analyzed) Continued:

- **Large Companies Average Expenses Paid:**
  - Breach Expenses: $5.6M
  - Crisis Services: $3.8M
  - Legal Expenses: $2.2M
  - Business Interruption: N/A*
  - Per-Record Costs: $296 per record
- **Large Companies Cause of Loss and average:**
  - Social Engineering: $409k
  - Ransomware: $15M
  - Hacker: $7.9M
  - Malware/Virus: $6.9M
  - Legal Action/Third Party: $1.9M
  - Business Email: $341k

**Insignificant Data – One incident mentioned of a non-criminal network outage/system glitch. Lost income reported for that event was $60M; the recovery expense was $20M.*

**Source: NetDiligence Cyber Claims Study 2019*

Small does NOT = Safe



SMALL BUSINESSES ARE VULNERABLE TOO

72% OF CYBER ATTACKS AFFECT COMPANIES WITH **LESS THAN** 100 EMPLOYEES

SMALL≠ SAFE

50% OF SMALL BUSINESSES THINK THEY ARE TOO SMALL TO BE HACKED

THE COST IS HEAVY

$188,242 THE AVERAGE AMOUNT IT TAKES A SMALL BUSINESS TO RECOVER FROM A CYBER ATTACK

The Cyber Risk is Real

Cyber ranked 4th in areas risk will increase

82%

of respondents expect increased risk of cyber attacks leading to theft of money or data

80%

of respondents expect increase in cyber risk around disruption of operations

Industry Cyber Loss Statistics

- **Healthcare -** $6.45M is average total cost of a data breach for healthcare industry ($429 per record; 236 days to Identify and 93 days contain to contain)
- **Retail** - $1.84M is average total cost of a data breach for retail industry ($119 per record; 228 days to Identify and 83 days to contain)
- **Education** - $4.77M is average total cost of a data breach for education industry ($142 per record; 212 days to Identify and 71 days to contain)
- **Hospitality** - $1.99M is average total cost of a data breach for hospitality industry ($123 per record; 200 days to Identify and 77 days to contain)
- **Transportation** - $3.77M is average total cost of a data breach for transportation industry ($130 per record; 203 days to Identify and 72 days to contain)
- **Financial Institution** - $5.86M is average total cost of a data breach for financial institution industry ($210 per record; 177 days to Identify and 56 days to contain)
- **Manufacturing & Construction -** $5.2M is average total cost of a data breach for industrial (including mfg & construction) industry ($160 per record; 220 days to Identify and 82 days to contain)

(source: Ponemon-IBM Cost of a Data Breach)

Why Might Your Organization Be A Target

What Kinds of Information are at Risk?

Client/Vendor/Employee/Competitive Information

- Intellectual Property: Plans, Processes, People, Clients
- Protected Healthcare Information (PHI), including health records, test results, appointment history, prescriptions
- Personally Identifiable Information (PII), like Drivers License, geolocation, biometric
- Financial information
- Access Credentials including ID and passwords

Employee Information

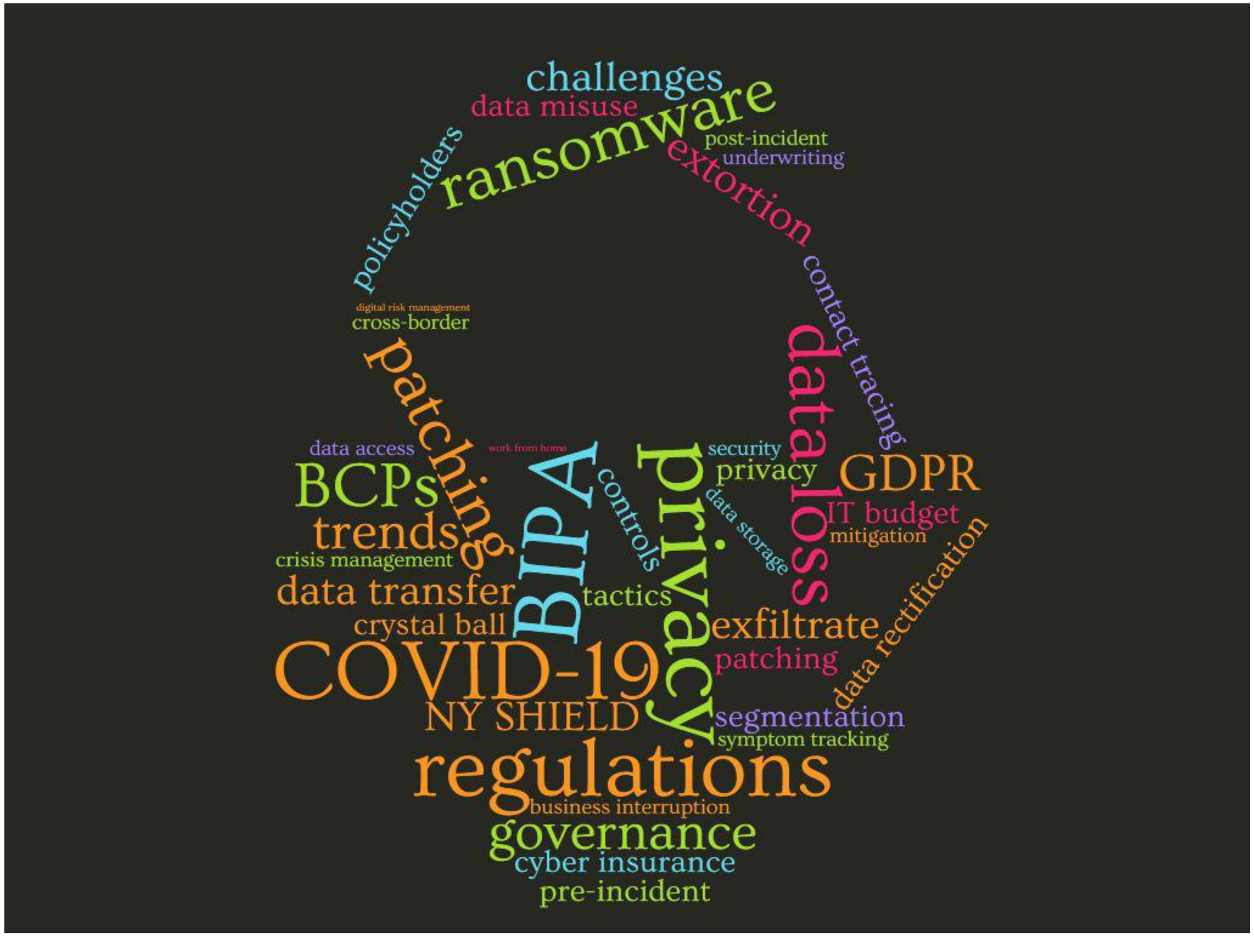
- Employers have at least some of the above information on all of their employees (Census)

Access to Vendor & Clients Information

Why Your Organization May Be A Target?

- **Computer-based systems for operations:** Many inter related systems
- **Multiple systems, or Ineffective integration of systems:** M&A
- **Staff or members take work home with sensitive organizational information**
- **Utilize free software or inexpensive hosting**
- **Use outsourced IT infrastructure or utilize an understaffed IT team**
- **Rogue employees / staff**
- **Resource scarcity–** no expertise or infrastructure to implement and maintain best practices for security.

Emerging Threat Trends



Source: NetDiligence

What Preventive Measure Organizations Can Take Against Threats

Cyber Preventative Measures

1. Establish / support VPN or other secure connectivity solutions to employee workstations and mobile devices via MDM.
2. Ensure multi-factor authentication (MFA) across critical systems
3. Back up & test system resiliency
4. External perimeter protections / Log and monitor access
5. Maintain clear inventories of digital assets and locations
6. Email controls - filters and sandboxing; strong passwords; frequent
7. Consistent employee awareness training
8. Verify requests for information

Cyber Preventative Measures

8. Encrypt whenever possible
9. Have written procedures in place to handle sensitive place
10. Be conscious of privacy issues with contact tracing and scanning of business invitees.
11. Schedule a third-party assessment and vulnerability scan of your network
12. Ensure updated patching of systems, browsers, software, anti-virus
13. Ready your incident response plan - Review MSA's of incident response firms such as legal and forensic firms that are approved by your cyber insurance carrier.
14. Consider cyber insurance in connection with your incident response plan
15. Segment your network
16. Contractual controls and audit

Contractual Considerations – 3rd Party Agreements

- Timing of Notice Back to Your Organization
  - X days to notify you of breach of your organization’s information

- Appropriate Privacy/Cyber/Data Liability Coverage
  - It may not mean the same coverage you carry

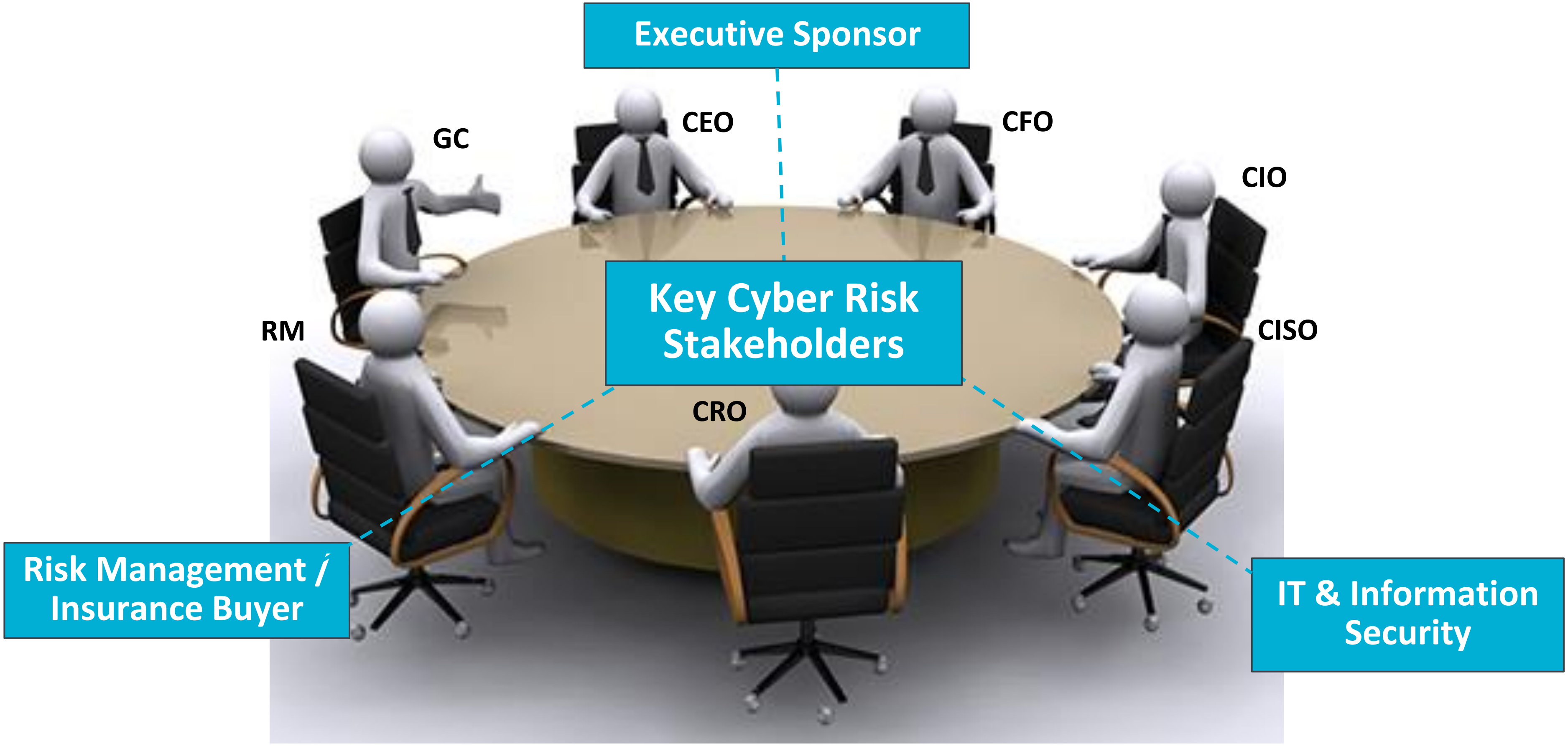
- Separation Terms/Provisions
  - X days to return/certify destroy your organization’s information

- Cloud Providers – For PII purposes, house data within US

Incident Response Plan

- Do you have a crisis response plan for a data security breach?
  - How do you Communicate?
  - Who is Involved?
  - When do you Communicate?
  - Assessing the scope of the breach and damage
  - Technological fixes and forensics
  - Notifications and remedial actions
  - Working with law enforcement
  - Working with governmental regulators
  - Public relations
  - Internal investigations and employee relations

Cyber risk has THREE core stakeholders



Executive Sponsor

Key Cyber Risk Stakeholders

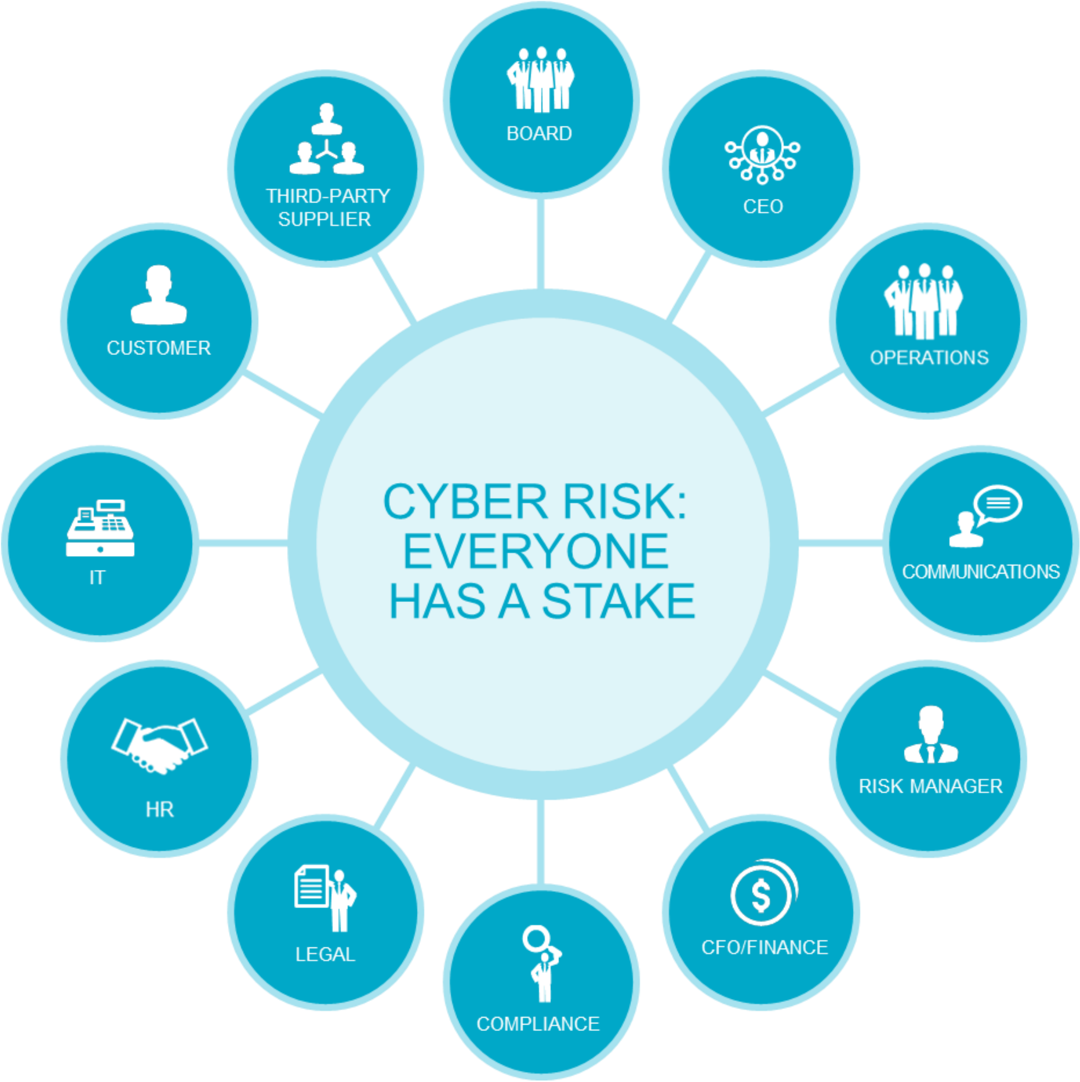
Risk Management / Insurance Buyer

IT & Information Security

DEFINING YOUR RISK
IMPACT ACROSS THE ORGANIZATION

Cyber is not just an IT issue.

It is an enterprise risk that impacts many key stakeholders within your organization.



Anticipate an Event: Not If, but When

A cyber breach isn’t always a disaster.

Mishandling it is.

Simplified Cyber Liability Timeline

Trigger of events as a result of cyber liability

Discovery

Actual or alleged theft, loss, or unauthorized collection/disclosure of confidential information that is in the care, custody, or control or the insured, or a 3rd party for whom the insured is legally liable. Discovery can come about in several ways:

- Self Discovery – usually the best case
- Customer inquiry or vendor discovery
- Call from regulator or law enforcement

First Response

Forensic Investigation and Legal Review

- Forensic tells you what happened
- Legal sets out options/obligations

External Issues

- Public Relations
- Notification
- Remedial/ Service Offering

Long Term Consequences

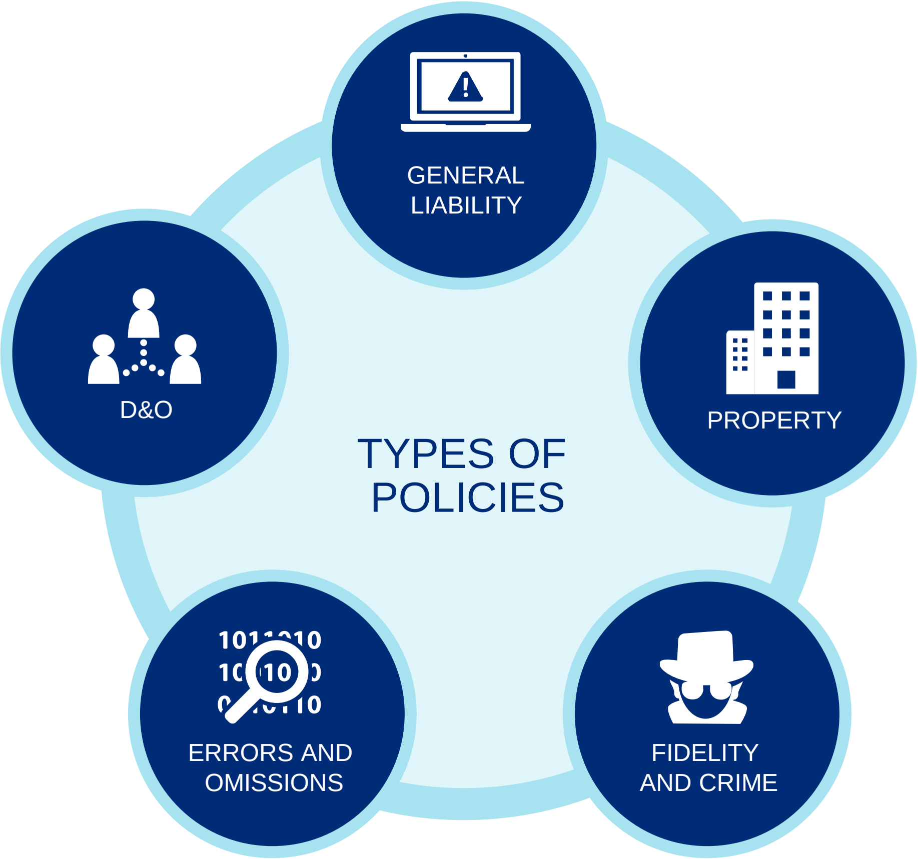
Forensic Investigation and Legal Review

- Forensic tells you what happened
- Legal sets out options/ obligations

Insurance Overview & Coverage Nuances

DESIGNING AN OPTIMAL & EFFECTIVE RISK MANAGEMENT PROGRAM

UNDERSTANDING THE GAPS IN COVERAGE



Insurance Coverage Gap Analysis

Privacy & Cyber Perils	Property	General Liability	Fidelity Bond	Computer Crime	E&O	Special Risk (KRE)	Broad Privacy & Cyber Policy
Destruction, corruption or theft of your electronic information assets/data due to failure of computer or network.	🟨 Becoming less available	🟥	🟥	🟨	🟥	🟨	🟩 Information asset protection
Theft of computer system resources.	🟨 Becoming less available	🟥	🟥	🟨	🟥	🟥	🟩 Information asset protection / crypto-jacking - sublimit
Business Interruption due to a material interruption in an element of your computer system due to failure of computer or network security (including extra expense and forensic expenses).	🟨 Becoming less available	🟥	🟥	🟥	🟥	🟨	🟩 Network Business Interruption
Business interruption due to your service provider suffering an outage as a result of their security failure or system failure	🟨 Becoming less available	🟥	🟥	🟥	🟥	🟥	🟩 Network Business Interruption (sublimitted or expanded based upon risk profile)
Indemnification of your notification costs, including credit monitoring.	🟥	🟥	🟥	🟥	🟥	🟥	🟩 Privacy Liability
Defense of regulatory action due to a breach of privacy regulation.	🟥	🟥	🟥	🟥	🟥	🟥	🟩 Privacy Liability
Coverage of Fines and Penalties due to a breach of privacy regulation.	🟥	🟥	🟥	🟥	🟥	🟥	🟩 Privacy Liability (where insurable by law)
Social Engineering Fraud	🟥	🟥	🟥	🟨	🟥	🟥	🟨 Cyber-Crime

🟥 Not Covered

🟩 Covered

🟨 Dependent upon specifics of claims, may not be covered

*For discussion and general information purposes only. Specific coverage details may vary.

Cyber Risk: Potential Costs & Liability

- How does a stand-alone cyber policy protect your company?

First Party

Data Breach Response
Data Restoration
Network Business Interruption
Security and Privacy Liability
Cyber Extortion

Third Party

Privacy Liability
Network Security Liability
Privacy Regulatory Defense Costs
Contingent Business Partner
Media Liability
Contingent Injury/Property Damage

Loss or damage to reputation

Legal liability to others for computer security breaches

Extra expense to recover/respond to a computer attack

Legal liability to others for privacy breaches of confidential information

Loss of revenue due to a computer attack

Costs to investigate and notify others of a breach

Loss of damage to data/information

Regulatory actions, fines and scrutiny

Electronic content

Cyber-extortion

Cyber-terrorism

Other Key Cyber Coverage Considerations

- **Additional Important Coverage and Placement Considerations**
  - Contingent Business Income Loss Reputational Based Income Loss
  - Voluntary Shutdown Coverage
  - Digital Data Restoration / Recovery
  - Regulatory Environment (GDPR / CCPA / BIPA / etc.)
    - Consumer Privacy Laws: Unlawful collection, retention, failure to remove; disclosure language absent a security breach
    - Does regulatory coverage extend to industry enforcement agencies
    - TCPA / CAN-SPAM exposure (defense & indemnification coverage; subject to AP, sublimit)
  - Bricking / Computer Hardware Replacement Coverage
    - Computer System Definition extends to ICS/SCADA especially for mfg; BYOD considerations
  - Contingent Bodily Injury / Property Damage Liability & First Party BI/PD
  - Invoice Manipulation Coverage
  - Crypto-Jacking / Utility Fraud
  - Betterment Coverage
  - Incidental Hospitality Technology Services (such as Wi-Fi offering; applicable for retail, hospitality, education, etc.
  - Silent / Non-Afifrmative Cyber - Coordination with Crime / K&R / Property Policies
    - Primary vs. Excess
    - Recognize erosion of deductible
    - Gap/Fill-in Policies with Property (Arceo; Amwins/C&F Cyber Risk Umbrella)
  - War Exclusion – Kinetic War; Ensure Cyber Terrorism carveback extends to Outsource Service provider
  - Claims Handling Experience & Reputation
  - Carrier Loss Mitigation Services – Request carrier onboarding call where applicable

Loss Mitigation Services

- **Loss Mitigation Services are commonly offered from leading carriers and MMA to improve an insured's security posture and risk profile. Examples of such services are below:**
  - Employee awareness training and phishing simulations
  - Blacklist IP Blocking and Domain Protection
  - Infrastructure Vulnerability Scan
  - Endpoint Detection and Response
  - Vendor Risk Management
    - Security ratings
    - Contract guidance / language best practices
  - Onboarding orientation risk planning session with legal breach coach / forensic / PR firms
  - Incident Response / Business Continuity Planning Seminar
  - Information Security Best Practices Seminar
  - Table Top Exercise / Mock Incident Simulation
  - Limit Adequacy Modeling, Benchmarking & Analytics ("Understand, Measure, Manage")

Questions

Dan.Hanson@marshmma.com
612-387-7315
Mario.Paez@marshmma.com
651-900-3771