



Cyber Liability in an Evolving World

**2022 Firearm Industry
Compliance Webinar Series**





HYLANT

Cyber Liability Insurance

Alex Clark

Vice President, Cyber Practice Leader

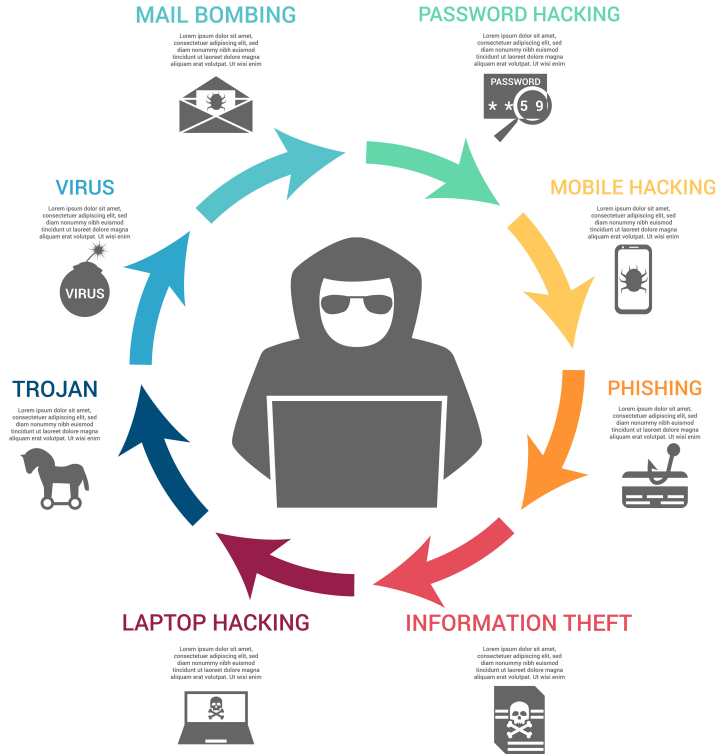
alex.clark@hylant.com 765-714-9123



State of the Cyber Market

- ❑ Every 11 seconds a new company is hit by ransomware
- ❑ The average ransomware payment is \$300,000 up 45% from a year ago
- ❑ Ransom payments account for only 10 to 15% of the total incident
- ❑ 207 Days is the average time to identify a breach
- ❑ 21 days is the average downtime caused by a ransomware attack

State of the Cyber Market



- Who is attacking you?
 - Cyber Gangs
 - Nation State Actors
 - Rogue Employees
 - Political Activists (Hacktivists)

Yelp Reviews?
Good or Bad Actors?
Why aren't they punished?
Should we pay or not pay?

What is Cyber Insurance?

First Party

- Cyber Incident Response
- Breach Consultation
- Data Forensics
- Public Relations
- PCI Expenses
- Network Extortion
- Data Restoration

Third Party

- Network Security and Privacy Liability Coverage
- Media Liability Coverage



State of the Cyber Market

Industry Underwriting

Manufacturing, Retail, Education, Healthcare, Law firms, Public Entity, Tech Firms

Controls

MFA, Backups, Employee Training, Endpoint Detection and Response, End of Life Technology, Patch Management

Coverage Trends

Restriction of Ransomware Coverage (including co-insurance and sub-limits)

Shrinking Capacity

Many primary \$10 million limits are being split into smaller layers

Pressure on rates and retentions for all industry classes, sizes, and loss history



Insurance Program

CYBER SECURITY LIABILITY

Coverage Limits:

Insuring Agreements	Per Loss or Claim Limit of Liability	Premium
A. Loss of Digital Assets	\$ 1,000,000	\$ 824.00
B. Non-Physical Business Interruption and Extra Expense	\$ 1,000,000	\$ 1,670.00
C. Cyber Extortion Threat	\$ 1,000,000	\$ 1,236.00
D. Security Event Costs	\$ 1,000,000	\$ 2,826.00
E. Network Security and Privacy Liability Coverage	\$ 1,000,000	\$ 3,476.00
F. Employee Privacy Liability Coverage	\$ 1,000,000	\$ 659.00
G. Electronic Media Liability Coverage	\$ 1,000,000	\$ 1,978.00
H. Cyber Terrorism Coverage	N/A	N/A
Special Expenses Aggregate Limit	\$ 1,000,000	
Customer Notification Expenses Sublimit	\$ 500,000	
Public Relations Expenses Sublimit	\$ 500,000	
POLICY AGGREGATE LIMIT OF INSURANCE: \$ 1,000,000		

Deductibles, Coinsurance and Time Retention:

Insuring Agreements	Deductible	Coinsureance	Time Retention
A. Loss of Digital Assets	\$ 10,000	N/A	N/A
B. Non-Physical Business Interruption and Extra Expense	N/A	20%	24 hrs
C. Cyber Extortion Threat	\$ 10,000	N/A	N/A
D. Security Event Costs	\$ 10,000	N/A	N/A
E. Network Security and Privacy Liability Coverage	\$ 10,000	N/A	N/A
F. Employee Privacy Liability Coverage	\$ 10,000	N/A	N/A
G. Electronic Media Liability Coverage	\$ 10,000	N/A	N/A
H. Cyber Terrorism Coverage	N/A	N/A	N/A
Special Expenses	N/A	20%	N/A

Claims Made Dates (Applicable only to the following):

Insuring Agreements	Continuity Date	Retroactive Date	P/P Litigation Date
E. Network Security and Privacy Liability Coverage	02/06/2021	02/06/2021	02/06/2021
F. Employee Privacy Liability Coverage	02/06/2021	02/06/2021	02/06/2021
G. Electronic Media Liability Coverage	02/06/2021	02/06/2021	02/06/2021

- \$500k sublimit for notification and public relations
- Business interruption with 20% co-insurance
- Retro dates limiting coverage
- No Cyber Crime
- No Hardware Replacement
- No Cyber Terrorism Coverage



Business Operations

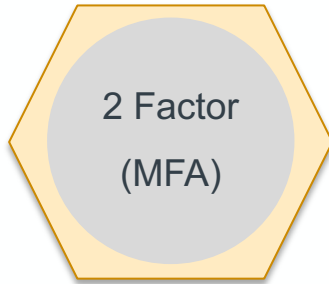
- What percentage of company's revenue is generated by web application services? Do we depend on web application services?
- International? Employees. Distribution. Sales.
- Third Parties? Do they have access to corporate networks?
- Third Parties? What level of dependency?
- Does your company have access to private information?
- Information Technology vs Operational Technology



I take cyber security very seriously.



“No Longer Business Name and Revenue”



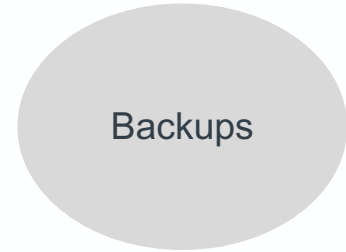
Remote access to network
Remote access to e-mails
Privileged users



Every Employee
Risk Manager
Head of IT
Cyber Response Team



End Point Detection
End of Life Software
Patching Cadence



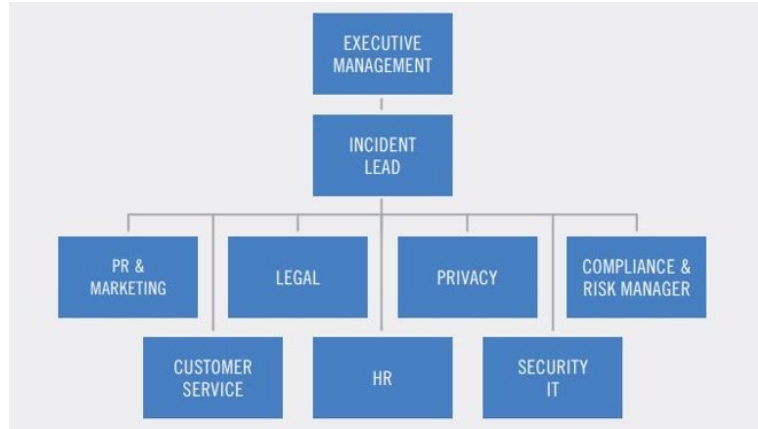
Process, Frequency
Testing
Infrastructure – domain controller
Segmented, Air-Gapped
Time to restore from backups

Depending on applications can backfire



Prepare: Cyber Risk Readiness

Response Team



1. Do we know our panel providers?
2. Who can approve a ransom demand?
3. Dedicated person to log and keep track of Scope of Works
4. How and when do we report a claim?

Response Model





The 5 Puzzle Pieces of a Cyber Renewal



Evaluate: Fact Finding and Risk Profiling



Quantify: Exposure Understanding



Transfer: Insurance Procurement



Prepare: Cyber Risk Readiness



Test: Tabletop Exercises and Training



HYLANT

Cyber Liability Insurance

Alex Clark

Vice President, Cyber Practice Leader

alex.clark@hylant.com 765-714-9123

Dan Silvers

Client Executive

dan.silvers@hylant.com 419-699-1489

Additional NSSF Compliance Resources

NSSF[®]
The Firearm Industry
Trade Association

SHOT
UNIVERSITY[™]

NSSF[®] online

Industry Compliance Courses:

- “Zero Tolerance” Policy
- Winning at ATF Inspections
- Completing the Form 4473
- Multiple Sales Report
- and more

