Brown & Brown

Coalition

Cyber Security In Construction

What you need to know

Presented by:

Sam Jones, MLIS
Brown & Brown

Katie Fairhart, CIC, MLIS
Coalition Insurance

Presentation Agenda

1. What is Cyber Insurance?
2. Buying Cyber Insurance
3. Cyber Claims Examples
4. Tools to Protect Your Business

01

What Is Cyber Insurance

Modern Cyber Risk

Setting the Stage for Cyber Exposure

- Internet of Things – IOT
  - » Devices, Data Phones, iPads, Laptops, etc.
- Everyone in the world works on the same programs
  - » Google, Facebook (Meta), Apple, Microsoft, etc.
- Low Barrier to Entry for Technology Use
- Cost & Convenience of “simply” plugging in Software
- Offsite or remote working
- How often do you ask, “should we be hooking these devices to the internet?”

A Growing Problem

Types of Cyber Attacks

Common Attacks

- Business Email Compromise
- Social Engineering – “Hacking People”
- Malware
- Phishing
- Ransomware a.k.a “Cyber Extortion”

Coverage Types

13 Key Insuring Agreements	
Coverage Type	Insuring Agreement
First-Party/Post Breach Response Coverage	1. Privacy Notification and Crisis Management Expense
Third-Party/Liability Coverages	2. Information Security and Privacy Liability 3. Regulatory Defense and Penalties 4. Payment Card Industry Fines and Assessments 5. Website Media Content Liability 6. Bodily Injury and Property Damage Liability
First-Party/Time Element Coverages	7. Business Interruption 8. Extra Expense
First-Party/Theft of Property Coverages	9. Data Assets 10. Cyber Extortion 11. Computer Fraud 12. Funds Transfer Fraud 13. Social Engineering/Fraudulent Instruction Coverage

Exhibit 8.1 “IRMI Cyber & Privacy Liability Exposures and How to Insure Them”

What does cyber insurance cover?

Breach Response Costs

Legal fees, forensics, PR, credit monitoring, etc.

Cyber Extortion

aka Ransomware

Stolen Funds

Lost Business Income

Computer Replacement

Technology Failures

02

Purchasing Cyber Insurance

Insurance Markets

ADMITTED INSURER

Pros:

- Meets the regulation requirements by the States “Department of Insurance (DOI)”.
- No fees or Taxes.
- Premiums, Rates, and Policies are reviewed and approved within the states guidelines.
- Policy is backed by the State if Insurer goes insolvent.

Cons:

- Admitted policies often have limited coverage options
- Narrower underwriting capability
- More likely to Non-Renew if exposures change dramatically

NON-ADMITTED INSURER

Pros:

- Broader, and Less restrictive coverages.
- More customizable and specific coverages for “Hard to Place” risks.

Cons:

- The insurer or specific policy may not comply the “States Insurance Regulations”.
- If insurance company goes insolvent, there is no guarantee that claims will be paid.
- No ability to appeal to the State for help with payment.

Hardening Market

Premium

- Increases of 100%+ have become the baseline.
- Not uncommon for 300% increases with no material changes in exposure.
- Expect further increases for accounts with recent losses or less than fully mature IT Security Controls

Retentions & Co-Insurance

- Retention Increases of up to 1,000%
- Markets requiring co-insurance & sub-limits for ransomware and contingent BI
- Waiting periods going from Hours to Days

Coverage

- Media, wrongful collection of information, biometrics, and contingent business interruption coverages are being limited
- Outside of scope coverages are outside of pure cyber have started to be restricted.

> “Insureds renewing in Q1 2022 should expect premium increases beginning in the 100% range and will need to work closely with their chief information security officers and IT security professionals to address concerns of underwriters.”

Brown & Brown Cyber Market Update
Q1 2022

Coalition is insurance built to solve cyber risk

Coalition launch 1/1/18
520+ EE's across 5 countries
Insurance & tech veterans

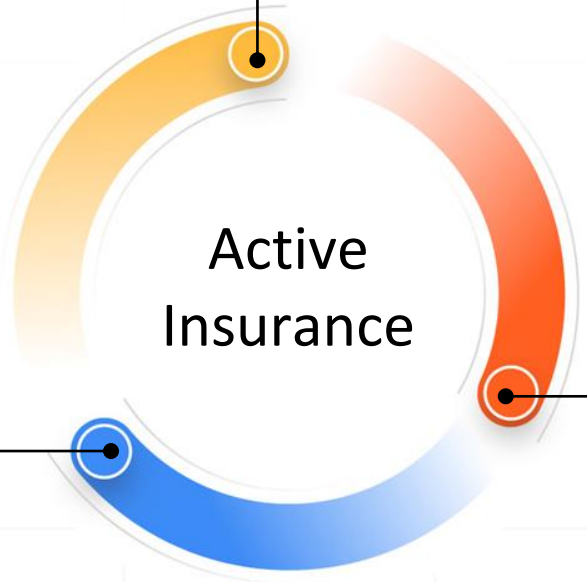
$250M+ GWP
25,000 Policyholders
48 trillion scans annually

Respond to business-halting threats with record speed

Active Protection
Active Response
Active Risk Assessment

Active Protection

Monitoring and alerting to identify and prevent risk before it escalates



Active Risk Assessment

Underwriting, quoting, renewals, and digital risk scores powered by real-time data

Active Response

In-house resources that accelerate response and coverage if an incident occurs

03

Cyber Claim Examples

- Cyber crime is increasing like never before – the business of cyber crime has shifted
- Ransomware is growing in severity - *Average ransom demand made to our policyholders in the second half of 2021 was* ***$1.8 million***
- Criminals are taking advantage of dislocation in how we work - *The average funds transfer fraud loss increased 78% from 2020 to 2021 to* ***$347,000.***
- **Small businesses are disproportionately impacted** – claim severity rose 56% for organizations under $25M in revenue increasing to $149,000.

The average ransom demand increased 20% to $1.8M

Ransomware Basics

- A ransomware infection involves some or all of the files on a computer becoming inaccessible
- The malicious actor leaves behind a way to contact them to get the data back. Usually this is in the form of a ransom note.
- The visual appearance of ransomware attacks can vary
- Without a solid backup solution, many victims have to entertain the possibility of paying the malicious actor for their data
- The preferred currency for attackers is Bitcoin (BTC)

04

Tools For Protecting Your Business

Best Practices

Enable Multi-factor Authentication (MFA)

- MFA is an authentication method that requires user to provide two or more verification factors to gain access to a resource or account.

Patch Old Vulnerabilities

- Microsoft Server Patches
- Log4J
- Sonicwall Updates

Ensuring Passwords are Strong

- Don’t use the same password for all your accounts.
- It is very likely your “go-to” password has been picked up in a breach at some point.

Maintain Offline and Immutable Back-Ups

- Don’t presume you onsite Microsoft Server is safe.

> “Enabling multi-factor authentication makes you 99% less likely to get hacked.”

Jen Easterly
Cybersecurity & Infrastructure Security Agency (CISA) Director

What can you do to protect your business?

Increase email security	Implement multi-factor authentication (MFA)	Backup your data	Enable secure remote access	Update your software
Use a password manager	Scan for malicious software	Encrypt your data	Implement a security awareness training program	Purchase cyber insurance