CYBER2021:
Cyber Risk and Insurance for Engineering Professionals
Table of Contents

1. The Most Common Types of Cyber Crime
2. Claims trends in a year of remote working and virtual meetings.
3. How to protect yourself?
4. What coverages are included in cyber insurance?
5. What is different about the ACEC cyber offering and Coalition?
6. What are the steps to getting a Cyber Risk Assessment and Quote?
3 Most Common Types of Cyber Crime

- Ransomware
- Funds transfer fraud
- Business email compromise
Cyber claims by the numbers
Cyber claims by the numbers

Coalition policyholders experience less than one-fourth the frequency of claims as of the rest of the market, due in no small part to our differentiated approach to underwriting and risk management.

Annualized Claims Frequency vs. Market

Market Frequency | Coalition Claims Frequency
---|---
2018: 4.7% (1.3%) | 2019: 6.2% (1.5%) | 2020 YTD: 1.6%

*Average market frequency based on data reported to the NAIC for all US standalone cyber policies written by US insurers. 2020 NAIC data is not yet available.
Ransomware, FTF and email compromise account for 87% of reported claims

Most common cyber incidents (% of reported claims)

- Ransomware: 41%
- Funds transfer fraud: 27%
- Email compromise: 19%
- Other: 13%

Majority of losses were picked up by three of the coverages on our policy: breach response coverage (forensics and IR), cyber extortion costs (following ransomware), and funds transfer fraud (resulting, largely, from social engineering).
Ransomware, FTF, and Email incidents account for the majority of claims

% of Claims by Category

- Ransomware: 45%
- Funds Transfer Fraud: 26%
- Business Email Compromise: 19%
- Other: 10%

90%
Phishing, remote access, and social engineering account for 89% of attack techniques.
Ransomware
Ransomware claims

Average ransom demand by malware strain

Average ransom demand

EFFECTS OF COVID-19

47%

Percentage increase in the severity of ransomware attacks from Q1 to Q2 2020
Case Study: Ransomware

WHAT HAPPENED? Essential working entity, with food supplier. CEO arrived at work to find all machines encrypted. Bad actor informed of exfiltration of data. Timeline given: No payment in 3 days will disclose the breach. No payment in 5 days will release the data.

COALITION ACTIONS The Coalition claims team contacted the Insured within minutes of receiving notice from broker. Performed immediate triage which including identifying and removing the point of entry (RDP.) Discussed next steps that included retention of counsel, forensics, verification of back-ups, potential payment of ransom. Within 5 minutes of initial notice, counsel was on the phone with insured and their IT firm. Back-ups were not viable and ransom negotiation started. Ransom paid and decryption occurred.

POST-BREACH ACTIONS Worked with insured to remove remote desktop protocol which was the access point. Discussed being a target watch for suspected FTF moving forward and implemented Funds Transfer SOP.
Funds transfer fraud
Funds transfer fraud claims

Percent of incidents where Coalition has recovered funds
- 45% Cases with no recoveries
- 55% Cases where we recovered funds

Percent of funds recovered by Coalition
- 16% Non-recovered funds
- 84% Recovered funds

39%
Percentage increase in the frequency of funds transfer fraud attacks from 2019 to 2020
Case Study: Funds Transfer Fraud

April 8, 2020
Fraudulent Email Received
Non-profit entity received wire change instructions from another entity. Unfortunately, it was from a spoofed email.

April 9, 2020
Insured Changed Wire Instructions
In accordance with the fraudulent email, our Insured changed the wiring instructions. Payment was processed on April 10th, 2020, sending $1.3M to the bad actor.

April 13, 2020
Insured Called Coalition
Within 5 minutes of receiving a call, Coalition’s team initiated clawback of funds and began work with counsel and forensic investigation. Initial security discussion with insured.

April 21, 2020
Funds Recovered!
Coalition was able to recover all but $500 of the $1.3M originally lost.

April 22, 2020
Security Discussion with Coalition
Coalition discussed with insured improvements to security for email (2fa) and funds transfer standard operating procedure.
Business email compromise
Business email compromise claims

60%
Percentage of claims reported to us where business email compromise was the initial point of entry

3.2x
Organizations that use Microsoft Office 365 are more than three times as likely to experience a business email compromise when compared to Google Gmail

67%
Percentage increase in the frequency of business email compromise attacks from 2019 to 2020
Recommendations to solve cyber risk
Recommendations to solve cyber risk

**Multi-factor Authentication**
Turn on multi-factor authentication (MFA) for all business-critical services including corporate email accounts, VPNs, financial accounts, and any other application where sensitive information is stored.

**Email Security**
Implement basic email security measures including SPF, DKIM, DMARC, and an anti-phishing solution. Email is the single most targeted point of entry into an organization for a criminal hacker.

**Routine backups**
Regularly back up your systems and information, and store backups in an “offsite” location. Offsite doesn’t have to mean physically offsite, but in a location that is not connected to your main business network.

**Wire Transfer Verification**
Implement a dual-control process when making funds transfers. Today, it is no longer safe to assume that email is a secure means of communication. Call the intended recipient of the transfer before you make it to confirm any changes.

**Password Management**
Encourage employees to use a password manager (e.g., Lastpass, 1Password, or the password managers built into web browsers like Chrome or Safari). Using strong, unique passwords for each of the services you use can help prevent claims.
Three easy tips, all free to implement!

**#1**
Multi-Factor Authentication
- Free to use with most email providers (Gmail, Outlook, etc.)
- Easy to implement
- MFA endorsement - expanded coverage for good security!

**#2**
Funds Transfer Standard Procedures
- All wire changes should be treated as suspect
- Do not rely upon the email request alone
- Call back provision to the last known phone - NOT the phone on the email

**#3**
Remove RDP (or put behind a VPN)
- VPN or Access management Tools (such as Cloudflare Access)
- Remember - not everyone needs remote access!
Cyber Insurance
Differentiated Coverage

Insuring cyber as a peril; innovative coverage tailored for SMBs

- Closing gaps across commercial insurance policies
- Unique underwriting capabilities and expertise for high risk industries (e.g., ICS/SCADA, crypto, etc.)

Unlike most insurance markets, coverages and premium are directly tied to risk exposure

- Enhanced business interruption waiting period when using an approved DDoS mitigation provider
- Only cyber market to use specific equipment exclusions to carve out exposure to risk configurations
Coverages Offered

- Network & Information Security Liability
- Regulatory Defense & Penalties
- Multimedia Content Liability
- PCI Fines & Assessments
- Bodily Injury & Property Damage
- Technology Errors & Omissions
- Pollution
- Computer Replacement
- Funds Transfer Fraud
- Service Fraud
- Digital Asset Restoration
- Business Interruption & Extra Expenses
- Cyber Extortion
- Breach Response
- Crisis Management & Public Relations
Coalition Overview

Secret master plan + business & performance program
Coalition is an insurance-driven technology company that keeps businesses safe.

**WHO WE ARE**

Coalition is an insurance-driven technology company that keeps businesses safe.

**PRODUCT LAUNCH**

January 1, 2018

**CARRIER PARTNERS**

Swiss Re, LLOYD’S, Arch, Argo PRC

**CURRENT PROGRAMS**

Cyber primary & excess up to $1B revenue in the US and Canada

**RUN-RATE PREMIUM**

$150 M (244% YoY growth)

**CUSTOMERS**

14,000+ policyholders

26,000+ SaaS users

**PLATFORM**

48 trillion scans annually

**TEAM**

- 160+ employees across 5 countries
- Deep bench of insurance & tech veterans

**FUNDING**

$125 M

Ribbit Capital, Valor Equity Partners, Felicis Ventures
This data is the foundation of the cyber risk assessment
Our in-house risk management team delivers fast and differentiated support

**Claims Team**

- Average response time under 5 minutes
- Customer advocate throughout the incident process
- Partnerships with financial institutions and law enforcement
- Clawed back 65% of all funds lost by our customers

**Coalition Incident Response**

- Pre-breach incident remediation available for free to all customers
- Contained 45% of all reported incidents before eroding policy limits
- In-house forensics capabilities ensures speedy response and remediation
Thank you!

Brian Specht
Business Development
(718) 753-6016
brian@coalitioninc.com

Rich Gatz, Esq. FIP
Claims Counsel
(630) 445-3187
rich@coalitioninc.com
Top 10 cybersecurity recommendations
1. Increase email security

- Despite popular belief, email is not a secure form of communication
- Business email compromise (BEC) was the initial point of entry for **54% of claims**
- Tactics to secure business email:
  - Implement SPF, DKIM, and DMARC
  - *Always* use MFA!

**VENDOR RECOMMENDATIONS**

**Email Hosting Provider**
- a platform that manages (aka “hosts”) your email
  - Google
  - Microsoft 365

**Mail Proxy**
- a mail proxy sits in front of an ESP to filter out malicious emails
  - Proofpoint
  - Mimecast
2. Implement Multi-factor Authentication (MFA)

- MFA requires users to have a second form of authentication to access accounts, such as:
  - Digital token
  - SMS message

- Implement MFA on all business-critical systems: corporate email accounts, internal services, and third-party services

VENDOR RECOMMENDATIONS

Authentication app
- Authy from Twilio
- Google Authenticator
- Microsoft Authenticator

Authentication solution
- Duo Security
- Okta
3. Maintain good backups

- Backups help ensure organizations can recover quickly from ransomware attacks, which account for 41% of claims.

- Ways to maintain effective backups:
  - Regularly back up business-critical data
  - Maintain backups on- and off-site
  - Test your backups by trying a full recovery

VENDOR RECOMMENDATIONS
- Acronis
- Backblaze
- Carbonite
- Crashplan
- Datto
- iDrive
- Veeam cloud
5. Update your software

- All software presents at least some risk to your organization
- Cybercriminals look for weaknesses and flaws (vulnerabilities) that can be used to gain access to systems or spread malicious software
- As much as software engineers try, there are almost always security "bugs" that must be corrected (or patched) in an update

VENDOR RECOMMENDATIONS

**Attack Surface Monitor**
*Coalition’s proprietary platform*
- ASM provides continuous scanning and automated security alerts, at no additional charge for Coalition policyholders
6. Use a password manager

- Passwords grant access to the most private information your company deems critical
- Passwords need to be unique, strong, and updated regularly
- Password managers help keep track of multiple passwords and generate new ones at random

VENDOR RECOMMENDATIONS
- 1Password
- Dashlane
- Keeper
- LastPass (free with limited use)
7. Scan for malicious software

- Every device you use (personal phone, work phone, laptop, desktop, tablet, etc.) can create an open door for hackers to target your organization.

- The rise in the number of endpoints attached to the networks we use every day has led to an increased need for endpoint protection.

- Endpoint detection and response (EDR) is an emerging technology that addresses the need for continuous monitoring and response to advanced threats.

**VENDOR RECOMMENDATIONS**

**Antivirus**
- Emsisoft
- ESET
- Malwarebytes
- Webroot
- Windows Defender

**EDR**
- Carbon Black
- Comodo
- Endgame
- SentinelOne
8. Encrypt your data

- Encryption is the process through which data is encoded so that it's hidden from bad actors who manage to gain access.
- Physical damage and loss are *far cheaper* than the loss of sensitive data.
- Individual states and other regulatory bodies may require a base level of encryption.

**Encryption Best Practices**

- Require a passcode to unlock the phone.
- Require an "auto-locking" feature.
- Require mobile phones to leverage encryption when possible.
- Keep your operating system software up to date from authorized vendors (e.g., Apple, Android).
9. Implement a security training program

- **60%** of the claims we’ve witnessed have been the result of human error
- Every member of an organization is responsible for cybersecurity
- Cybercriminals rely on the manipulation of busy employees to gain access to a company’s networks and devices — making education critical

**VENDOR RECOMMENDATIONS**
- Curricula
- KnowBe4
- Proofpoint
- SANS Security Awareness
10. Purchase cyber insurance  ✔

- Even with the best security in place, mistakes and accidents happen
- Insurance helps you recover financially should the worst happen
- Our Security and Claims teams are here to help!

**COALITION OFFERS MORE THAN INSURANCE**

- Free ongoing security monitoring + alerts notifying you of any vulnerabilities we identify
- Access to our Security and Incident Response team to address security concerns
- Other benefits, including free limited access and exclusive discounts for security awareness training and ransomware prevention software