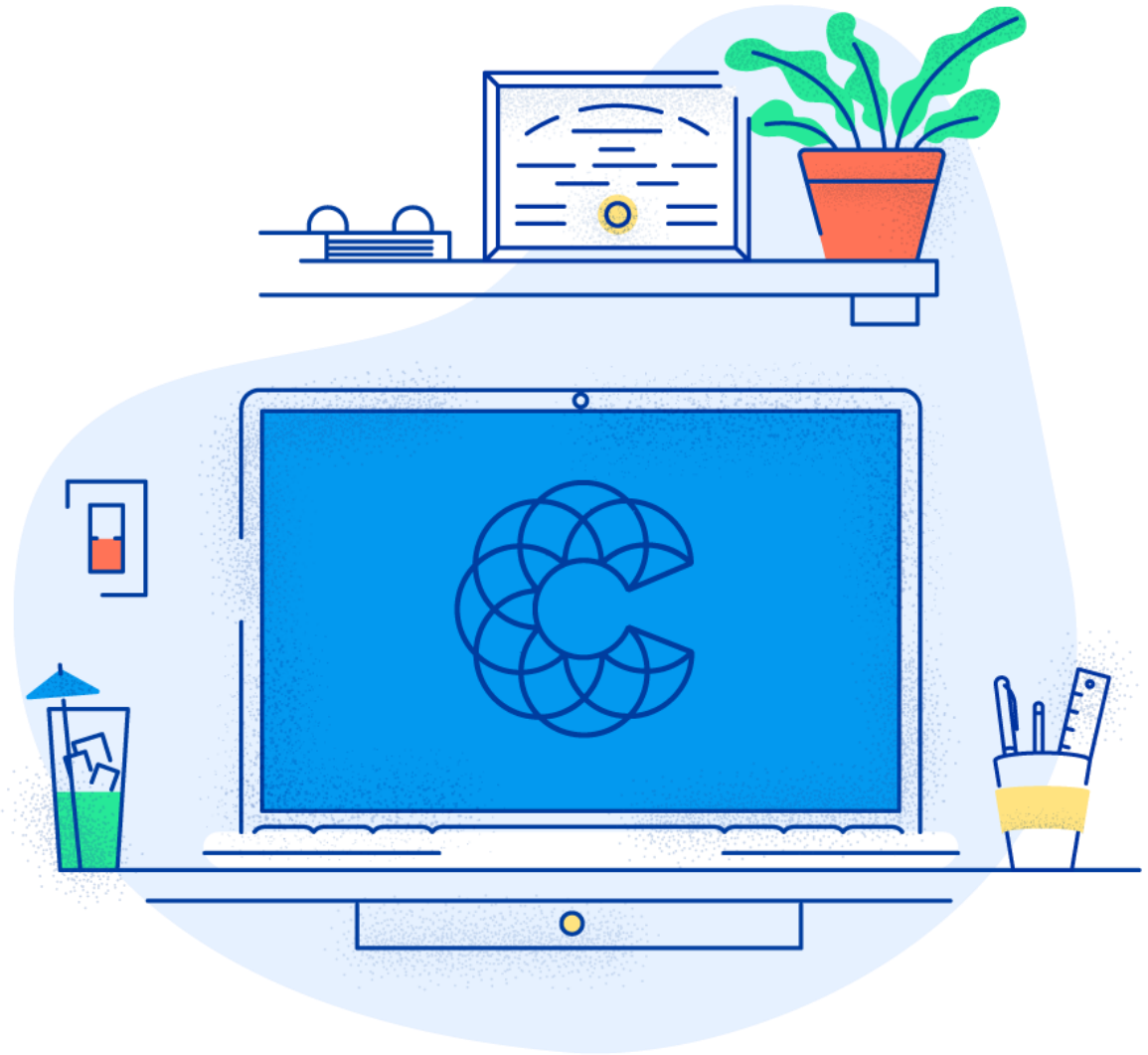
CYBER RISK, SOLVED.

COALITIONINC.COM

Coalition®

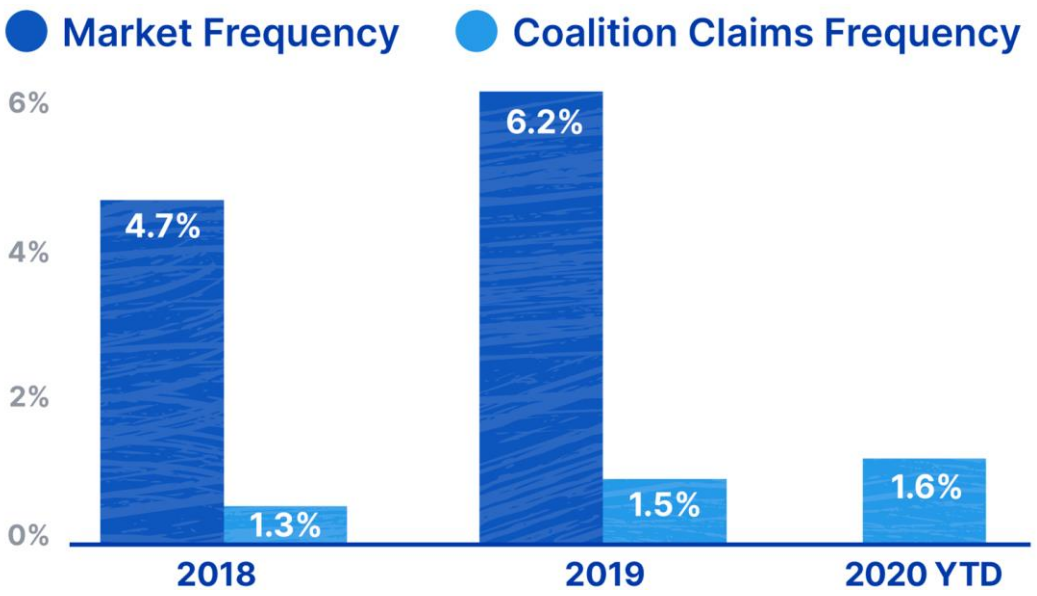
# Setting the stage

- Claims data comes from three sources: our own policyholders, market data (NAIC), and insurance applications
- Our underwriting and risk engineering capabilities are unique among cyber insurance providers, and our claims reflect this
- Rapid changes in technology, processes, and communications during COVID-19 has made organizations more exposed to  cyber threats



# Cyber claims by the numbers

## Annualized Claims Frequency vs. Market

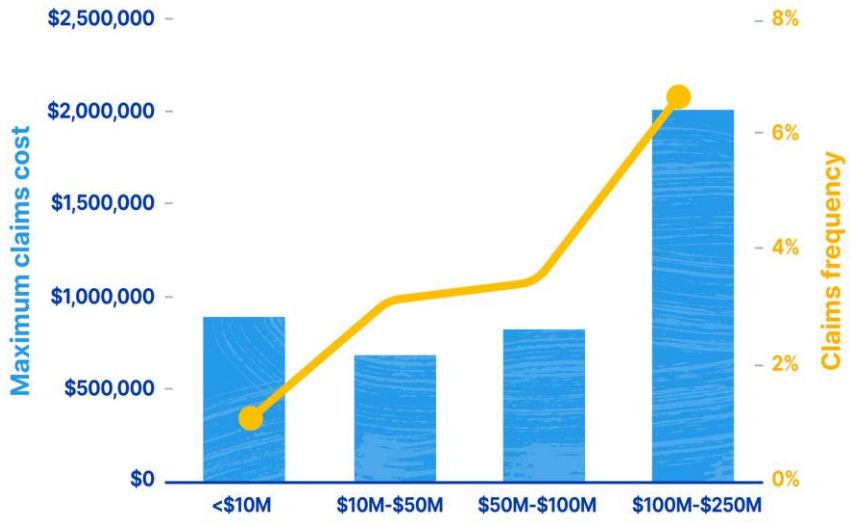



Coalition policyholders experience **less than one-fourth** the frequency of claims as of the rest of the market, due in no small part to our differentiated approach to underwriting and risk management.

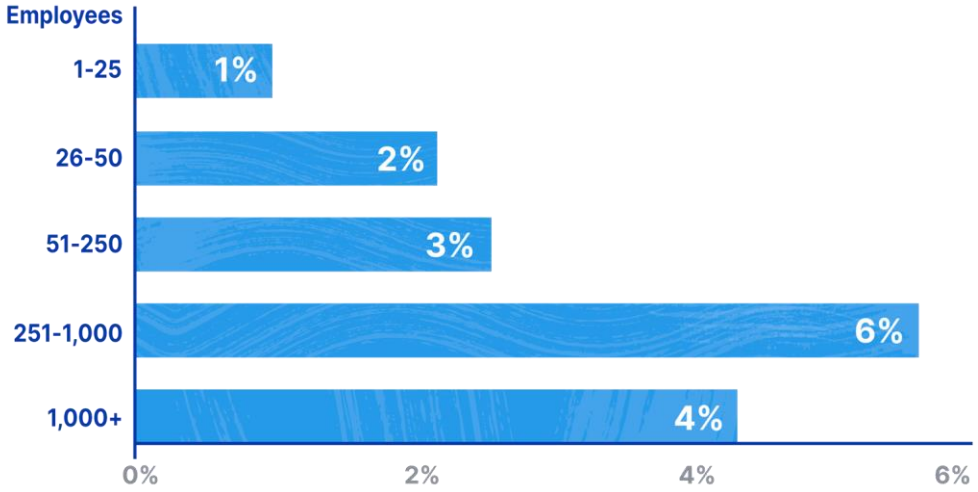
** Average market frequency based on data reported to the NAIC for all US standalone cyber policies written by US insurers. 2020 NAIC data is not yet available.*

# Claims by company size

## Claims trends by revenue band



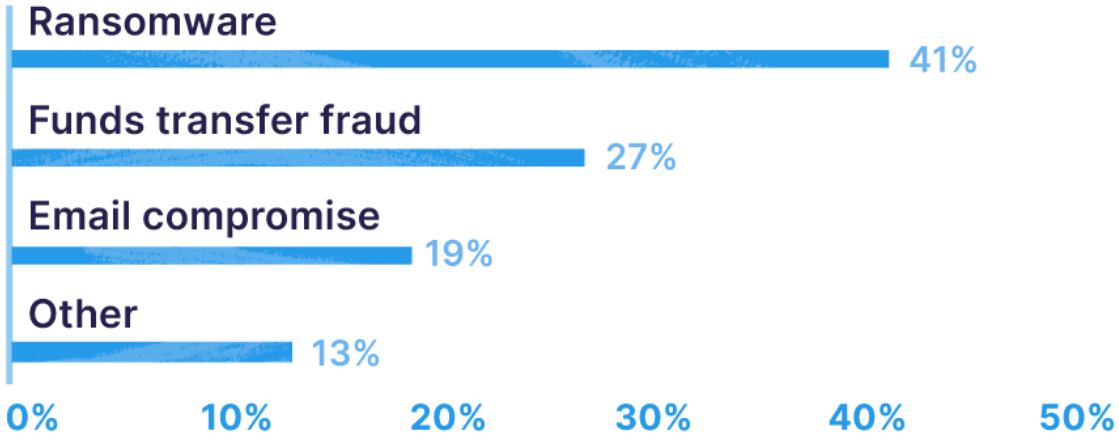

## Claims frequency by employee count



# Claims trends

# Ransomware, FTF and email compromise account for 87% of reported claims

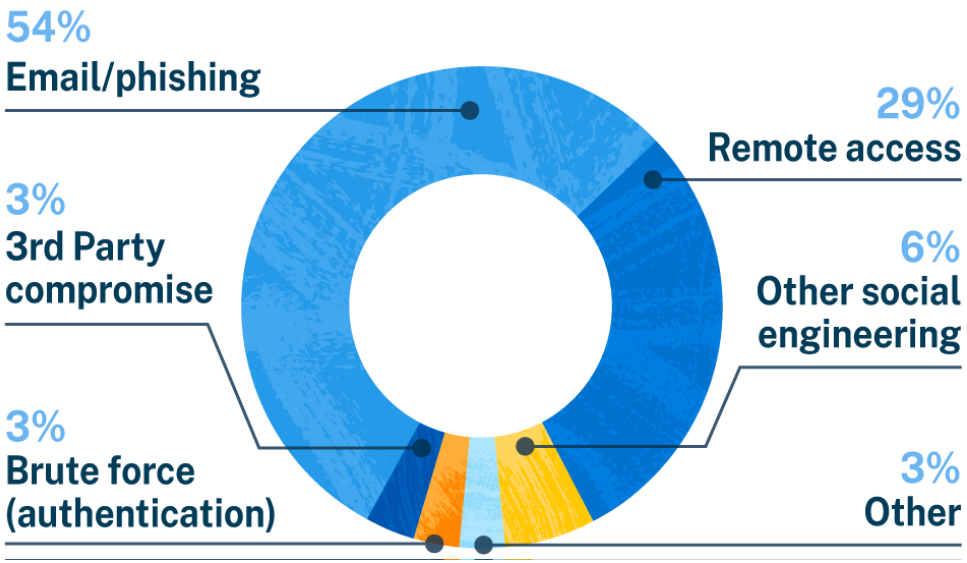
**Most common cyber incidents (% of reported claims)**




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).

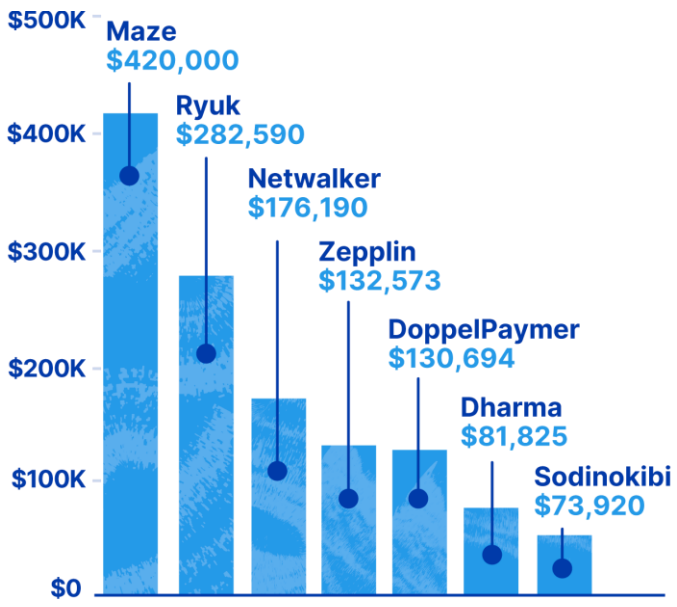
# Phishing, remote access, and social engineering account for 89% of attack techniques

## Percentage of claims by attack technique

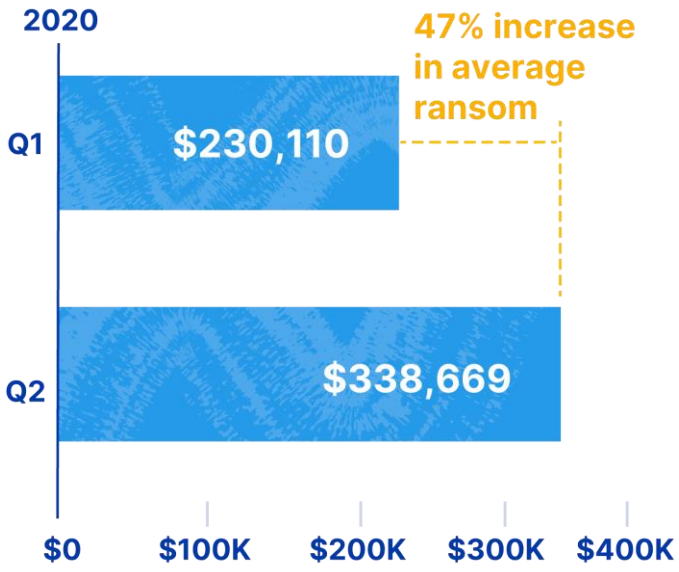


# Ransomware claims

## 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

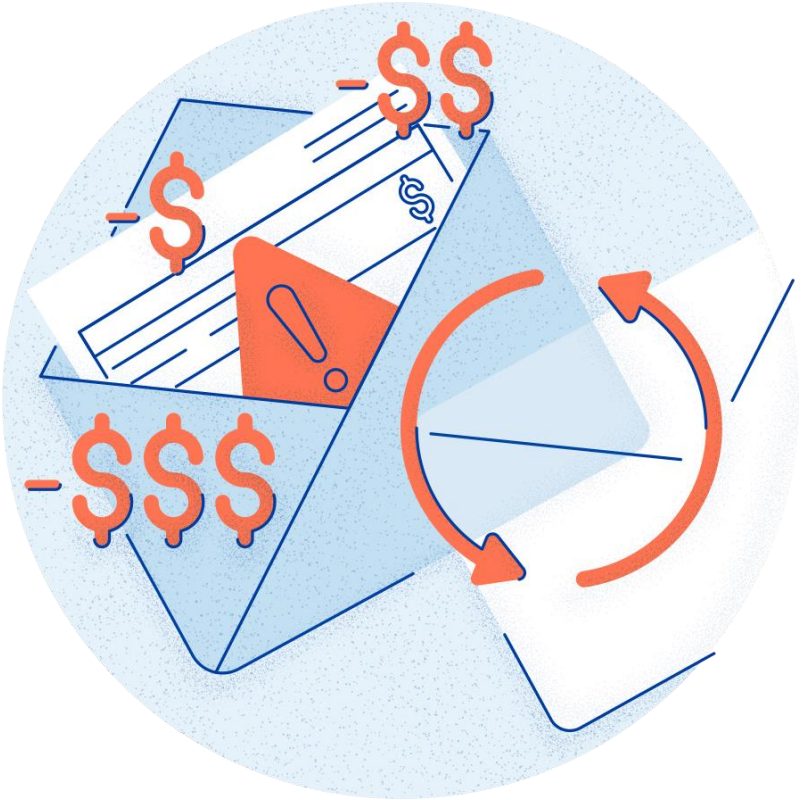
# Ransomware

# Case Study: Ransomware

WHAT HAPPENED? Essential working entity, 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.



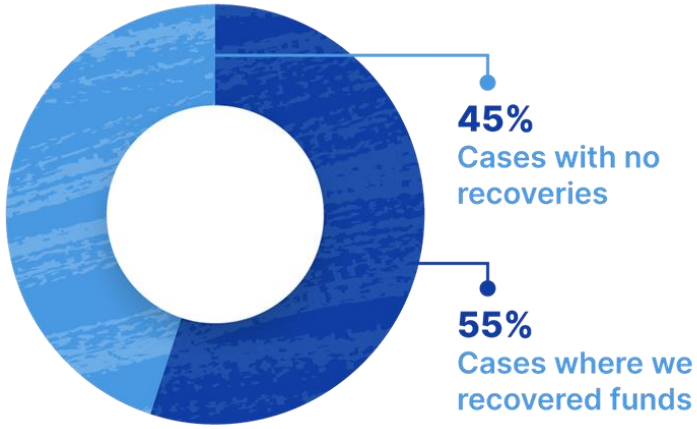
# Coverage

- 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

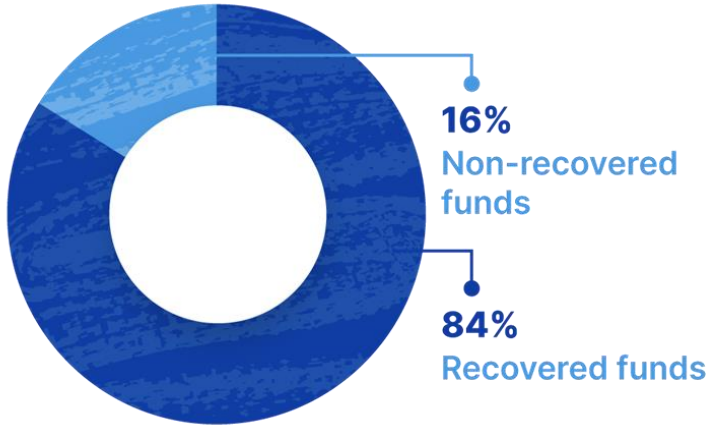
# Funds transfer fraud/BEC

# Funds transfer fraud claims

## Percent of incidents where Coalition has recovered funds




## Percent of funds recovered by Coalition




**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

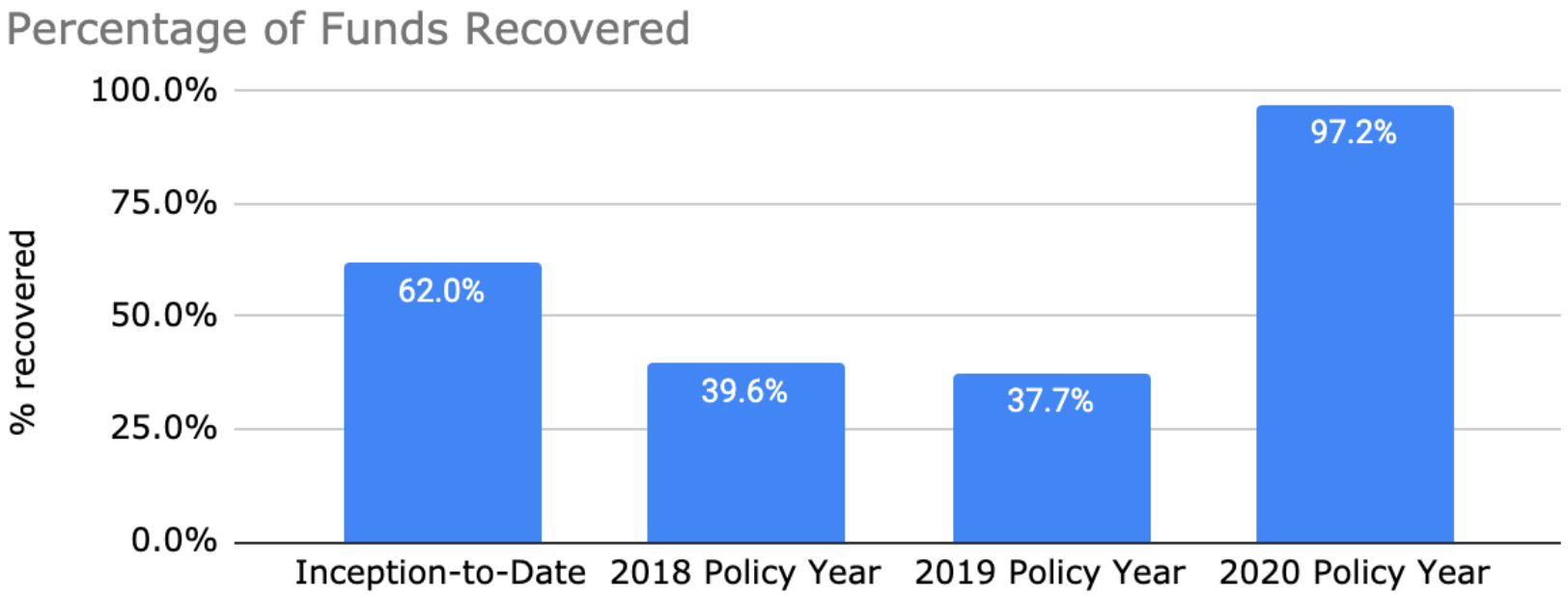
## Security Discussion with Coalition

Coalition discussed with insured improvements to security for email (2fa) and funds transfer standard operating procedure.

# Coverage

- 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

# Wired money to a criminal?
# Not to worry, we'll ~~pay~~ get it back!




*PS: we also pay back anything we can't recover!*

# The best solution is *prevention*

## Prevention:

1. Any new or change of payment request
2. Call last known phone number to validate the request
3. Avoid a fraudulent transfer!

## Recovery:

1. Call, email, or chat our claims team
2. Let Coalition use deep banking/security relationships to reverse transactions
3. File formal fraud report with the bank
4. Demand a clawback
5. Insist sending bank call receiving bank and freeze account and find out how much money in account;
6. IC3 and/or call FBI
7. Be the squeaky wheel
8. Investigate as to which entity at fault
9. Hopefully, get your money back!

# 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

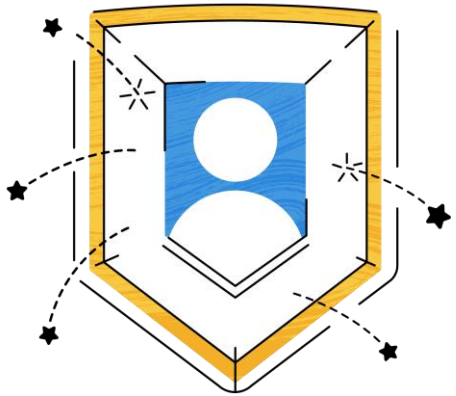
Regularly back up your systems and information, and store backups in an “offsite” location. Offsite doesn’t have to mean physically offsite, but in a location that is not connected to your main business network.

## 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.



# CYBER INSURANCE & RISK MITIGATION

## FOR THE INDUSTRIAL & MANUFACTURING INDUSTRY

Brought to you by

ISRI

Voice of the Recycling Industry™

# THE PARTNERSHIP

Through our membership with the National Association of Manufacturers, we now offer this exclusive cyber insurance and risk mitigation program for our members.

NATIONAL ASSOCIATION OF Manufacturers

AHT INSURANCE A BALDWIN RISK PARTNER

Coalition®

### MANUFACTURER ADVOCATE

Our work is centered around four values that make our industry strong and America exceptional: free enterprise, competitiveness, individual liberty and equal opportunity.

Representing 14,000 member companies—from small businesses to global leaders—in every industrial sector, we are the nation's most effective resource and most influential advocate for these values and for the industrial and manufacturing industry across the country.

### INSURANCE BROKER PARTNER

For more than 25 years, AHT's boutique Manufacturing practice has been nationally recognized as a leader in risk management and global machinery manufacturing. Led by a team of professionals spanning more than 50 years of combined industry experience, AHT is positioned to help manufacturers manage the unique risks they face.

### UNDERWRITER PARTNER

Backed by an A+ carrier, Coalition is the only provider offering an industry-leading policy that covers the unique exposures facing manufacturing firms. With Coalition, you get more than just insurance. Its technology platform delivers insurance plus proactive cybersecurity tools to keep your business safer, including risk management, security tools, incident response, claims and business recovery.

## NAM CYBER COVER

Cyber insurance and risk mitigation for manufacturers

# A TARGET ON YOUR BACK

> "The manufacturing and industrial industry are one phishing, ransomware, or industrial control system (ICS) incident away from exposure"

Manufacturing is the
**2nd most targeted industry**
for cyber attacks

**86% of cyber attacks**
against industrials are
deliberate, targeted attacks

The average claim size for
Coalition's SMB industrial
policyholders is **$130,000**

# WHAT IS NAM CYBER COVER?

**NAM Cyber Cover** brings the power of a leading cyber insurance provider, Coalition, together with a nationally recognized broker, AHT Insurance, to identify, protect and manage the unique exposures facing the industrial and manufacturing industry.

## MANAGE YOUR RISKS

A complimentary **Cyber Risk Assessment** allows you to see the weaknesses that exist as easy targets for a hacker.

**Patch manager** scans your systems for out-of-date software and weaknesses. Immediate alerts are sent when something unusual is found.

**Threat Monitor** constantly monitors for new outside risks and notifies you before damage can be done.

**60%** **of breaches** involved vulnerabilities for which **a patch was available but not applied**

**95** **Average number of exposed passwords** for small to midsize businesses

**$160,000** **Average loss from a ransomware attack** for a small business

# CYBER RISK ASSESSMENT

Cyber Risk Assessments are performed based on publicly available data

Coalition

GENERATED ON NOVEMBER 5, 2020

## Risk Assessment

PREPARED FOR

**Acme org.**

coalitioninc.com

## 1 Executive Summary

This assessment evaluates cybersecurity risk using data-driven, objective, and publicly available metrics together with Coalion's proprietary claims data. The findings and recommendations in this report are intended to help proactively identify, quantify, and manage cybersecurity risk. All findings can be investigated in greater detail using Coalition's BinaryEdge Security Platform.

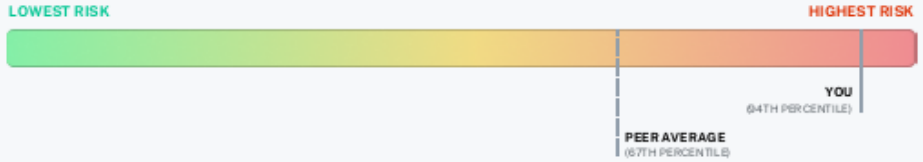
**Acme org.**

Domain: acme.com
Last scan: November 5, 2020
Revenue: $100,000,000

Industry: Financials
Employees: 150
Records: 0

**You rank in the 94th percentile of all Coalition policyholders**

Discovered vulnerabilities will not impact your coverage. However, resolving them may reduce your premium.




### Vulnerabilities by Criticality

Prioritized list of vulnerabilities we found on your assets. Critical vulnerabilities represent an active threat and should be remediated as soon as possible.

| CRITICAL RISK | HIGH RISK | MEDIUM RISK | LOW RISK |
|---|---|---|---|
| 1 | 0 | 20 | 6 |

### Detected Assets

Outside-in view of the Web properties we identified.

| DOMAINS | IPS | APPLICATIONS | SERVICES | HOSTING |
|---|---|---|---|---|
| 36 | 262 | 27 | 23 | 4 |

Request Your Cyber Risk Assessment Here

**How at risk are you?**

**What immediate vulnerabilities need to be addressed?**

# WHAT IS NAM CYBER COVER?

## MITIGATE THE SEVERITY

A training platform and simulated phishing emails help **train your employees to avoid mishaps**.

Enlist ethical hackers to find vulnerabilities in your systems with **Hacker One Response** – take that burden off your team.

**90%**

**OVER 90% of security incidents** are caused by human error

**1**

**1 vulnerability is all a hacker needs** to breach a business' defenses

NAM CYBER COVER

Cyber insurance and risk mitigation for manufacturers

# WHAT IS NAM CYBER COVER?

## RESPOND QUICKLY

Law enforcement capabilities can only go so far – that's where NAM Cyber Cover begins to respond

**Security & Incident Response Team**
available to you at no additional cost 24/7/365

- Get actionable recommendations
- Investigation, containment & remediation of security incidents
- Forensic collection, analysis, recovery & reporting

## RECOVER FROM AN ATTACK

Recovery is the key to survival of your business after an attack

- Recovery of lost data
- Ransomware negotiations, recovery & restoration of encrypted data to help restore your operations quickly and efficiently
- Assistance recovering stolen funds

# MEMBER BENEFITS

- **BROAD COVERAGE** tailored to the needs of the industrial and manufacturing industry
- **COMPLIMENTARY SECURITY TOOLS** that coordinate with your current technology solutions
- **BROADENED COVERAGE AND LIMITS** for being our association member
- **EDUCATION TOOLS AND SECURITY WEBINARS** for you and your key employees
- **PROGRAM PRICING DISCOUNT** for being our association member
- **911 COALITION** incident response
- **ACCESS TO UP-TO-DATE RESOURCES**
  - Webinars
  - Blogs
  - Case Studies
  - And more...

Get Your Complimentary Cyber Risk Assessment (CRA) Today

Request Your Cyber Risk Assessment Here

NAM CYBER COVER

Cyber insurance and risk mitigation for manufacturers