Coalition®

Coalition Team Bios

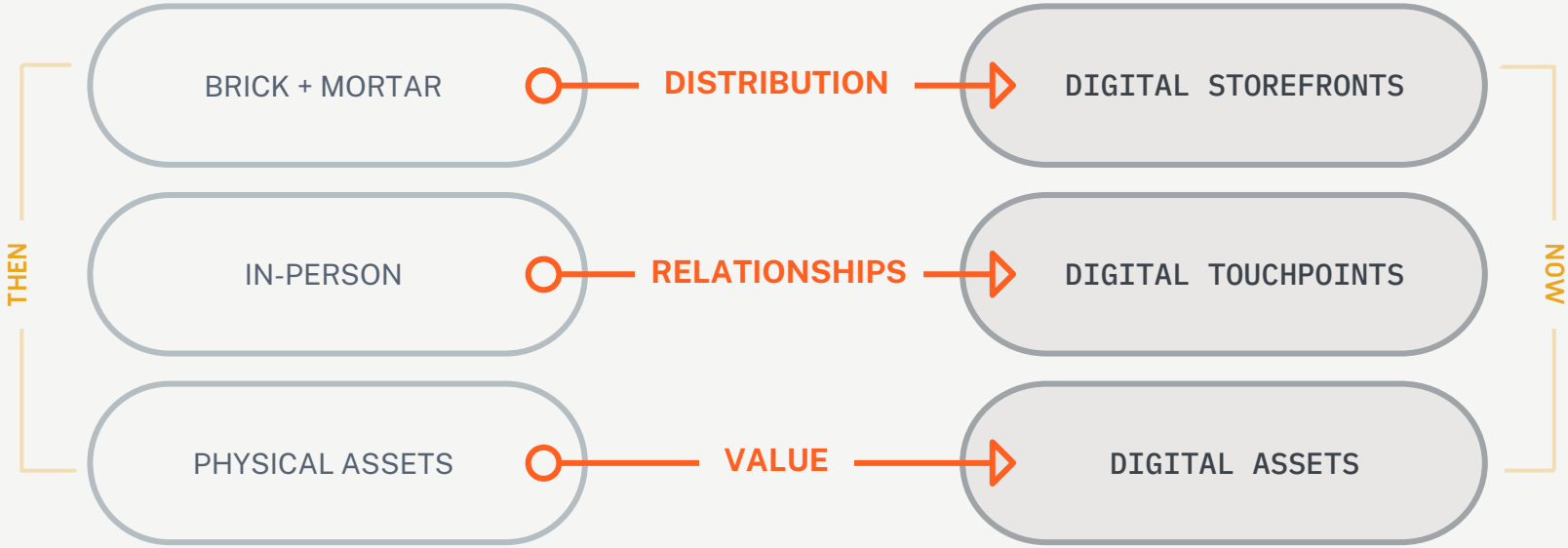
Zac Sawin, MBA - Business Development: Central Zone

Zac joins Coalition after a career as a Cyber and Technology Errors & Omissions broker and producer for Aon and Arthur J. Gallagher. During that time he consulted directly for organizations ranging from the smallest pre-revenue SMEs to fortune 500 companies, helping them navigate a volatile threat landscape and cyber insurance market. Zac has extensive experience with just about every industry vertical, including construction, design, and industrials, as well as the products and services of a majority of cyber insurers. Acting as a breach response coordinator, cybersecurity & compliance specialist, panel speaker, and general cyber consultant for some of the largest firms in the world, he brings a unique skill set to bear for Coalition and its' policyholders.

Erica Yampierre - Business Development: Eastern Zone

Erica joined Coalition in August 2021 with 10 years of experience handling cyber, professional liability, and environmental site exposures. Erica has underwritten cyber accounts for variety classes of business and revenue size. In her current role, Erica collaborates closely with broker partners to ensure their insured's understand their cyber exposure.

We are living in a digital-first world

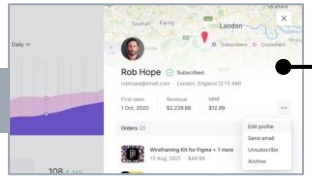


65% of the global GDP will be digitized by the end of 2022*

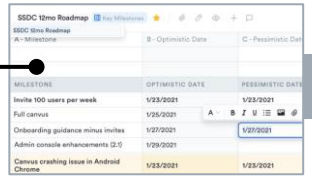
*IDC FutureScape: Worldwide Digital Transformation 2021 Predictions

Technology is now critical part of every organization

Customer Information



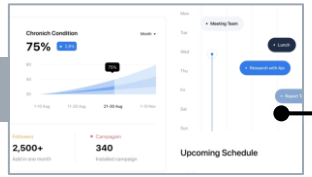
Finances & invoices



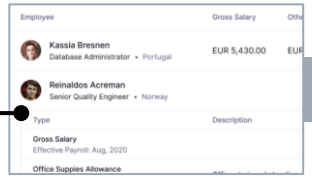
Order & Supplier info

Employee info

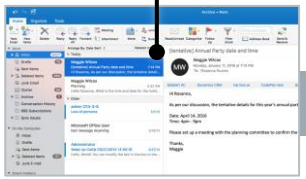
Business plans & IP



Payroll



Email



*IDC FutureScape: Worldwide Digital Transformation 2021 Predictions

And the threat to businesses is growing

Attacks are getting more sophisticated

$1.8M

Average ransom demand made against our policyholders, a 40% increase since 2020

More stolen funds

78%

Increase in the average funds stolen from our policyholders, up to $366,000 in 2021

Ongoing attacks

56%

Increase in attacks against small businesses with <$25M in revenue

Source: Coalition's 2022 Cyber Claims Report

Understanding cyber policies and coverage

First Party Coverage

Out of pocket expenses an organization incurs to recover from a loss.

Example: Breach response costs, cyber extortion, lost business income etc.

Third Party Coverage

Any resulting liability or third party action as a result of a cyber incident.

Example: Network Information and Security Liability, Multimedia Content Liability

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

...and more!

Not all cyber insurance is created equal

Things to look for in a cyber insurance provider:

Active risk management tools and services that reduce the likelihood of loss

Operational and **technical** support during incidents, in additional to financial recovery

Coverage for emerging **digital risk exposures** like reputation repair, cryptojacking, BI/PD

Unique cyber exposures for your industry

Construction, A&E, and Industrial firms face unique cyber exposures…

HIPAA data violations - BAA

Bodily Injury and Property Damage (BIPD)

Modelling Software & Intellectual Property

Smart Buildings, BIMS, SCADA, ICS

IoT exposure

Network exposure to third parties & Cloud Resources

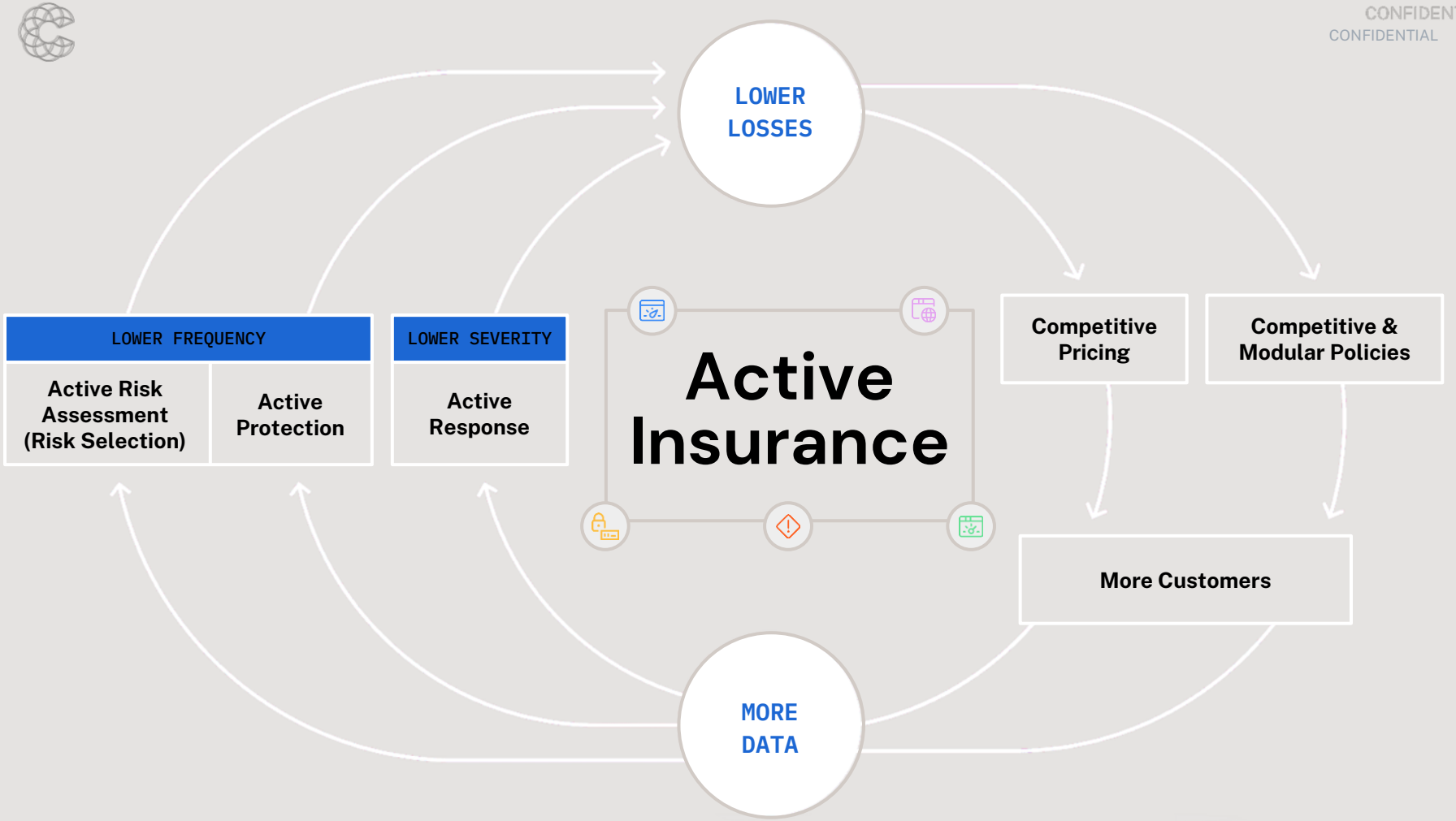
Stolen funds

Licensing technologies & more…

Active Protection Risk Platform

It's time for a new approach to Cyber Risk and Insurance in general

CONFIDENTIAL



Active Risk Assessment

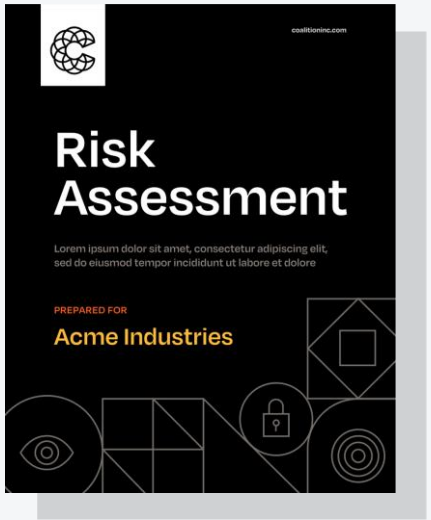
Remove the slow, painful steps at quote, bind & renewal

Personalized digital risk profiles
Remove lengthy questionnaires and avoids mistakes in cyber and exec risks

Automated, intelligent underwriting engine
Accurately prices digital risk in near real-time, saves brokers time so they can grow their business faster

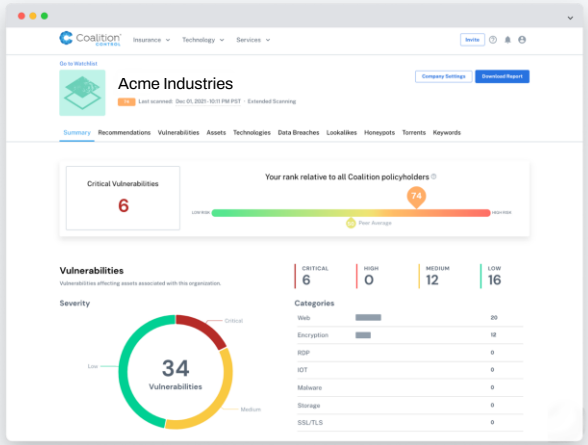
More accurate quotes and risk pricing
Make Coalition a trusted partner for the long term

Coalition Risk Assessment



Share digital risk insights and knowledge with your clients

Coalition Control



Empower organizations with the knowledge to track and manage their own digital risk

Active Protection

Spot and mitigate risk BEFORE it strikes

Continuous scanning and monitoring

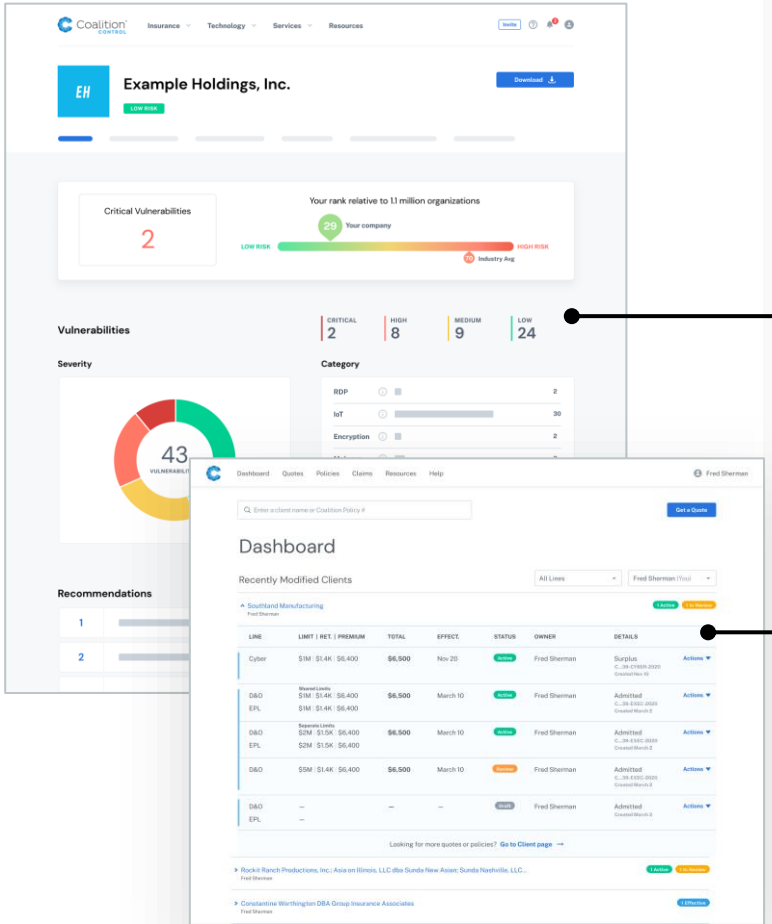
Connected assets & digital risk factors associated with cyber and exec risk

Automated notifications

Insureds and brokers stay informed, when new risks arise, or critical business changes occur

Support and guidance

help policyholders address technical needs or update policy information quickly when time matters



Actively monitor and alert both brokers and policyholders

Exec Risks Policyholder Dashboard

Empower organizations with the knowledge to track and manage their own risk

Coalition Broker Portal

Share our insights with your clients

Claims case studies

Email phishing and funds transfer fraud

- $200M revenue construction firm in Colorado
- $800k funds lost through phishing scam

Ransomware attack with $2M demand

- $150M revenue GC in Texas
- Ransomware attack with HelloKitty
- Recovery from back ups, required data mining, and notification

Design Professional Claims

OPERATIONAL DEPENDENCY

Ransomware encrypts entire network — including tablets and mobile devices. Inability to manage change orders, review work in progress, or function entirely.

FORCED TO PAY RANSOMS

Data uniqueness makes recreation difficult if not impossible when unrecoverable. Design firms are more likely to be forced to pay ransom demands–unless the most prudent of backup controls are in place.

CONTRACTUAL LIABILITY

Contractual deadlines missed due to network security incidents. If missed, damages may not be covered by insurance.

Cyber Incident timeline

SECURITY CONCERN

Policyholder suspects a security concern and/or receives an alert from Coalition, and sets up an investigation call with Coalition

ASSESSMENT

Coalition's team determines if there's sufficient reason to complete a forensics investigation.

Indicators we look for:

- Legitimate log-ins to the email
- Password changes
- New accounts created
- Malicious email headers

FORENSICS

Coalition Incident Response (CIR) or a 3rd party vendor completes forensics work and remediation

RECOVERY

Coalition pays claim expenses and enables the policyholder to get back to business

Thank You!