cowbell®

PROUD TO PARTNER WITH

Charity First

Wednesday, February 7, 2024

Agenda

Agenda

- Cyber Risk and SMEs
- Who is Cowbell?
- Coverage Highlights
- Risk Engineering and Value Added Services
- Claims
- Team

Cyber Risk and SMEs

FACT: The majority of US SMEs have experienced a cyber incident: **57% of SMEs have been the target of a cybersecurity breach**; 31% in the last year alone.

FACT: The average cost of a data breach for a company with less than 500 employees is estimated at **$2.98 million.**

FACT: In the U.S., **75% of SMEs say cybersecurity is a major concern** and the majority, **59% plan to increase investments** in cybersecurity over the next year.

Sources: Guardz SME Survey 2023; IBM's *Cost of a Data Breach* report, 2021; Sage Survey, Oct 2023.

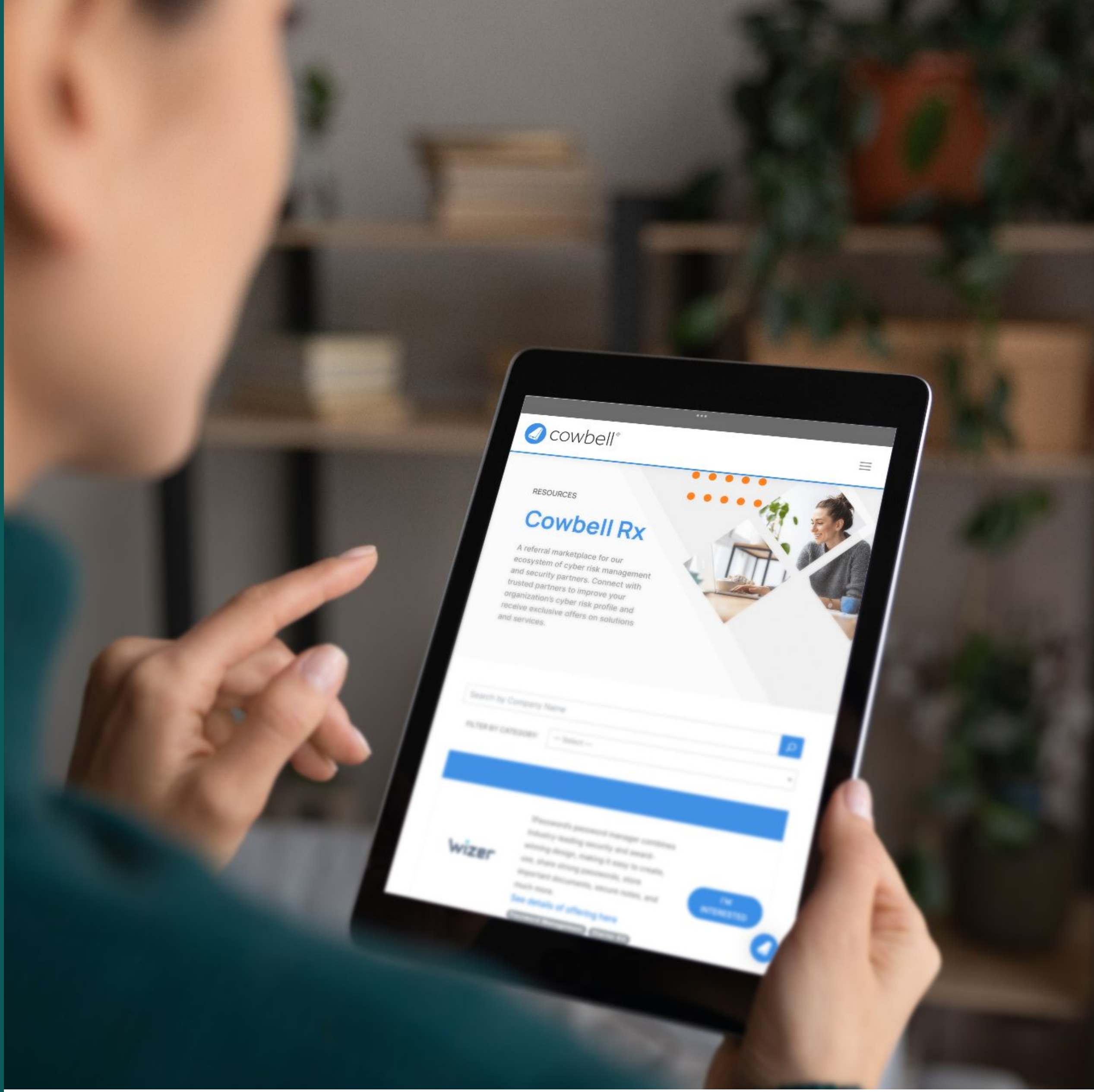
Who is Cowbell?

ADVANCED CYBER SOLUTIONS

We are your true cyber partner.

Cowbell is more than an insurance provider. We offer intelligent cyber insurance and security solutions to small and medium-sized business across the U.S. and U.K.

From AI-led risk assessment to personalized risk consulting services, our approach gives policyholders more than financial peace of mind.


cowbell
RESOURCES
Cowbell Rx
A referral marketplace for our ecosystem of cyber risk management and security partners. Connect with trusted partners to improve your organization's cyber risk profile and receive exclusive offers on solutions and services.
wizer

COWBELL YOU CAN **COUNT ON**

Just like you, we value trust, stability, and expertise

With Cowbell as a partner, you can count on us to provide a consistent and stable experience as we continue to innovate our products and expand our footprint.

- Executive team with significant leadership experience in insurance, cybersecurity, and tech
- Backed by over 20 prominent leading global (re)insurance partners
- Funded by security, AI, and insurance VCs

SETTING YOU UP FOR **SUCCESS**

Cowbell is the gold standard for brokers and policyholders alike.

CYBER INSURANCE **SIMPLIFIED**

ADVANCED CYBER SOLUTIONS

COWBELL YOU CAN **COUNT ON**

CYBER INSURANCE **SIMPLIFIED**

Cowbell makes it easy and accessible.

- Simplified Application Process via JotForm
- **Here** when you need us
- Ongoing **education and training**

Coverage Highlights

INSURANCE **PRODUCTS**

Cowbell Prime 100

Essential cyber insurance.

Product Details

◉ **Up to $100M** in revenue

◉ Admitted in 47 states and D.C. on “A” rated paper

◉ Ideal for first time Cyber insurance buyers

◉ 100% automated underwriting

◉ Limits **up to $3M**

Prime 100 Coverages

Designed to address the diversity of cyber incidents and resulting damages that can impact businesses.

Security Breach Expense
Coverage for losses and expenses directly associated with recovery activities in the aftermath of a cyber incident. This can include investigation and forensic services, notification to customers, call center services, overtime salaries, post-event monitoring services such as credit monitoring for impacted customers and more.

Security Breach Liability
Coverage for third party liability directly due to a cyber Incident and that the insured becomes legally obligated to pay. This includes defense expenses, compensatory damages, and settlement amounts, and fines or penalties assessed against the insured by a regulatory agency or government entity, or for non-compliance with the Payment Card Industry Data Security Standards.

Restoration of Electronic Data
Coverage for the costs to replace or restore electronic data or computer programs in the aftermath of an incident. This can also include the cost of data entry, reprogramming and computer consultation services to restore lost assets.

Extortion Threats and Ransom Payments
Coverage for expenses related to the investigation, negotiation, and possible payment of an extortion threat and ransom. This can include fees and costs associated with ransom negotiators, the payment of ransom, interest costs paid to a financial institution for a loan to pay the ransom, and/or reward payments for information leading to an arrest.

Public Relations Expense
Coverage for the fees and costs to restore reputation in response to negative publicity following a cyber incident or a security breach. This includes, for example, the fees associated with the hiring of a public relations firm that handles external communications related to the breach.

Computer & Funds Transfer Fraud
Coverages *for the losses due to a fraudulent computer operation that causes money (or other property) to be transferred from an insured's account. This also covers losses incurred by a fraudulent instruction directing a financial institution to debit money from the insured's transfer account.*

PCI Fines and Penalties
Coverage for loss and defense expenses as a result of a claim in the form of an action by a Card Company for non-compliance with the Payment Card Industry (PCI) Data Security Standards (DSS), including coverage of related fines or penalties (to the extent such fines or penalties are insured by law).

Social Engineering
Coverages for a loss resulting from a social engineering incident where the insured is intentionally misled to transfer to a person, place or account directly from good faith reliance upon an instruction transmitted via email by an imposter. A document verification procedure requirement needs to have been completed in order to be provided coverage.

Website Media Content Liability
Coverage for loss and defense expenses from intellectual property infringement, other than patent infringement, related to media content on the company website or its social media accounts only.

Regulator Defence and Penalties
Coverage for loss and defense expenses as a result of an investigation, demand of Regulatory Proceeding, brought by or on behalf of an administrative or regulatory agency, or any federal state, local or foreign government entity in an official capacity.

Hardware Replacement Costs
Coverage for the cost to replace computers or any associated devices or equipment operated by the insured that are unable to function as intended due to corruption or destruction of software or firmware, resulting from a cyber incident.

Business Income, Contingent Business Income & Extra Expense
Coverage for the losses and costs associated with the inability to conduct business due to a cyber incident or an extortion threat. Business income includes net income that would have been earned or incurred. Note that the business interruptions due to system failure or voluntary shutdown are not covered.

Post Breach Remediation Coverage
Coverage for labor costs incurred to resolve vulnerabilities or weaknesses in the insured's computer system that are identified by an independent security firm after a cyber incident. Identified upgrades or improvements must reduce the probability or potential damage of a future incident to qualify. Coverage for labor costs incurred to resolve vulnerabilities or weaknesses in the insured's computer system that are identified by an independent security firm after a cyber incident. Identified upgrades or improvements must reduce the probability or potential damage of a future incident to qualify.

Telecommunications Fraud
Coverage for the cost of unauthorized calls or unauthorized use of the insured's telephone system's bandwidth, including but not limited to phone bills.

Prime 100
Coverage Highlights

Designed to address the diversity of cybersecurity incidents and business impacts.

Liability Expense

- Security Breach Liability
- Website Media Content

First Party Expense

- Security Breach
- Extortion & Ransom Payments
- Business Income & Extra Expense

First Party Loss

- Hardware Replacement
- Restoration of Electronic Data
- Social Engineering

Full coverage available by request.

Prime 100: Risk Appetite

Target Classes

Financial Services

Healthcare

Retailers

Manufacturing

Law Firms

Medical & Dental Offices

Insurance Agencies

Professional Service

Hospitality

Accounting Firms

Nonprofit Organizations

Contractors

Truckers

Wholesale **and more!**

Restricted classes of business

Political Affiliated Organizations, Social Media including Crowdsourcing, Adult Entertainment, Cryptocurrency, Payment Processors, Gambling (Online), Cannabis, Data Aggregators, Online Trading Platforms.

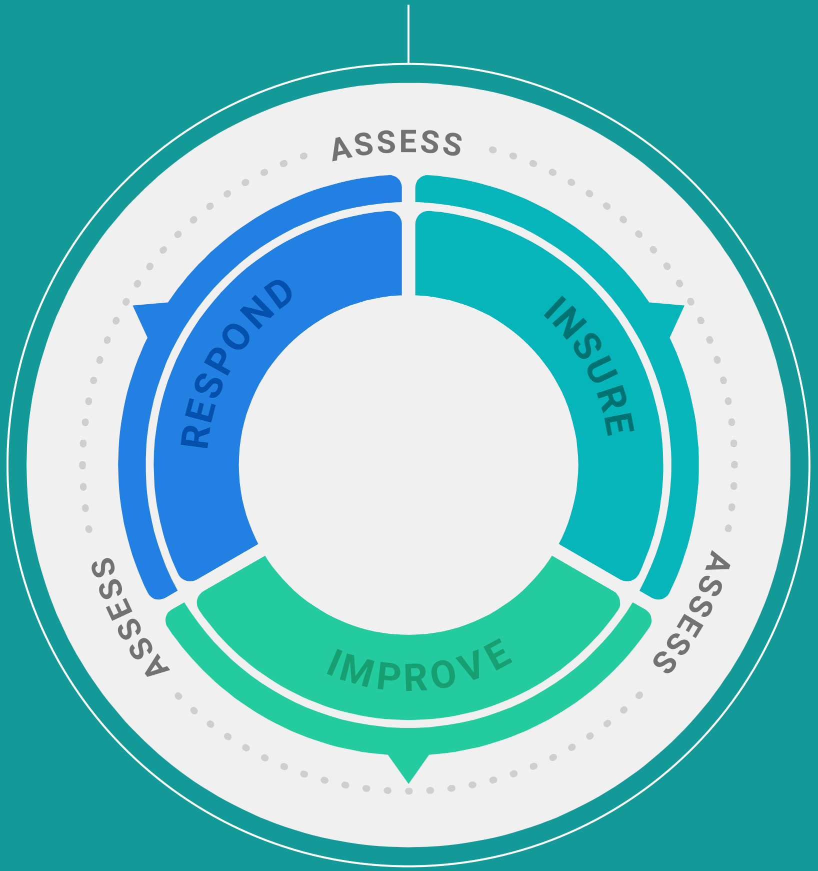
Risk Engineering and Value Added Services

Closed-loop risk management

At Cowbell, one good thing leads to another. That's especially true when it comes to our closed-loop risk management approach.

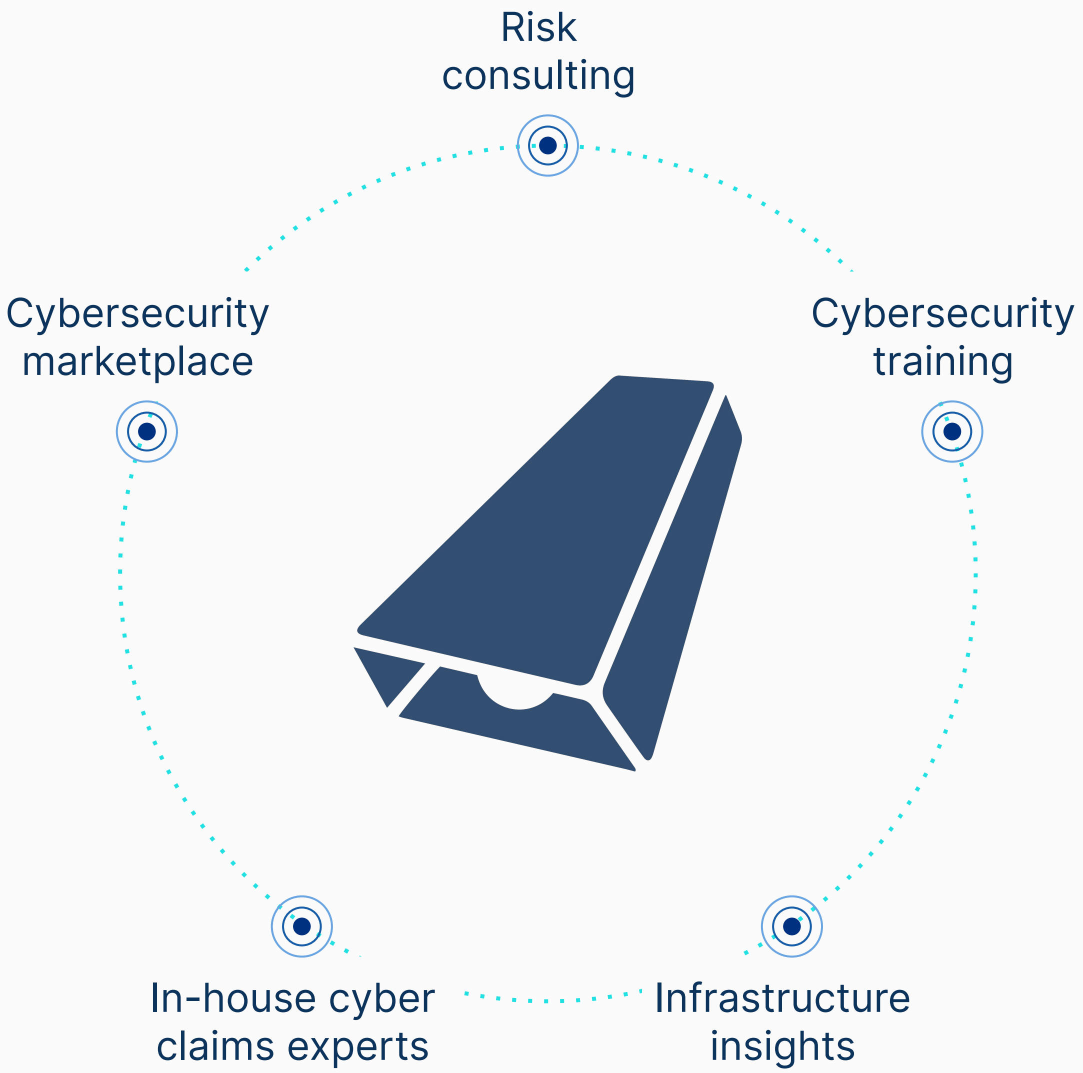
We use an always-on approach that continuously assesses and mitigates risk, improves policyholder outcomes, and ultimately increases retention rates.

THE **COWBELL** APPROACH



Cowbell 365

Risk management services, on demand.



Personalized Risk Management

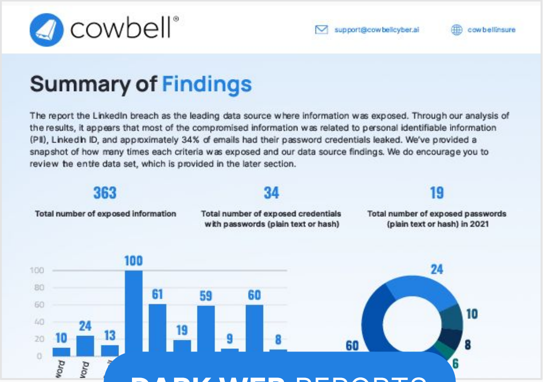
Policyholders have cyber risk experts and cybersecurity resources on their side.

RISK CONSULTATIONS

Live, **60-minute consultations** provide the insured with a detailed risk assessment and expert recommendations to improve their cybersecurity posture.

ON-PLATFORM INSIGHTS

Insureds get **personalized, realtime recommendations** delivered directly to their Cowbell dashboard.



cowbell® support@cowbellcyber.ai cowbellinsure

Summary of Findings

The report the LinkedIn breach as the leading data source where information was exposed. Through our analysis of the results, it appears that most of the compromised information was related to personal identifiable information (PII), LinkedIn ID, and approximately 34% of emails had their password credentials leaked. We've provided a snapshot of how many times each criteria was exposed and our data source findings. We do encourage you to review the entire data set, which is provided in the later section.

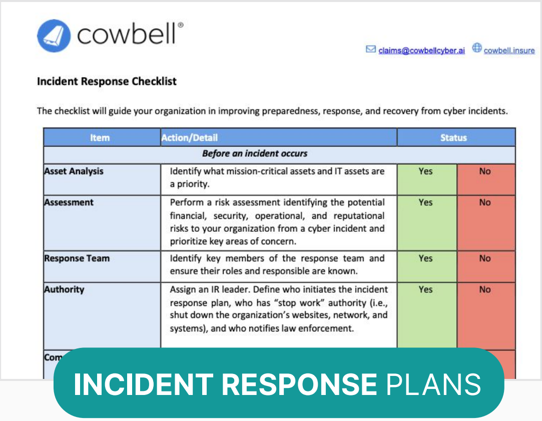
363
Total number of exposed information

34
Total number of exposed credentials with passwords (plain text or hash)

19
Total number of exposed passwords (plain text or hash) in 2021

DARK WEB REPORTS

When we detect dark web information, we do a deep dive and provide policyholders with a **custom report** including detailed insights and advice.



cowbell®

claims@cowbellcyber.ai cowbell.insure

Incident Response Checklist

The checklist will guide your organization in improving preparedness, response, and recovery from cyber incidents.

Item	Action/Detail	Status	
Before an incident occurs			
Asset Analysis	Identify what mission-critical assets and IT assets are a priority.	Yes	No
Assessment	Perform a risk assessment identifying the potential financial, security, operational, and reputational risks to your organization from a cyber incident and prioritize key areas of concern.	Yes	No
Response Team	Identify key members of the response team and ensure their roles and responsible are known.	Yes	No
Authority	Assign an IR leader. Define who initiates the incident response plan, who has "stop work" authority (i.e., shut down the organization's websites, network, and systems), and who notifies law enforcement.	Yes	No
Com			

INCIDENT RESPONSE PLANS

It's all about being prepared in case of a cybersecurity incident. Insureds can download personalized Incident Response Plans so they can **act fast and effectively.**

Micro Penetration testing is also available at no cost to Cowbell policyholders.

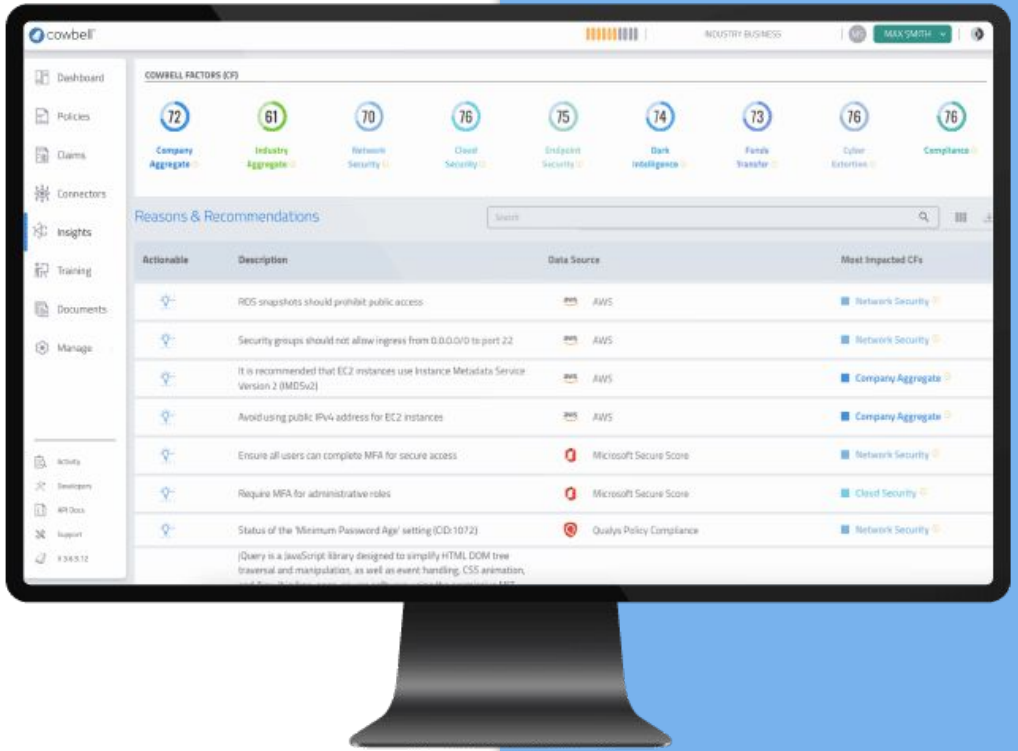
Cowbell Insights

Continuous Risk Awareness

Cowbell Insights are recommendations provided to remediate cybersecurity weaknesses and improve organization's risk profile.

They answer the following questions:

1. Which cyber risks are potentially impacting my organization?
2. Which Cowbell Factors are impacted by the findings?
3. How can I remediate the discovered security weakness?



Reasons & Recommendations

Actionable	Description	Data Source	Most Impacted CFs
	RDS snapshots should prohibit public access	AWS	Network Security
	Security groups should not allow ingress from 0.0.0.0/0 to port 22	AWS	Network Security
	It is recommended that EC2 instances use Instance Metadata Service Version 2 (IMDSv2)	AWS	Company Aggregate
	Avoid using public IPv4 address for EC2 instances	AWS	Company Aggregate
	Ensure all users can complete MFA for secure access	Microsoft Secure Score	Network Security
	Require MFA for administrative roles	Microsoft Secure Score	Cloud Security
	Status of the 'Minimum Password Age' setting (CID:1072)	Qualys Policy Compliance	Network Security
	jQuery is a JavaScript library designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation,		

Cowbell Academy

Uplevel your education, better serve your customers, and access no-cost Continuing Education courses.

- **Introduction to Cowbell Policies**

  How to generate and bind a quote.

- **Coverage Breakdown**

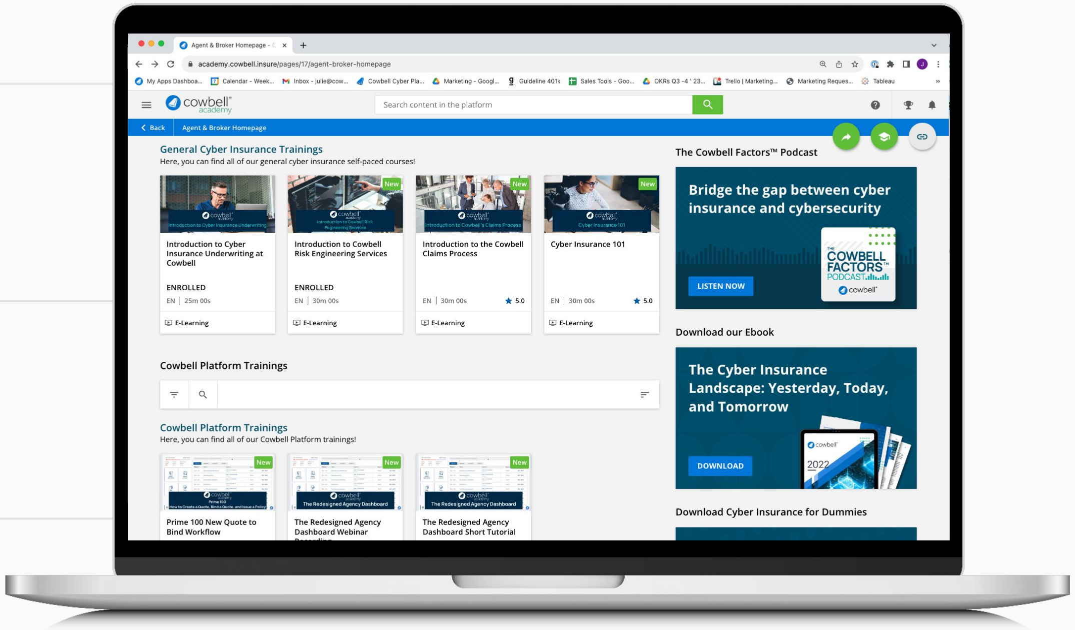
  A deep-dive into Cowbell coverage.

- **Cyber Insurance Underwriting**

  Learn how Cowbell assesses risk.

- **Cyber Insurance 101**

  A resource for new agents and staff.


Agent & Broker Homepage - C
academy.cowbell.insure/pages/17/agent-broker-homepage
My Apps Dashboa...
Calendar - Week...
Inbox - julie@cow...
Cowbell Cyber Pla...
Marketing - Googl...
Guideline 401k
Sales Tools - Goo...
OKRs Q3 -4 ' 23...
Trello | Marketing...
Marketing Reques...
Tableau
cowbell academy
Search content in the platform
Back
Agent & Broker Homepage
New
cowbell academy
Introduction to Cyber Insurance Underwriting
Introduction to Cowbell Risk Engineering Services
Introduction to Cowbell's Claims Process
Cyber Insurance 101
Prime 100
How to Create a Quote, Bind a Quote, and Issue a Policy
The Redesigned Agency Dashboard
LISTEN NOW
THE COWBELL FACTORS™ PODCAST
cowbell
DOWNLOAD
2022

General Cyber Insurance Trainings

Here, you can find all of our general cyber insurance self-paced courses!

Introduction to Cyber Insurance Underwriting at Cowbell
ENROLLED
EN | 25m 00s
E-Learning

Introduction to Cowbell Risk Engineering Services
ENROLLED
EN | 30m 00s
E-Learning

Introduction to the Cowbell Claims Process
EN | 30m 00s ★ 5.0
E-Learning

Cyber Insurance 101
EN | 30m 00s ★ 5.0
E-Learning

Cowbell Platform Trainings

Cowbell Platform Trainings

Here, you can find all of our Cowbell Platform trainings!

Prime 100 New Quote to Bind Workflow

The Redesigned Agency Dashboard Webinar Recording

The Redesigned Agency Dashboard Short Tutorial

The Cowbell Factors™ Podcast

Bridge the gap between cyber insurance and cybersecurity

Download our Ebook

The Cyber Insurance Landscape: Yesterday, Today, and Tomorrow

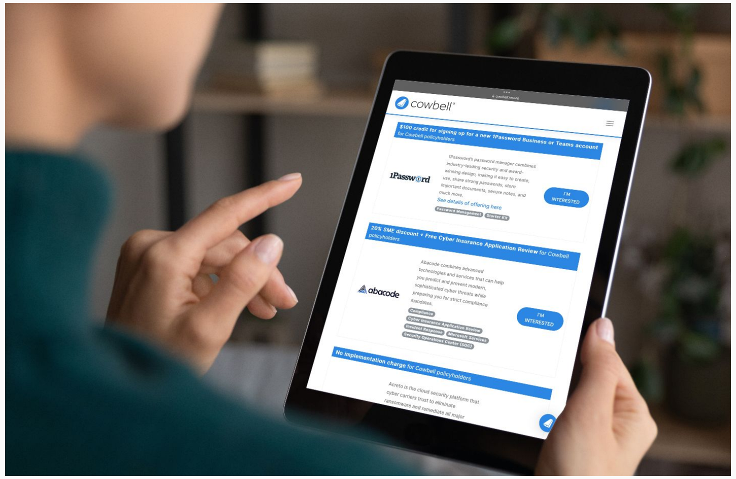
Download Cyber Insurance for Dummies

Additional Money-Saving Resources

Partner savings and complimentary cybersecurity awareness programs

Cybersecurity Marketplace

Cowbell Rx is a referral marketplace of vetted cyber risk management and security partners providing policyholders with **discounted cyber solutions**.



$100 credit for signing up for a new 1Password Business or Teams account for Cowbell policyholders

1Password's password manager combines industry-leading security and award-winning design, making it easy to create, use, share strong passwords, store important documents, secure notes, and much more.

See details of offering here

20% SME discount + Free Cyber Insurance Application Review for Cowbell policyholders

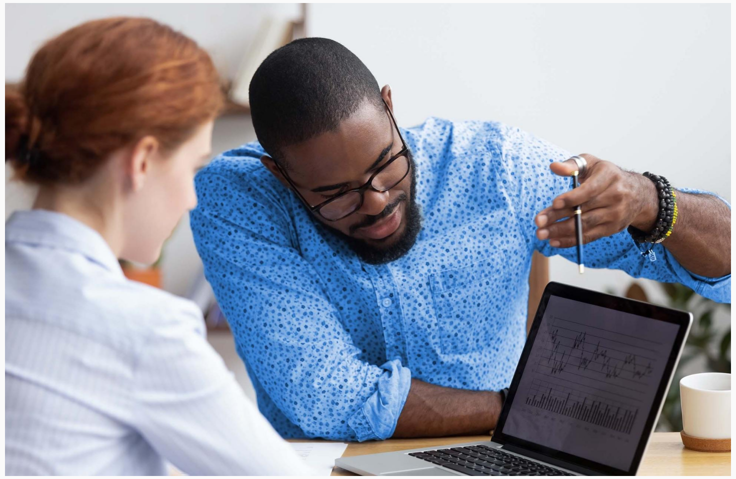
Abacode combines advanced technologies and services that can help you predict and prevent modern, sophisticated cyber threats while preparing you for strict compliance mandates.

No implementation charge for Cowbell policyholders

Acreto is the cloud security platform that cyber carriers trust to eliminate ransomware and remediate all major

Cybersecurity Awareness Training

Employee cyber awareness training **reduces the cost of phishing by more than 50%**. We offer it an no cost to policyholders through our partner, Wizer.



Cowbell 365 Improves Policyholder Outcomes

100% of policyholders who underwent a comprehensive risk consultation prevented ransomware incidents.

After 12 months with Cowbell, policyholders' saw a **9% improvement** on their risk profile

As a result, cowbell maintains a **3% claims frequency** year after year.

*Compared to industry peers

Claims

Since writing our first policy in 2020, we’ve paid

more than $100 Million in claims.

We’re backed by a panel of 20 leading reinsurers including Swiss RE, Munich RE, Renaissance RE, and Arch.

Our Claims Process

Report

Incident is reported through our claims hotline or by email.

Review

A review of policy and coverage is conducted and policyholder is informed.

Respond

Cowbell’s incident response team is deployed.

Breach counsel, digital forensic and incident response investigators, professional ransom negotiators, etc.

In the Event of a Cyber Incident

1. Ensure that policyholders **do not** attempt to resolve the issue on their own.

2. **Report** to Cowbell at (833) 633 – 8666

3. Ask the policyholder to develop a summary or **timeline of events** leading to the discovery of the cyber event.

4. Ask the policyholder to **track any costs**, that might have incurred to date associated with the cyber event.

Ransomware Incident

Claims Case Study

Policyholder:

A professional services company with $70M in revenue and 150-200 employees

Scenario:

The company received an alert that a suspicious IP address had accessed their system and shortly thereafter, employees were locked out. That was followed up by a ransom demand of $1.5M from an aggressive group of cyber criminals. The policyholder immediately contacted Cowbell.

Action plan:

Within the hour, Cowbell assembled a team of trusted incident response partners to assist. We worked with the policyholder to review the status of their data backups, recover data and operations, recommend necessary recovery workstreams, and assigned response partners to assist after hours.

Results:

- Reduced initial ransom amount **by 70%**
- Company quickly up and running with **minimal business disruption**
- **Improved cybersecurity configuration** to prevent future incidents

Prime 100 Claims Panel

Industry's leading experts

Credit Monitoring & Notification Services

IDEXPERTS® E-CARD ID Products Ltd.

experian

KROLL

TransUnion

Defense Counsel

MC MULLEN COUGHLIN

CONSTANGY BROOKS, SMITH & PROPHETE LLP

CIPRIANI & WERNER ATTORNEYS AT LAW

BakerHostetler

Forensic Investigators & Data Recovery

Arete

KROLL

ARCTIC WOLF

Booz | Allen | Hamilton

Breach Counsel

McDonald Hopkins

CONSTANGY BROOKS, SMITH & PROPHETE LLP

CIPRIANI & WERNER ATTORNEYS AT LAW

MC MULLEN COUGHLIN

WSHB WOOD·SMITH HENNING·BERMAN