cowbell®

Cyber Roundup:

Claims Report 2025

Insights from Cowbell's claims data and trends

Executive Summary

Cyber Attacks Continue to Rise Globally While Ransomware Claims Frequency Remains Steady

Cyberattacks are increasing in volume and sophistication, driven by AI-enhanced campaigns and an ever-changing global security environment. According to the 2024 NAIC Cyber Insurance Report, the U.S. cyber insurance market saw a record 33,561 reported claims - the highest annual total to date - underscoring a steady rise in frequency across the industry.

While overall claims frequency has trended upward across the market, Cowbell's recent analysis shows a more stable pattern in ransomware-related incidents, which consistently accounted for 17–19% of total Cowbell claims between 2022 and 2024. During the same period, average ransom payments declined by approximately 20.5%, reflecting improved claims management and more effective negotiation strategies in response to ransomware events.

Despite the persistent and strategic activity of threat actors, this development underscores the importance of robust partnerships in risk management, comprehensive cyber defenses, responsive claims handling, and immediate incident response (IR) capabilities. This report provides insights for brokers and businesses aiming to confidently address and mitigate cyber risks in an increasingly challenging environment.

While ransomware frequently captures media attention, it represents just one aspect of the broader cyber risk spectrum. Modern attackers capitalize on common vulnerabilities to execute harmful attacks ranging from phishing schemes and business email compromise (BEC) to funds transfer fraud. In such a dynamic threat landscape, achieving true resilience involves more than just fortified defenses. It requires proactive measures, flexible technological solutions, and enhanced collaboration between organizational leaders, cybersecurity experts, and specialized cyber risk partners like Cowbell.

In the subsequent sections, we analyze pivotal claims trends, provide new data-driven insights, and outline actionable strategies designed to help organizations of all sizes stay prepared and resilient against emerging cyber threats.

Note: Unless otherwise specified, Cowbell's claims data referenced in this report covers incidents from the last 18 months

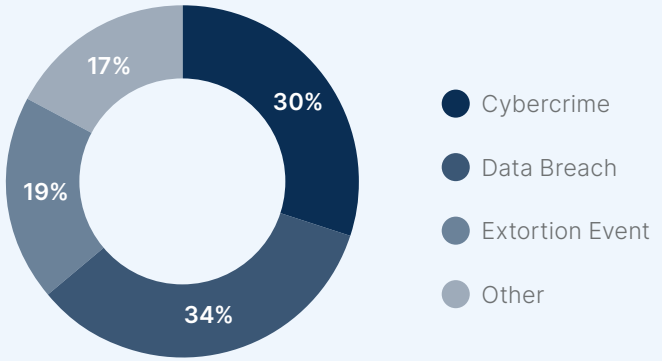
Top Threats Driving Claims

How Do Most Attacks Start?

The answer is often phishing. Phishing emails, malicious links, and fake login pages remain some of the most common ways attackers gain initial access to an organization's systems. Even when significant losses ultimately involve ransomware, business email compromise (BEC), or funds transfer fraud, phishing frequently serves as the entry point. In 2024, the FBI identified phishing and spoofing scams as the most commonly reported cybercrimes in the United States, with 193,000 complaints. This underscores that employee awareness, robust email security, and proactive threat detection form essential first lines of defense against cyberattacks.

These tactics are elements of a larger threat known as social engineering, where attackers manipulate human behavior to access systems, data, or finances. As social engineering grows increasingly sophisticated, businesses require comprehensive defenses combining cutting-edge technology, regular employee training, and swift incident response strategies.

Incident Types Driving Claims Frequency



Cyber incidents impacting organizations come in various forms, each requiring distinct responses and preparedness. Cowbell's claims data reveal three primary incident types that account for the majority of reported claims: cybercrime, data breaches, and extortion events.

Cybercrime (30%): These incidents typically involve financial or data theft through tactics like phishing, business email compromise (BEC), and funds transfer fraud, exploiting human vulnerabilities.

Data Breach (34%): Breaches involving unauthorized access or disclosure of sensitive information remain prevalent, emphasizing the need for strong data security and rapid response measures.

Extortion Event (19%): Ransomware and other extortion-based attacks continue to threaten operational stability by encrypting critical data and demanding payment for its release.

Example Breach Path

Phishing Email
The attacker sends a deceptive email designed to trick the recipient into engaging.

User Action
The recipient clicks a link, opens a file, or enters credentials unknowingly enabling the attack.

System Access Gained
The attacker establishes a foothold within a network or device, often escalating privileges.

Attack Deployed
Ransomware, BEC, or FTF is executed, causing damage or demanding payment.

Threat Actor "Attack Chain"

Social engineering attacks often start with phishing, then escalate into serious incidents like ransomware, business email compromise, or funds transfer fraud.

Systemic Cyber Events on the Rise

Not all attacks start from isolated incidents. Systemic vulnerabilities, exemplified by high-profile breaches such as MOVEit and PowerSchool, demonstrate how one vulnerability can cascade through multiple organizations simultaneously. These systemic events emphasize the critical need for multi-layered defenses, rapid threat detection capabilities, and proactive risk management plans designed to minimize widespread damage.

Why It Matters

Today's cyber threats illustrate a critical truth: sophisticated technology combined with human vulnerability creates significant risk. Effective risk management isn't just beneficial, it's essential. Proactively addressing vulnerabilities and educating clients about cyber risks can significantly reduce their exposure and limit the impact of cybercrime.

Among these threats, ransomware stands out as particularly damaging. Who's behind these attacks, and how can brokers proactively guide their clients? Let's explore further.

Ransomware Trends & Broker Insights

Ransomware Threats Are Evolving

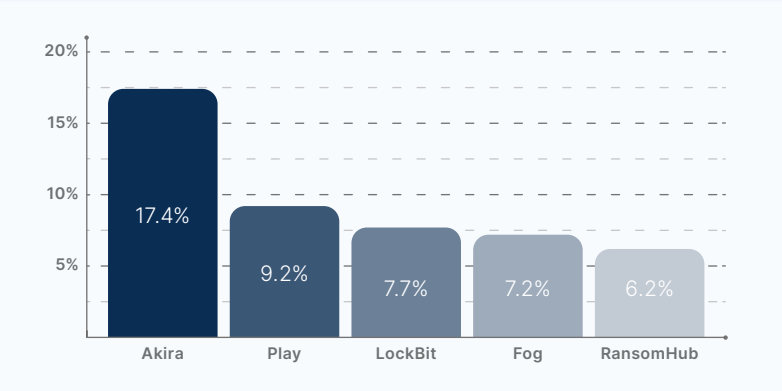
Cybercrime headlines often focus on the identity of attackers. Yet, for brokers and businesses, the real story is what these threats reveal about organizational vulnerabilities and resilience.

Who's behind the attacks?

Cowbell's claims data identifies a handful of prominent ransomware groups behind a significant portion of severe incidents. In fact, nearly half (48%) of the cases with identified threat actors involve just five groups:

- Akira (17.4%): Specializes in double extortion attacks targeting mid-sized businesses.
- Play (9.2%): Employs stealthy ransomware tactics with delayed detonation.
- LockBit (7.7%): A highly prolific ransomware-as-a-service operator globally.
- Fog (7.2%): A newer group exploiting vulnerabilities in unpatched VPN and email systems.
- RansomHub (6.2%): Known for extortion by stealing and threatening to publicly leak data.

Threat Actor Breakdown



Cowbell's claims data reveals that nearly half of severe ransomware incidents with known threat actors are linked to just five prominent groups.

Organizations with advanced endpoint protection services, such as Managed Detection and Response (MDR), fully recover from cyberattacks nearly three times faster than those relying on basic security measures alone[1].

[1] Sophos, 2025

Most operated out of Eastern Europe and North Asia, exploiting basic, preventable weaknesses like outdated software, misconfigured email accounts, and unpatched network boundaries.

At Cowbell, average ransomware payments to threat actors have steadily decreased, dropping almost 4% from 2022 to 2023, followed by a further 17.5% decline from 2023 to 2024. This consistent reduction underscores Cowbell's negotiation expertise, robust incident response capabilities, and effective partner coordination in minimizing payouts and weakening threat actors' leverage.

What Brokers Should Know

The specific identity of attackers matters less than the preparedness of your clients. Organizations with robust layered defenses, including endpoint protections, strong access controls, and consistent patch management, consistently achieve quicker claims resolutions and experience significantly lower financial impacts. Cowbell's adaptive risk management strategies and rapid claims support ensure businesses can respond effectively to any emerging threat.

Industries under heightened threat need brokers who deeply understand these vulnerabilities and can guide clients toward effective, proactive risk management practices.

Industry Spotlight – Who's at Risk?

The Professional Services, Educational Services, Healthcare, Construction, and Manufacturing sectors consistently experience some of the highest rates of cyber claims. These industries' heavy reliance on sensitive data and operational continuity makes them particularly vulnerable. Safeguarding these sectors requires proactive coverage paired with intelligent, industry-specific risk management strategies.

Unique Risks by Sector:

- Professional Services: Sensitive client data, including Personally Identifiable Information (PII), makes these businesses prime targets for data extortion.
- Educational Services: Cyber threats frequently target sensitive student data and aim to disrupt online learning platforms.
- Healthcare: Dependence on critical patient care systems heightens urgency during cyber incidents, resulting in increased ransom demands.
- Construction: Extensive vendor networks, complex supply chains, and highly mobile workforces significantly widen potential attack vectors.
- Manufacturing: Cyberattacks can completely halt production, causing extensive operational downtime and significant financial losses.

Industries handling sensitive information typically face higher-than-average ransom demands and longer recovery periods.

When a cyber event occurs, swift action, clear communication, and expert claims handling can drastically influence the outcome, underscoring the importance of partnering with specialists adept in rapid response and detailed cyber incident management.

We reduce ransom amounts by an average of 66%* through negotiations with the threat actors.

Beyond claims, Cowbell equips brokers with essential tools, actionable data, and comprehensive education to drive growth and effectively manage risks in today's evolving cyber landscape.

*Average ransom reduction of 66% is based on historical data from negotiations. Actual results vary significantly based on individual circumstances, threat actor behaviors, and specific negotiation contexts

Claims at Cowbell

Delivering Outcomes that Matter

At Cowbell, quickly resolving claims with transparency and in the best interests of our insureds is paramount. Our experienced claims team, boasting a combined 60+ years of expertise, includes former breach counsel, claims advocates, and professionals from traditional insurers, insurtechs, MGAs, and coverage law firms.

From the moment a claim is received, Cowbell provides acknowledgment within minutes and swiftly assigns dedicated internal support.

Average Response Time:

- Initial acknowledgment: within 1 hour
- First contact after claim submission: typically within 24 hours, with urgent issues such as ransomware addressed within 1 hour.

Busiest Claim Day: “Cyber Friday” - threat actors often exploit weekends to conduct unnoticed attacks, leading to increased activity on Fridays and the subsequent Mondays following long weekends.

Our claims process emphasizes expert negotiation, incident response coordination, and proactive, hands-on support. Our team not only manages claims efficiently but also expertly guides insureds through the complexities of cyber events. Fast action, coordinated expertise, and consistent policyholder support define the Cowbell claims experience.

Claim Case Studies

Cowbell’s cyber risk experts are on-call and always ready to help you immediately with a full range of incident response strategies. Explore our case studies for detailed insights on the claims process at Cowbell.

- Small Business Claims: Construction
- Small Business Claims: Healthcare
- Small Business Claims: Retail
- Mid-sized Business Claims: Energy
- Mid-sized Business Claims: Professional Services
- Mid-sized Business Claims: Construction

What Our Partners Say

"Your team was on the phone with the client within 15 minutes after they reported a cyber incident, providing immediate reassurance during a critical moment."

- Broker Partner

"During a complex ransomware incident, your swift connection to breach counsel and forensics experts significantly relieved the insured's stress and uncertainty."

- Broker Partner

"Cowbell's proactive support and the expert team assembled quickly during our claim gave us confidence and clarity in managing an unfamiliar and challenging situation."

- Policyholder

Leveraging Cowbell Factors™ for Better Cyber Risk Management

Cowbell Factors are core to Cowbell's unique approach to understanding and managing cyber risk. By assessing risk across multiple dimensions, such as network security, cloud security, compliance posture, and employee vigilance, Cowbell Factors provide clear, actionable insights into an organization's overall cybersecurity health.

Cowbell Factors significantly improve the prediction of cyber risk:

- A 436% improvement in predicting claims frequency.
- A 254% increase in predicting claims severity.
- Organizations utilizing connectors such as Microsoft 365 exhibit notably better risk profiles, especially concerning ransomware and extortion threats.
- Detailed industry benchmarking using granular NAICS codes increases risk assessment precision by up to 42 times.

Organizations maintaining higher Cowbell Factor scores experience fewer cyber incidents and significantly lower financial impacts when incidents occur. By closely monitoring and actively improving Cowbell Factors, brokers can guide their clients toward enhanced cyber resilience and optimized insurance outcomes.

Industry Claims Prediction for Remainder of 2025

Based on current industry trends and expert insights, we anticipate:

- **Continued Rise in Targeted Attacks:** Sectors like healthcare, professional services, and construction will remain highly targeted, driven by attackers' focus on industries reliant on continuous operations and sensitive data.
- **Increasing Complexity of Ransomware:** Ransomware groups will increasingly adopt multi-layered extortion techniques, raising the stakes for effective incident response and proactive defense strategies.
- **Greater Emphasis on Preventative Measures:** Businesses will increasingly seek out partners who provide proactive tools and resources, such as AI-driven monitoring, vulnerability assessments, and cyber hygiene training, to actively reduce their cyber risk.

Cowbell remains committed to empowering brokers and policyholders not only through robust claims support but also by providing resources that enhance cybersecurity resilience.

Cowbell Cybersecurity Resources

Cowbell equips policyholders to strengthen their cyber posture and avoid incidents through targeted services:

- **Cowbell Resiliency Services (CRS):** Comprehensive subscription-based support to enhance cybersecurity maturity, including Managed Detection and Response (MDR), penetration testing, training, and more.
- **Micro Pen Testing:** Quick, focused assessments identifying vulnerabilities.
- **Cowbell Rx Cybersecurity Marketplace:** Curated cybersecurity solutions from trusted partners.
- **Incident Response Plan Template:** A clear, actionable framework for efficient incident management.

Ready to better protect your clients?

Visit the Cowbell platform or connect with your Cowbell representative to access these and many other resources to guide your clients toward a stronger cybersecurity posture.

cowbell®

support@cowbellcyber.ai | (833) 633-8666 | **cowbell.insure**

US0072 0525