CYBER ROUNDUP

2026 Claims Report

Insights and trends from Cowbell's claims data

cowbell®

Executive Summary

While AI Accelerates Cyberattacks, Ransom Payments Drop Significantly

With geopolitical tensions and AI innovation defining the cyber threat landscape, the cyber insurance industry is feeling the impact. According to an AM Best Report, U.S. cyber insurance premiums declined for the first time to $9.14B, while claims rose 40%, signaling increased loss activity despite reduced premium volume.

This signals a more active risk environment, even as pricing adjusts. Ransomware remains a consistent part of that landscape, representing 19% of Cowbell claims between 2022 and 2025. At the same time, average ransom payments have decreased by approximately 44%, reflecting stronger negotiation strategies and more effective claims handling.

However, cyber risk today extends well beyond ransomware. Social engineering, phishing, business email, compromise, and supply chain vulnerabilities continue to impact organizations of all sizes. Meaningful protection of those threats needs to entail intentional resilience that consists of not just a comprehensive cyber insurance policy.

In the sections that follow, we share key claims trends, data-driven insights, and practical steps organizations can take to strengthen their resilience.

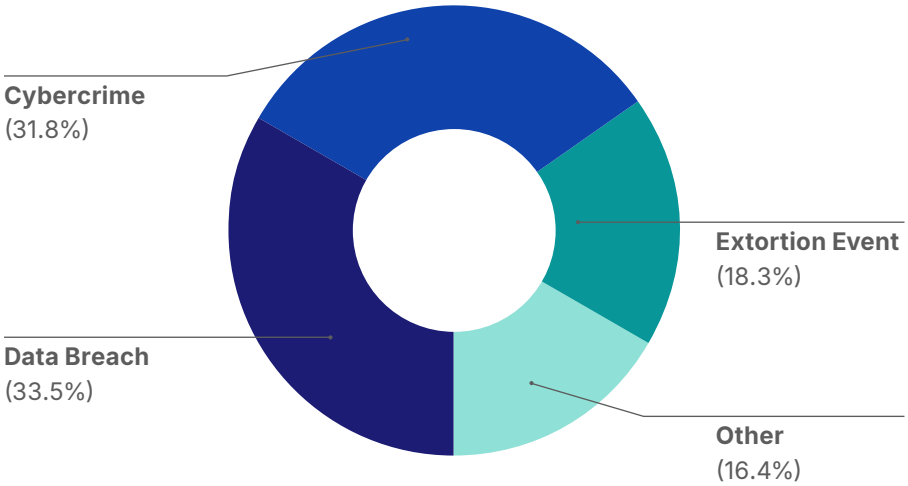
Note: Unless otherwise specified, Cowbell's claims data referenced in this report covers incidents from the last 18 months

Top Threats Driving Claims

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: data breaches, cybercrime, and extortion events.

Proportion of Claims by Incident Type



Data Breach (33.5%): Breaches involving unauthorized access or disclosure of sensitive information remain prevalent. These incidents often stem from stolen credentials and system vulnerabilities, with around 74–95% of breaches involving the human element, emphasizing the need for strong data security and rapid response measures.

Cybercrime (31.8%): These incidents typically involve financial or data theft through tactics like phishing, business email compromise (BEC), and funds transfer fraud, exploiting human vulnerabilities. As of early 2026, Business Email Compromise (BEC) remains one of the most financially damaging cybercrimes. These attacks exploit human trust through impersonation, AI-generated content, and social engineering to fraudulently obtain funds.

Fast Fact:

When it comes to cyber events, time is of the essence. The quicker a victim reports a claim, the better the chances for a swift recovery.

Extortion Event (18.3%): Ransomware and other extortion-based attacks continue to threaten operational stability by encrypting critical data and demanding payment for its release. These attacks are evolving from mere encryption to "double-extortion" and "data-only" schemes, where hackers threaten to leak sensitive information if demands are not met.

How Do Most Attacks Start?

Human error and manipulations prevail as the most common entry point for threat actors. Based on 2025 APWG data identifying approximately 3.8 million phishing attacks globally, phishing and spoofing remain the most prevalent cyber threats, underscoring the need for strong employee awareness, email security, and proactive threat detection as critical first lines of defense.

Often delivered at scale and designed to appear credible, threat actors continue to refine these scam tactics using AI, making messages more convincing and harder to detect.

Variants of phishing, like smishing (text messages) or vishing (phone calls) expand these risks across channels. These tactics are designed to exploit trust and create a sense of urgency to bypass security protocols. Practical defenses like multi-factor authentication (MFA), employee training, and rapid response, remain some of the most effective ways to reduce exposure.

Systemic Cyber Events on the Rise

Recent large-scale incidents like PowerSchools, Change Healthcare, TriZetto, and SonicWall serve as clear examples that many attacks do not start as isolated incidents. Instead, they highlight how systemic vulnerabilities can lead to a cascading effect, impacting multiple organizations simultaneously. These systemic events underscore the critical importance of maintaining a proactive risk management strategy. To minimize widespread damage, it is essential to implement multi-layered defenses and robust, rapid threat detection capabilities.

What Our Partners Say

"You handled the claim for our insured, and you did an excellent job—thank you. As we approach renewal, the client has chosen to remain with Cowbell, largely due to the strong support they received throughout the claim process."

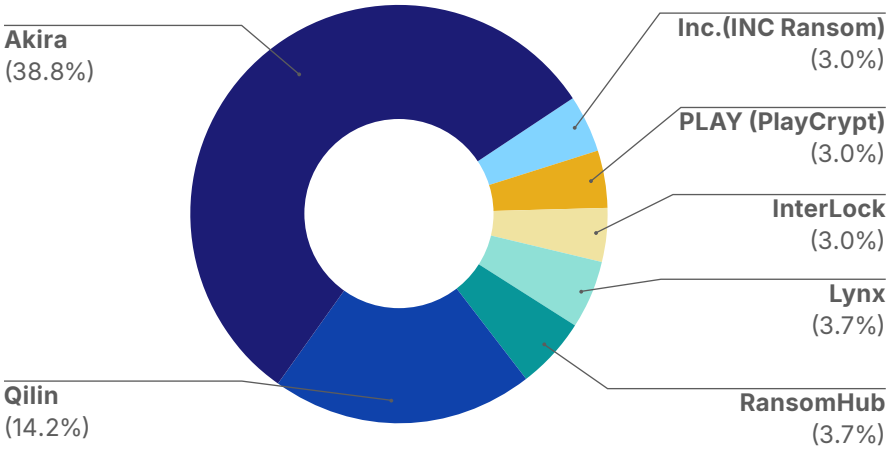
- Broker Partner

Ransomware Trends & Broker Insights

Ransomware Threat Actors Around the Globe

Ransomware threat actors are usually not individuals targeting organizations they have a personal vendetta against. Instead, they are highly sophisticated, often state-funded businesses with protocols and payroll. At Cowbell, we have identified the most notorious groups that are responsible for hundreds, if not thousands, of attacks every year.

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, more than two-thirds (69%) of the cases with identified threat actors involve just seven groups, with the top two threat actor groups making up more than half of the cases:

- **Akira (38.8%):** Double extortion ransomware targeting small and mid-sized enterprises (SMEs) via VPN and remote access exploitation.
- **Qilin (14.2%):** Ransomware as a service (RaaS) group using data exfiltration plus encryption against high-value enterprise targets.
- **RansomHub (3.7%):** Operates as a ransomware as a service group, enabling affiliates to carry out fast-moving, opportunistic attacks.

Fast Fact:

According to a Mimecast report, 95% of breaches involve human mistakes

Source: https://www.scworld.com/news/95-of-data-breaches-involve-human-error-report-reveals

- **Lynx (3.7%):** Emerging group targeting smaller organizations with rapid encryption and extortion tactics.
- **InterLock (3.0%):** Developing threat actor exploiting remote access weaknesses for data theft and extortion.
- **PLAY (PlayCrypt) (3.0%):** Targets large enterprises with tailored ransomware and data leak extortion techniques.
- **Inc.(INC Ransom) (3.0%):** Newer double extortion group focusing on organizations with less mature security controls.

In 2025, ransomware attacks surged by roughly 45% with Qilin and Akira emerging as dominant threats, often surpassing the previously prolific RansomHub and Lynx by mid-year. These groups utilize double extortion (encryption + data theft), targeting manufacturing and SMEs via unpatched VPNs (e.g., SonicWall) and remote access vulnerabilities, frequently operating from Eastern Europe.

What Brokers Should Know

For brokers, the specific identity of attackers matters less than the preparedness of their clients. Their methods are often similar, and effective defence measures will protect clients better against all of them. Cybersecurity solutions like Micro Penetration Testing, strong access controls, cybersecurity awareness training for all employees, and a robust backup strategy can be highly effective when it comes to minimizing the possibility and impact of a cyber event.

What Our Partners Say

"I want to express my appreciation—your support during our event was exceptional. You connected us with the right people and guided us through every step of the process, and it made all the difference."

- Policyholder

Industry Spotlight

Which Industries are Most at Risk?

Certain industries consistently face higher exposure due to the nature of their operations and data. Professional Services, Construction, Manufacturing, Healthcare, and Wholesale Trade all rely heavily on systems and sensitive information. This makes preparation and response planning especially important. Each sector faces unique challenges, but the goal remains the same: clear visibility into risk and practical steps to manage it.

Unique Risks by Sector:

- **Professional, Scientific, and Technical Services:** Large volumes of sensitive client data, including PII and proprietary information, increase exposure to data theft and extortion.
- **Construction:** Decentralized operations, subcontractors, and complex supply chains create multiple entry points for cyber incidents.
- **Manufacturing:** Reliance on production systems means attacks can halt operations, causing significant downtime and financial loss.
- **Health Care and Social Assistance:** Critical patient care systems and sensitive data increase urgency during incidents and elevate ransom demands.
- **Wholesale Trade:** Interconnected supply chains and high transaction volumes increase the risk of fraud, disruption, and third-party compromise.

If a policyholder suspects a cyber event, they should not hesitate to contact their insurer. There is no penalty associated with a “false alarm”; however, if they did fall victim, time is of the essence.

Fast Fact:

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

Claims at Cowbell

Moving with Expertise, Urgency, and Empathy

When a cyber event happens, clarity and speed matter most. Cowbell's in-house, global claims team, boasting a combined 90+ 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. Our hotline is monitored 24/7/365, including weekends and holidays. Notifications can be submitted via phone, email, or through the Cowbell Platform.

Outside of standard business hours, a dedicated claims team member is always on call to handle new reports. Additionally, our hotline is monitored by a breach counsel firm during weekends and holidays to ensure immediate 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 approach is simple: guide policyholders step by step, coordinate the right expertise, and help them move forward with confidence. We know these situations are stressful. Our role is to make the process clear, provide steady support, and focus on outcomes that help businesses recover.

What Our Partners Say

"The Insured is extremely impressed with the vendor team, the speed of the work being performed, and the professionalism and help received from Cowbell throughout the process. The Insured firmly stated he wishes to remain a Cowbell Insured."

- Broker Partner

Meet the Claims Leadership

Cowbell's claims leadership has a combined experience of over fifty years, and shines through expertise in cyber and management.

Mamta Birla, SVP & Head of Global Claims

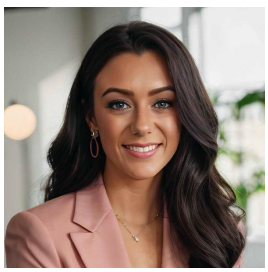
Mamta has been in the insurance field for over seven years, working directly in claims. She began her career as an Associate Claims Counsel with Hiscox Insurance, where she worked on the Cyber, Technology, and Media claims team. Prior to Hiscox, she practiced law at an employee benefits law firm.

Lili Knushaj, Director, Claims

Lili leads complex first- and third-party cyber claims, while working cross-functionally to align claims insights with underwriting and product strategy. Prior to Cowbell, Lili held senior cyber and professional liability claims roles at Chubb, managing complex E&O and excess liability portfolios. She holds an LL.M. in American Business Law and a Bachelor of Laws, and is a licensed Texas Adjuster.

Stephanie Hewerdine, Director, Claims

Stephanie has over six years of experience in senior positions within the cyber insurance industry, most recently serving as a Claims Counsel at Coalition and managing a claims team at Segwick. Prior to working directly for insurance carriers, Stephanie was a trial attorney for 25 years, supporting insurance carriers in litigation and advisory roles, and was a full-time law school professor.



Kirsten Maley, Director, Claims UK and Australia

With more than a decade of insurance industry experience, most recently as Senior Claims Adjuster for cyber at CFC, Kirsten brings expertise in complex claims management, incident response coordination, and regulatory knowledge across multiple jurisdictions. She oversees Cowbell's UK and Australia claims operations to drive the company's claims process and deliver market-leading customer service to clients, brokers, and insureds.

Conclusion & predictions

Industry Claims Prediction for the remainder of 2026

Staying ahead of the cyber threat landscape can help businesses better prepare themselves for attacks. Based on current industry trends and expert insights, we anticipate:

- **Emergence of New Threat Actors:**
  Smaller, younger groups driven by financial gain and notoriety will continue to enter the landscape, while major groups like Akira, Qilin, and Scattered Spider face increased law enforcement pressure.
- **Continued Targeting of Professional Services:**
  Law firms remain a top target due to highly sensitive data and often outdated security controls, such as legacy systems and weak authentication.
- **Rise in Advanced Social Engineering:**
  Attacks are shifting beyond email, with threat actors increasingly using AI to enhance phone-based impersonation and multi-channel attacks to steal credentials.
- **Growth in Litigation Exposure:**
  Third party claims and class actions are expected to increase following cyber incidents targeting companies for inadequate security and failure to disclose breaches.
- **Ongoing Business Interruption Losses:**
  Business Interruption (BI) and Contingent Business Interruption (CBI) claims remain a primary driver of insurance losses in 2026, ranked as a top-three global risk by the Allianz Risk Barometer 2026. Driven by cyber attacks, complex supply chain dependencies, and climate-related events, these losses are amplified by inflationary pressures on repair costs and extended downtime.
- **Shift in Ransom Dynamics:**
  Ransomware dynamics have shifted significantly, with decryption payments declining as victims improve backups, while data extortion and suppression payments rise due to the proliferation of double-extortion tactics.

Fast Fact:

We reduce ransom amounts by an average of 65% through negotiations with the threat actors*.

*Average ransom reduction of 65% is based on historical data from negotiations. Actual results vary significantly based on individual circumstances, threat actor behaviors, and specific negotiation contexts.

Conclusion: In the Age of AI, Cyber Resilience Must Become Standard Business Practice

Cyber risk is now part of doing business. Attacks are not limited by size or industry, and the pace of change continues to accelerate. The good news is that preparation works. With the right combination of coverage, insight, and support, businesses can reduce their exposure and respond effectively when incidents occur. At Cowbell, we believe protection should create confidence, not complexity. By making cyber risk easier to understand and manage, we help brokers and businesses focus on what matters most: keeping their operations strong and moving forward.

This also means that the broker role needs to evolve from just providing their clients with access to a cyber insurance policy to an educator around the resources that insurance providers offer, often at no additional charge, to help boost clients' cyber resiliency. The result will be improved client satisfaction, fewer and less severe claims, and an overall more secure American economy.

Ready to better protect your clients & elevate your brokerage?

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.

Resources

Stay Informed, Stay Ahead

Cowbell offers more than just a policy. We equip your clients to strengthen their cyber posture and avoid incidents through targeted services:

- Cowbell Resiliency Services (CRS): Comprehensive complementary and subscription-based support to enhance cybersecurity maturity, including Managed Detection and Response (MDR), penetration testing, cybersecurity awareness training, and more.
- Micro Pen Testing: Quick, focused assessments identifying vulnerabilities.*
  *First test available at no additional cost.
- Cowbell Rx: Curated cybersecurity solutions marketplace from trusted partners.
- Incident Response Plan Template: A clear, actionable framework for efficient incident management.

For detailed insights, explore our claims case studies:

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

Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.

cowbell®

US0039 0426