PUBLICATION

Cybersecurity Awareness Month 2025: Avoid Cyber Claims Scares

Authors: Matthew George White, Alexander Frank Koskey, III
October 14, 2025

October is Cybersecurity Awareness Month – a perfect time to take stock of what's really driving today's cyber losses and how your business may be affected. NetDiligence's 2025 Cyber Claims Study, analyzing more than 10,000 incidents from 2020 – 2024, paints a clear and costly picture: attacks are getting more expensive, business interruption and recovery costs are rising, and ransomware and business email compromise (BEC) continue to dominate the threat landscape.

Key Findings:

- Ransomware remains the top driver of loss, responsible for nearly half of all major incidents. Average ransom demands reached record highs – some as high as $150 million, with payments up to $75 million.
- BEC attacks surged in 2024, with nearly 470 reported incidents, many tied back to a single click on a malicious link. The average cost per BEC claim was $75,000, but the total impact often far exceeds that when recovery and legal expenses are included.
- Small and midsize enterprises (SMEs) – those under $2 billion in revenue – accounted for 98 percent of all claims and 49 percent of total losses, but their average incident cost jumped nearly 30 percent to $264,000.
- Business interruption and recovery expenses drove massive cost increases, especially in ransomware-related claims. For SMEs, incidents involving downtime averaged $1.8 million, more than 250percent higher than non-BI events.
- Criminal activity caused 98 percent of incidents, underscoring the growing sophistication and persistence of threat actors.
- Third-party and supply chain incidents are rising, with cascading effects across industries – especially when a single vendor supports multiple clients.

Why It Matters:

The study reinforces what we see daily in breach response and litigation: the risks of financial and operational fallout from a cyber incident are growing exponentially – and many businesses are underprepared. Even well-prepared companies are struggling with mitigating vendor risk, adapting to new and evolving threats, engaging in ransom negotiations, and withstanding operational system downtime. For SMEs, one major incident can be business-ending.

Action Items:

- *Update and test your incident response plan.* Tabletop exercises are no longer optional – they're your best way to uncover gaps before threat actors do.
- *Reassess your cyber insurance coverage.* Rising costs and retentions mean organizations must know what's covered – and what's not – before a breach.
- *Harden identity and payment controls.* Multifactor authentication, least privilege access, and dual authorization, especially for payments, remain the most effective frontline defenses.
- *Demand vendor accountability.* Supply chain exposures are now systemic; require your vendors to maintain equivalent security and recovery standards.

Final Takeaway:

Cyber events are no longer isolated "IT problems" – they're enterprise-wide financial risks. Whether you're a bank, hospital, manufacturer, or professional services firm, this year's data confirms that preparation, resilience, and legal readiness are the best investments you can make.

If your organization hasn't updated its cyber incident response plan or reviewed its insurance coverage recently, now is the time. The authors, Matt White and Alex Koskey, routinely help clients design, test, and strengthen their defenses – before the next incident hits. If an attack happens, we can guide you through the breach response, mitigate risks, and help you navigate the legal and regulatory landscape following the attack. For more information or if you have any questions, please contact Matt White, Alex Koskey, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.

October is National Cybersecurity Awareness Month

Observed annually in October, Cybersecurity Awareness Month is a collaborative effort between the public and private sectors to raise awareness about cybersecurity. It was launched in 2004 by the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA).

Throughout Cybersecurity Awareness Month, we will provide proactive tips and information in order to mitigate your cyber risks.