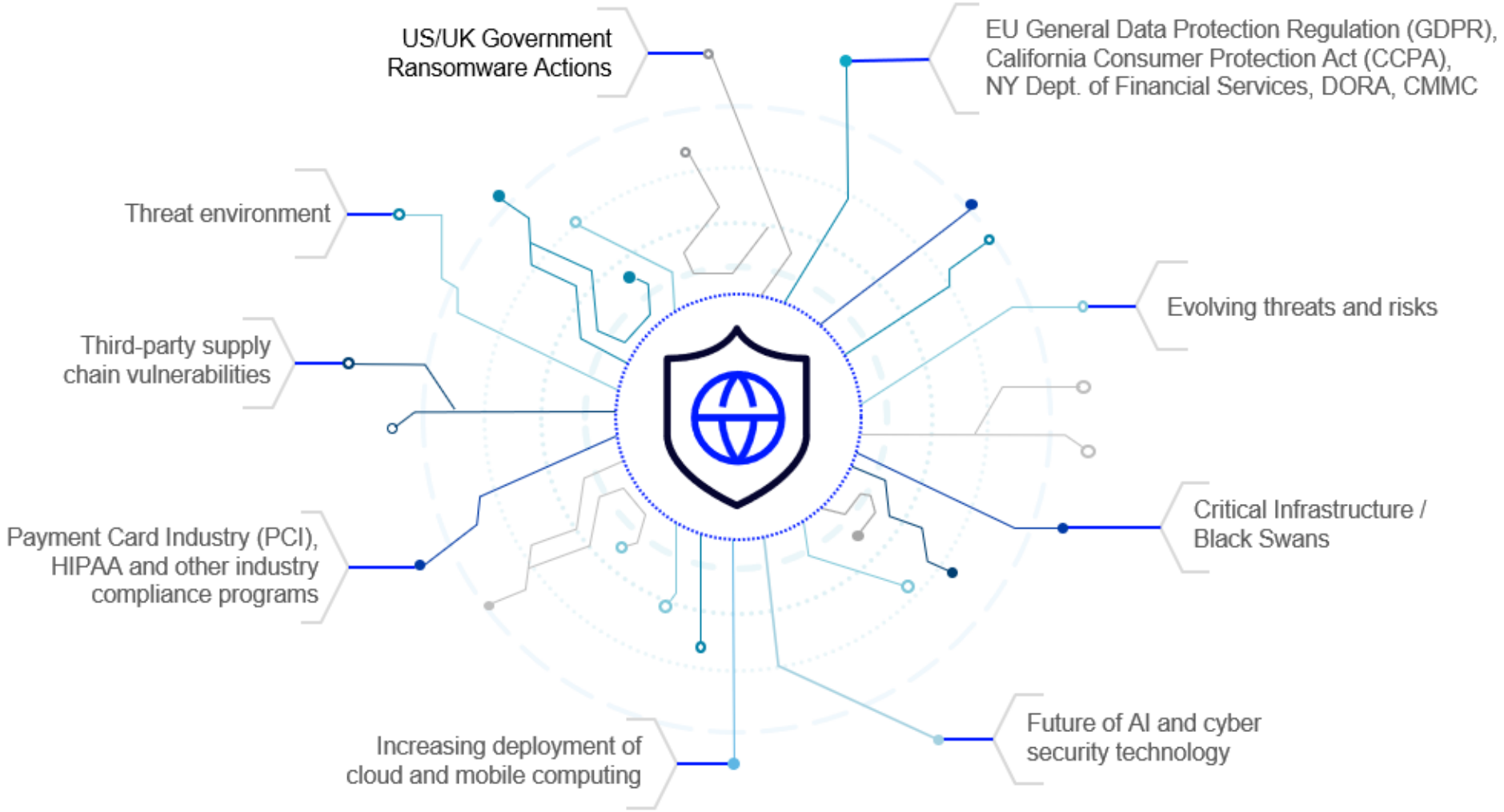
FEI Madison March 2026 Chapter Meeting

Cybersecurity: One Year Later

Complexity of the Cyber Challenge

Cyber Risk Requires Enterprise-Wide Approach



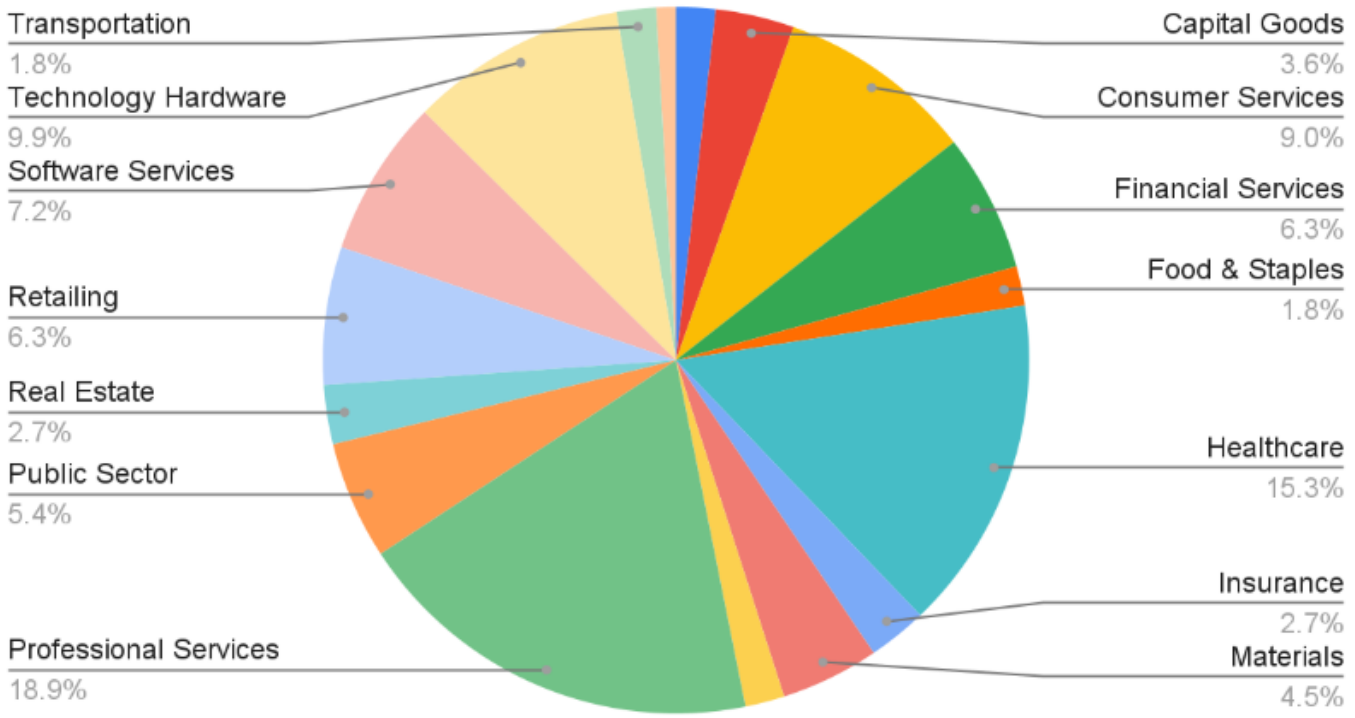
Observed Ransomware Event Trends

Q4 2025

Size of Company Impacted

Employee Count	Percentage Frequency
50,001+	2.80%
25,0001-50,000	1.80%
10,001-25,000	5.40%
1,001-10,000	17.10%
101-1000	30.60%
11-100	37.80%
Up to 10	4.50%

Ransomware Victims by Sector



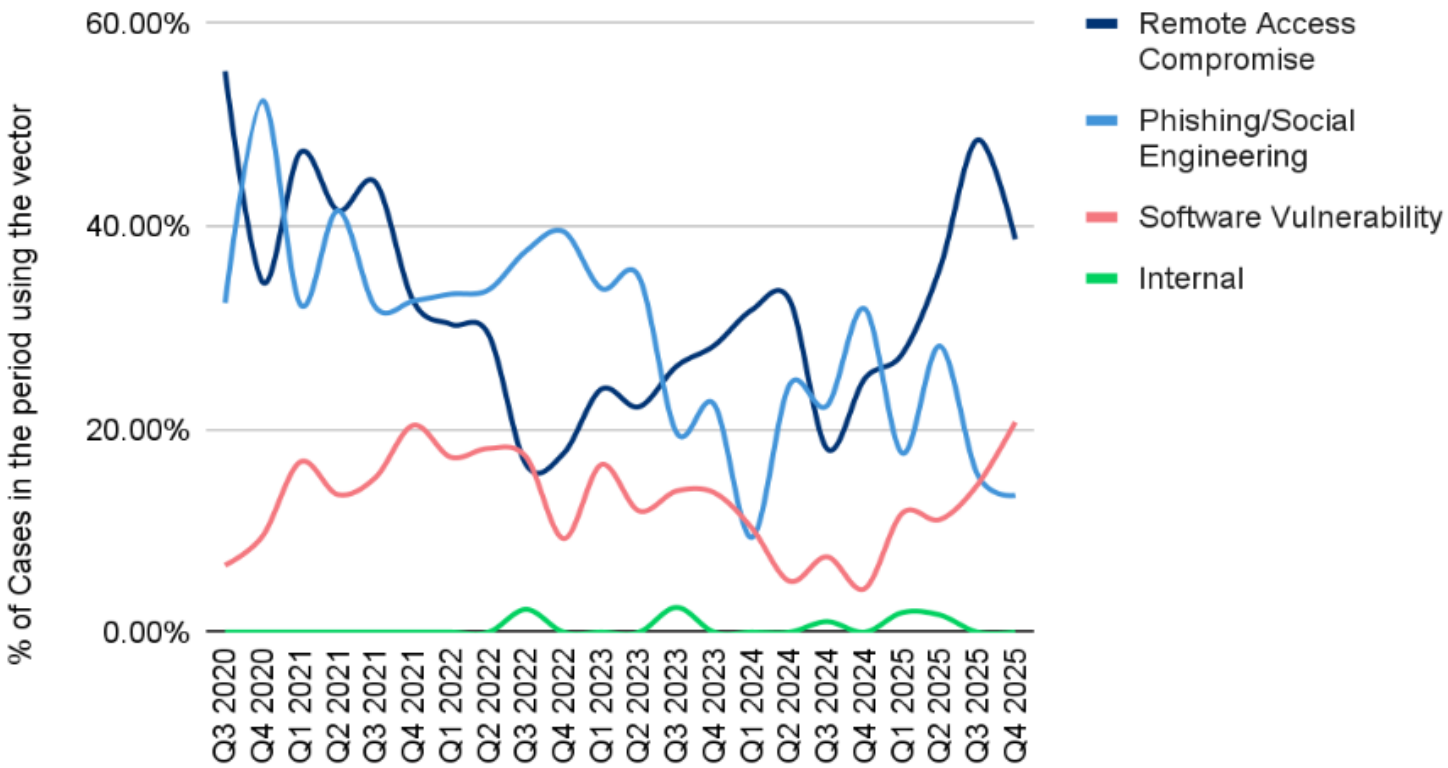
Observed Ransomware Event Trends

Q4 2025

Top Ransomware Groups

Group	Market Share
Akira	14%
Qilin	13%
Lone Wolf	12%
C10P	7%
Silent Ransom	6%
Shiny Hunters	4%

Most Common Attack Vectors



Cyber Event Financial Trends

Q4 Ransomware Case Outcomes

Overall Percentage of Companies Paying Ransoms

20%

Percentage of Data Exfiltration Victims Paying Ransoms

25%

Average Payment

$591,988

Median Payment

$325,000

Average | Median | Largest

	Initial Ransom Demand	Ransom Paid	Days to Acceptable Restoration	Forensic Investigation Cost	Individuals Notified
BUSINESS & PROFESSIONAL SERVICES	$2,184,074 $775K | $15M	$352,811 $250K | $1M	9.1 9	$35,165 $14.5K | $330K	1,252 104 | 19K
EDUCATION	$996,543 $725K | $1M	$98,948 $98,948 | $100K	13.4 10	$53,878 $35,488 | $318K	2,088 249 | 18.7K
ENERGY & TECHNOLOGY	$1,852,856 $303K | $10M	$235,139 $111K | $750K	10.1 7	$60,981 $33.6K | $241K	16,653 1,300 | 96K
FINANCE & INSURANCE	$6,997,473 $285K | $40M	$6,750,749 $150K | $20M	8.4 7	$29,895 $10.5K | $590K	33,236 409 | 2.158M
GOVERNMENT	$544,906 $650K | $1M	$600,000 $600K | $600K	13 12	$48,775 $34,275 | $148K	1,007 513 | 4K
HEALTHCARE	$1,889,573 $1.4M | $7M	$847,875 $375K | $2.5M	27.2 24	$36,314 $14,750 | $226K	58,520 876 | 2.151M
MANUFACTURING	$4,951,440 $1.75M | $28.7M	$562,857 $180K | $3M	10.3 10	$49,784 $21,575 | $439K	1,379 263 | 23K
NONPROFIT	$187,500 $187.5K | $350K	$150,000 $150K | $150K	7 7	$19,767 $10.5K | $114K	2,585 47 | 16K
RETAIL, RESTAURANT & HOSPITALITY	$2,360,071 $1.95M | $8.2M	$840,286 $743.5K | $1.8M	9.3 9	$50,482 $34,133 | $240K	81,384 400 | 1.96M

Source: Baker Hostetler 2025 Data Security and Incident Response Report and Coveware Q4 2025 Quarterly Report

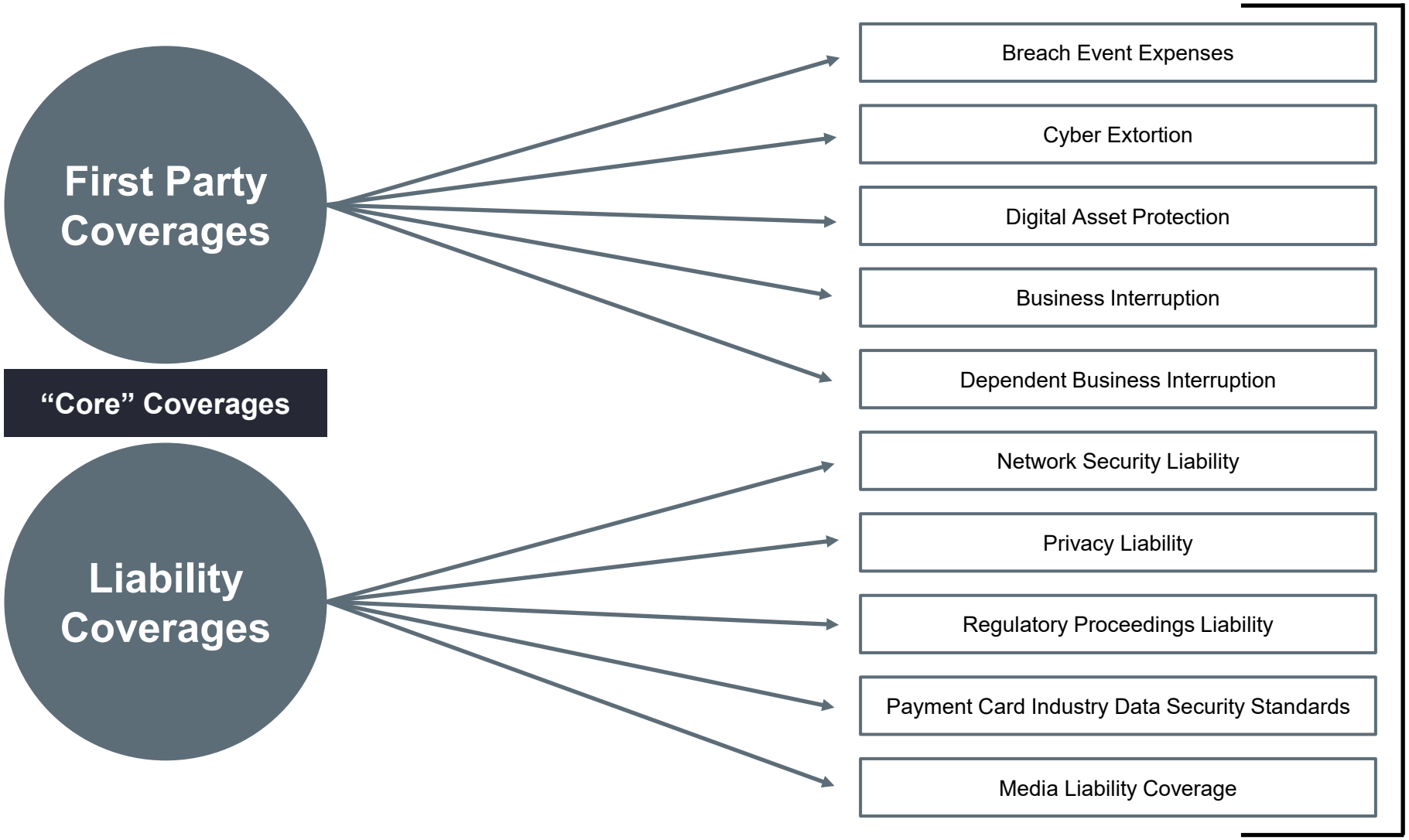
AON LevelBlue

Access Claim Trends

Marketplace Minimum Expectations

Multi-Factor Authentication (MFA)	Endpoint Detection and Response (EDR)	Phishing Exercise/ Cyber Awareness Training
Vulnerability Scanning & Patch Management	Secure RDP/VPN	Incident Response Plan/ Ransomware Exercise
Access Control/ Service Accounts	Disaster Recovery/Backups	Email Filtering & Security (DMARC / DKIM)
Zero Day Vulnerabilities and Supply Chain Risks	Network Segmentation/ Network Monitoring	M&A Due Diligence and Integration

Cyber Coverage



The Ransomware Effect

Potentially Impacted Insuring Agreements Stemming From a Ransomware Event

1st Party Insuring Agreements

Cyber Extortion	Reimbursement coverage for any extortion payment. **Tie-in** – Social engineering (whaling, spear phishing) and invoice manipulation are both direct phishing attempts.
Reputational Harm	Reimbursement coverage for loss income as a result of an adverse media report of a privacy incident. **Tie-in** – Ransomware groups hold all sorts of privacy records (Ex. Conti held passports for ransom). These threat actors intentionally exfiltrate data to initiate payment faster.
Network Business Interruption	Reimbursement coverage for net income loss, caused by computer system outage (Security or System Failure). **Tie-in** – Ransom negotiations can often become drawn out and result in a direct hit on the business's net income. 1st party business interruption coverage can help combat this element of an attack.
Computer Hardware Replacement / Bricking	Reimbursement coverage for insureds replacement of computer hardware due to unauthorized reprogramming/**ransomware** **Tie-in** – Ransomware or malware has the capability to corrupt and ruin all electronic equipment, turning the device into a 'brick'.
Digital Asset Protection	Reimbursement coverage for the insured for non-physical assets (software and data). **Tie-in** – Most ransom payments correlate with non physical assets being held hostage, similar to a network security failure.
Breach Event Expenses	Reimbursement coverage for insured's costs to respond to security incident . **Tie-in** – When ransomware is paid out, expenses can include computer forensics, legal expenses, expenses related to advertising.

3rd Party Insuring Agreements

Network Security Liability	Liability coverage for damages suffered by others stemming from a network security failure (confidential info, unauthorized access). **Tie-in** – Once the threat actors deploy malware and begin exfiltrating/holding an organization's data hostage, a large amount of that data may be 3rd Party information (client data), and can result in liability suits against the insured.
Privacy Liability	Often included in conjunction with Network Security Liability, Privacy Liability provides coverage for damages suffered by others to protect confidential 3rd party info. **Tie-in** – Data exfiltration is a key component of modern-day ransomware attacks, especially against organizations who house a large amount of sensitive 3rd party information.
Regulatory Proceedings Liability	Liability coverage for defense costs brought by a government agency/regulatory body due to a failure to protect private information. **Tie-in** - Third party coverage for actions/ investigations resulting from a violation of privacy law. If a government agency was to have a cyber breach; Ex, Police Department's files corrupted, would have to implement the regulatory proceedings coverage. Also will typically include coverage for GDPR, CCPA, and/or other state privacy laws where applicable.

Major Market Topics

Artificial Intelligence	• Cybercriminals leverage artificial intelligence (AI) and machine learning to automate and scale attacks. • Significant data privacy risks exist when AI tools and platforms are used to increase efficiency without proper governance or monitoring. • Many software development AI tools are trained on open-source code, which can constitute unlicensed use and may lead to copyright infringement claims. • Insurers are interested in understanding how organizations are using AI to enhance and expand their cybersecurity defenses. • Many cyber policies are 'silent' when it comes to AI-related claims or losses. However, many insurance carriers are now adding affirmative coverage endorsements or specific AI exclusions. AI coverage and gaps are evolving constantly.

Global IT Events & Supply Chain Risks	• 2025 saw several potential catastrophic cyber events. The financial impact on the global cyber insurance market, while still being adjusted, is expected to be minimal.
	• 2025 Notable Events:
	  ○ Jaguar Land Rover: The automotive company fell victim to a cyberattack on August 31, 2025, forcing a shutdown of global IT systems, resulting in the suspension of production at some plants and a reduction in retail operations. While some impacted plants are up and running, as of October 7, 2025, production lines are not yet back to normal.
	  ○ Collins Aerospace: A third-party service provider for airport check-in and boarding systems experienced a ransomware event in September 2025, causing significant cyber-related disruptions and delays to several busy European airports.
	  ○ Oracle Vulnerability: Cl0P ransomware group exploited a zero-day vulnerability in September 2025, affecting a product within Oracle E-business Suite, exposing thousands of organizations to malicious activity and data theft.
	  ○ SalesLoft Vulnerability: A threat actor utilized compromised OAuth credentials to exfiltrate data from affected customers' Salesforce environments, resulting in data exfiltration and extortion events.
	• Organizations can expect cyber insurers to have a heighted focus on the usage and management of supply chain vendors and cyber security platforms.

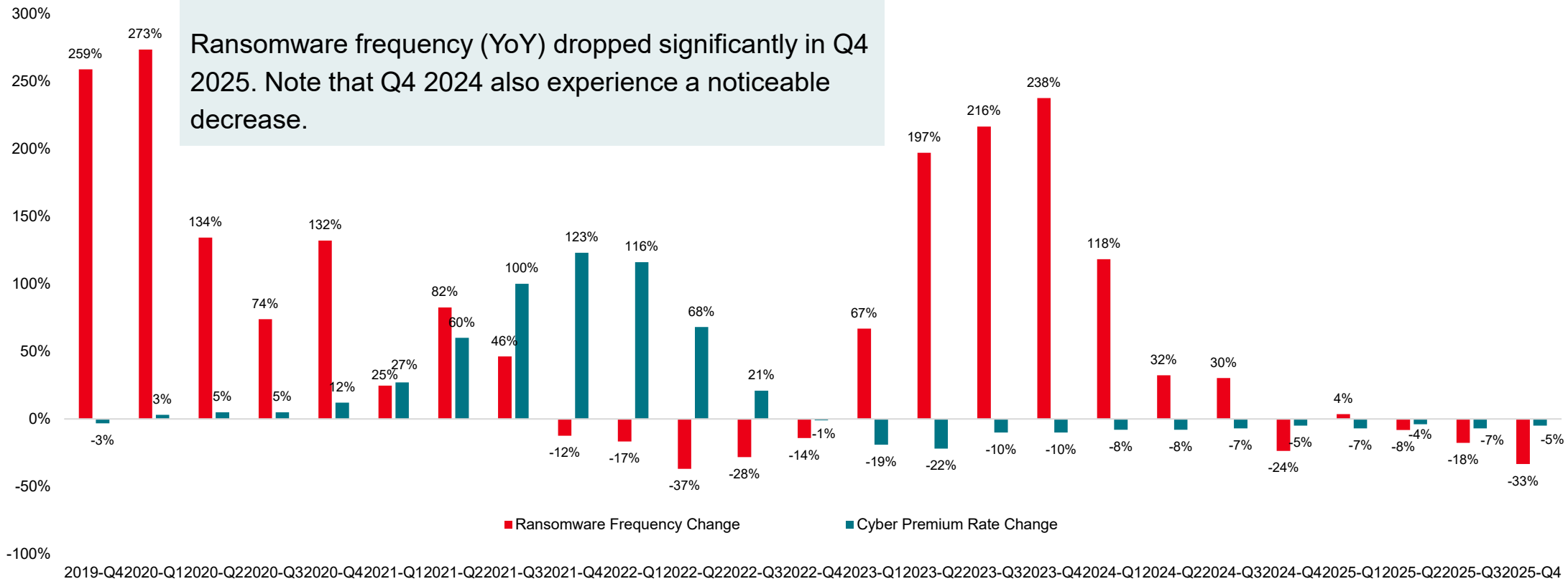
Privacy Litigation	• Privacy regulatory exposures around the world continue to become restrictive, as privacy laws are added or expanded. • Privacy claims related to website tracking, pixel tracking, CIPA, VPPA and BIPA continue to increase and are proving to take years to settle. • Insurers are continuing to review policy language and coverage related to wrongful or unlawful collection, and some insurers only offer defense costs coverage and exclude damages and settlements.
Ransomware	• Ransomware activity driven by groups like Scattered Spider accelerated in certain industry classes, such as insurance companies, airlines, and retailers (in the UK), in Q2 2025. This created heightened awareness, increased loss activity, and additional underwriting diligence for cyber insurers writing these classes of business. • Dependent Business Interruption is a significant concern for insurers as large vendor incidents can trigger numerous policies, as a result of a single extortion event. • Insurers are continuing to grapple with underwriting to systemic events that can lead to aggregation issues.

Ransomware Frequency & Cyber Premium Rates

Year-over-Year Change

Q4 2025 continued the year-over-year rate decrease.

Ransomware frequency (YoY) dropped significantly in Q4 2025. Note that Q4 2024 also experience a noticeable decrease.



Source: Flashpoint, analysis by Aon. Data as of 1/1/2026; Claim count development may cause these percentages to change over time

Key Recommendations

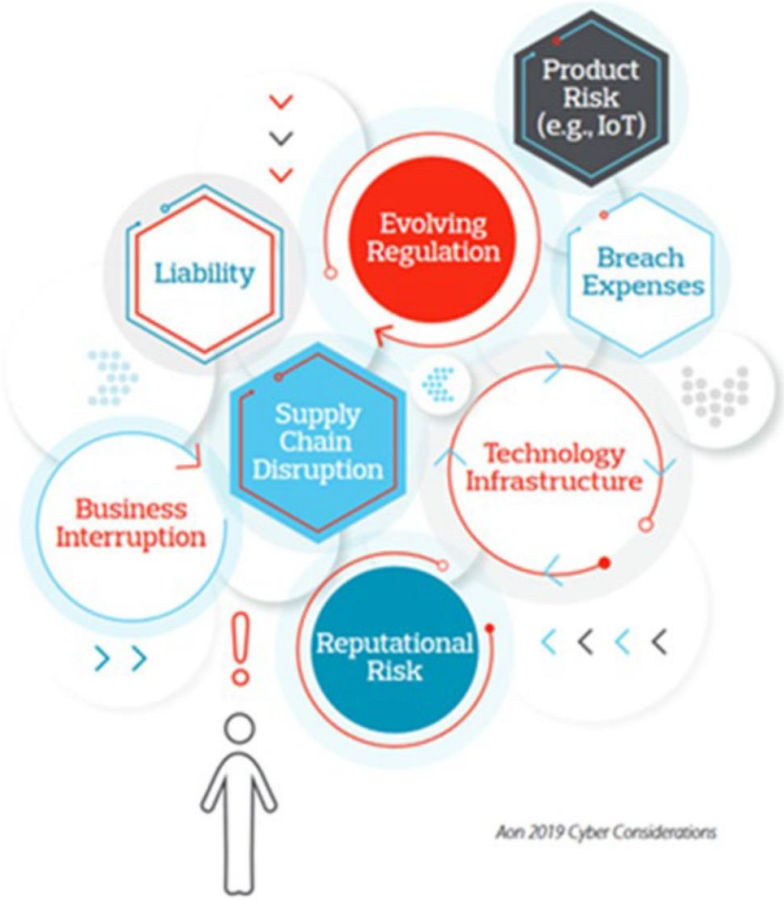
Know Your Partners

Recommended Relationships

1. Breach Coach/Outside Legal Counsel
2. Digital Forensics and Incident Response Firms
3. Cyber Insurance Carrier

Potential Ancillary Pull Through Providers

1. IT MSP/IT Restoration
2. Ransomware Negotiators and Payment Services
3. Notification Providers
4. Public Relations Firms
5. E-Discovery/Privacy Review
6. Forensic Accounting



Phishing on the Rise, AI Enhancing Its Impact

AI has become a common component of phishing campaigns

- Phishing remains a prevalent threat
  - 94% of organizations report being hit with phishing attacks
  - Most common ransomware attack vector 2025
  - There was 202% increase in phishing emails in the second half of 2025
- 2025 Reporting, 82% of phishing emails use Artificial Intelligence (AI). This represented a 60% year over year increase
- AI-powered phishing can quadruple victim click through rated compared to traditional phishing

Traditional Phishing	AI – Powered Phishing
Generic message sent to target	Personalized message sent to target
Created using a combination of human input and automation	Large Language Models (LLMs) can incorporate near real-time content from public data sources to create tailored emails
Spelling and grammatical errors	Little to no spelling/grammatical errors
Static	Evolving
Lower click rate	Higher click rate
Easier to detect by user	**Harder to detect by user**

How Organizations Can Guard Against AI-Powered Phishing Attacks

Addressing Human and Technical Countermeasures

Organizational Perspective

Human Component	Technical Component
Security Awareness Training	Anti-phishing software with LLMs
Phishing exercises that include feedback to employees	Advanced email filtering
Financial controls processes	Ensure proper configuration of email security standards (SPF/DKIM/DMARC)

Individual Perspective

Human Component
Individual Vulnerability Assessment
Online Takedowns
Limit sharing of personal information online

Supply Chain & Supplier Cyber Risk

Risk Management & Mitigation Measures

- Audit your supplier's cyber security
- Understand criticality of your supplier and potential disruption
  - Business Impact assessment
- Monitor suppliers' cyber security risk
- Supplier relationship management (contract elements)
  - Expectations of cyber security
  - Measure expectations
  - Compliance metrics
  - Responsibilities; notification requirements
- Share Best practices with Suppliers
- Business Continuity planning

Roles and Responsibilities

Management v. Board

MANAGEMENT

- Educate Board on cybersecurity risk; provide access to outside cybersecurity experts as appropriate
- Understand cybersecurity risk posture
- Ensure cybersecurity risk is addressed enterprise-wide
- Establish framework and infrastructure to support collaboration throughout to identify and mitigate cybersecurity risk
- Ensure allocation of sufficient human and capital resources
- Develop and implement incident response, disaster recovery, and business continuity plans and processes

BOARD

- Exercise good faith, care, and loyalty
- Engage in enterprise-wide risk oversight
- Understand the strategic importance of IT to business operations and associated risk
- Ensure Management has placed qualified people in leadership roles and appropriately allocated resources to mitigate cybersecurity risk
- Understand incident response framework
- Ensure Management is enforcing an enterprise-wide cybersecurity risk management program and developed appropriate risk management policies
- Remain informed of threats, vulnerabilities, and incidents

Questions

Will Miller
Aon
william.miller@aon.com
+1 920 621 5904

Dave Collier
LevelBlue
david.j.collier@levelblue.com
+1 312 320 6426

Jacob Mast
Aon
jacob.mast@aon.com
+1 262 424 7634

AON LevelBlue