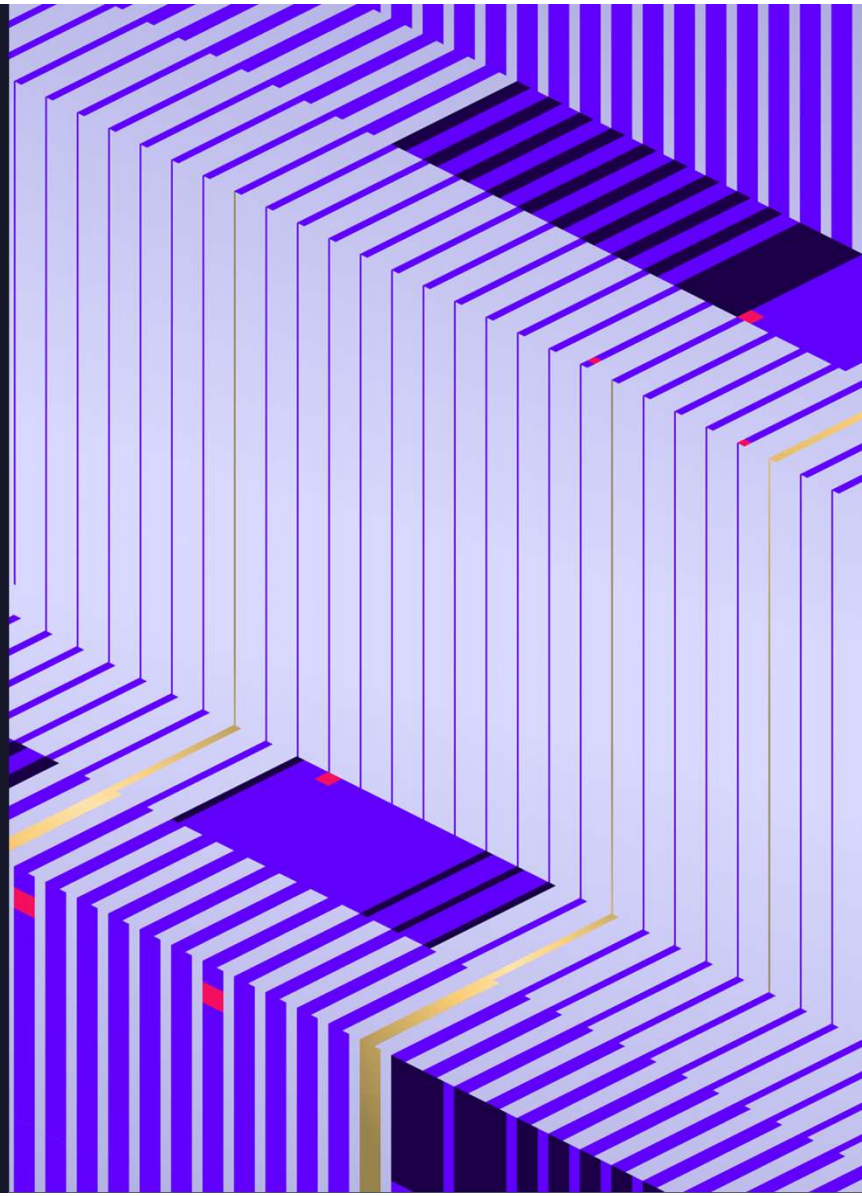
Charleston CyberLaw Forum

January 23, 2025

SentinelOne Secure Tomorrow

CHARLESTON SCHOOL OF LAW

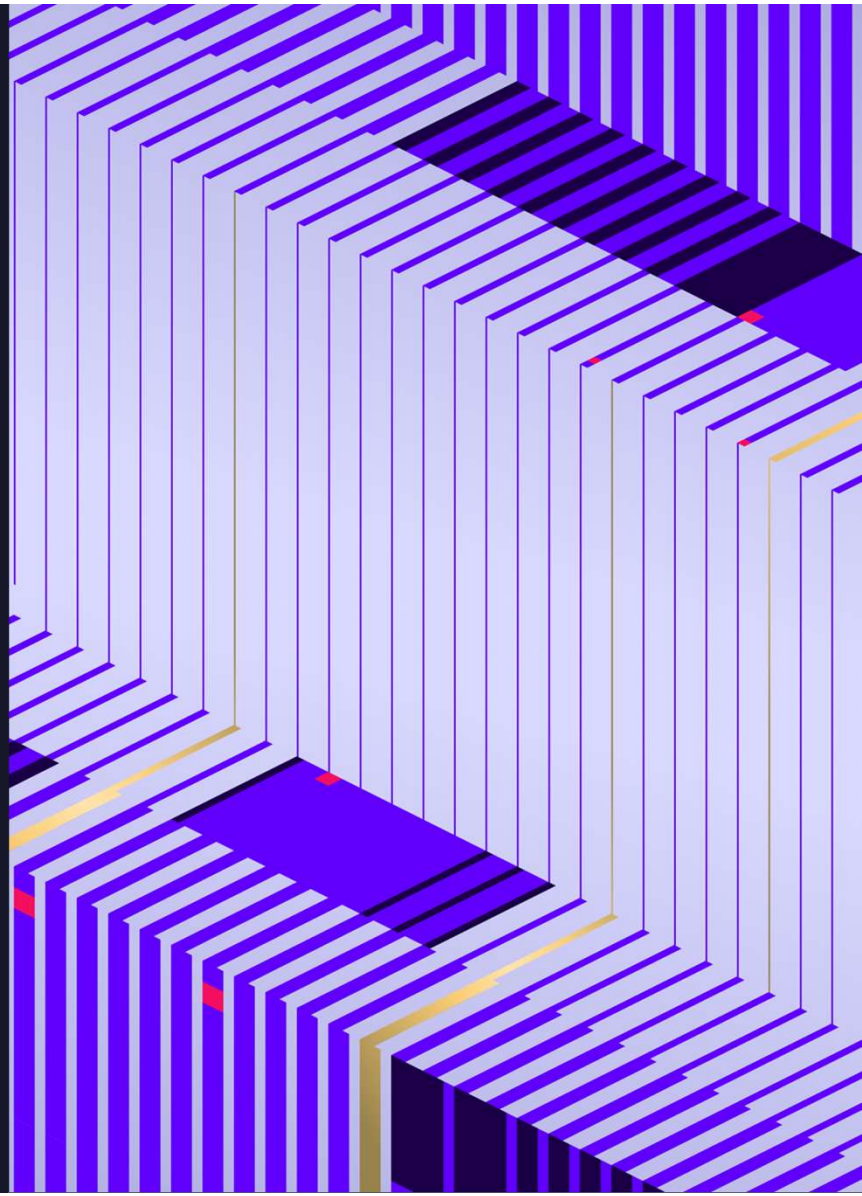


State of the Cyber Insurance Market: Securing Coverage, Premiums & Controls

The CLE materials are sponsored by SentinelOne and Charleston Law School. All CLE materials are prepared by law firms and attorneys as noted in the materials, and do not offer any specific legal advice or guidance.

SentinelOne
Secure Tomorrow

CHARLESTON
SCHOOL OF LAW



Presenters

Chris Keegan

Sr. Managing Director
Brown & Brown

Tiffany Calhoun

Deputy Head of Cyber, Tech & Media
Allianz

Sezaneh Seymour, PhD

VP Head of Regulatory Risk &Policy
Coalition

Brandon Russ

Cyber Claims Specialist
CFC

Presentation Agenda

- IT Controls, Insurance Premium & Term
- Insurance Involvement in Event Response
- Government Insurer Cooperation

SentinelOne

SentinelOne Secure Tomorrow

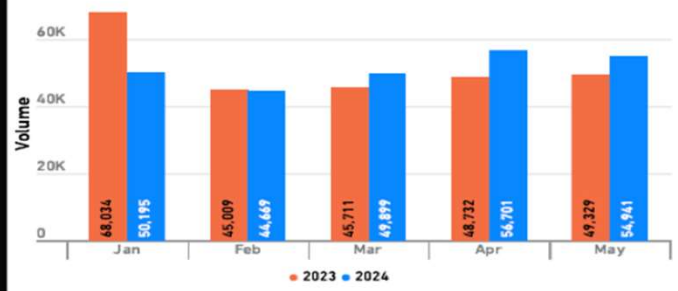
CHARLESTON SCHOOL OF LAW

Cyber Incident Costs & Trends

INCIDENT COST BY REVENUE SIZE 2019-2023

Revenue Size	Claims	Minimum	Average	Maximum	Total
Nano-Rev (<$50M)	3,891	1K	139K	10.4M	539.3M
Micro-Rev ($50M–$300M)	1,584	1K	317K	10.4M	502.7M
Small-Rev ($300M–$2B)	405	1K	1.8M	108.0M	746.8M
Mid-Rev ($2B–$10B)	112	1K	4.7M	111.0M	530.6M
Large-Rev ($10B–$100B)	42	10K	33.3M	503.5M	1.4B
Mega-Rev (>$100B)	3	10.6M	26.1M	55.0M	78.2M
Unknown	2,401	1K	50K	2.7M	120.9M

GLOBAL RANSOMWARE STARTED TO RISE IN 2024



Source: Mid-Year 2024 SonicWall Cyber Threat Report

Coverage, Premiums and Controls

Coverage:

- Process: securing coverage is a highly dynamic process and tailored to ensure that companies receive appropriate coverage that aligns with their specific risk exposures.
- Terms: terms are also customized, and the result of a detailed underwriting process

Premiums: Cyber insurance premiums are a function of risk and coverage

Risk Assessment:

- What specific cyber risks does a company face?
- Insurers may look to established cybersecurity frameworks to determine necessary controls and coverage levels (NIST, ISO)

Controls:

- Advanced cyber insurers go beyond, to mind their own claims data, have their own threat teams, and use technology like external scans or APIs.

Insurance Involvement in Event Response

Claims

- What are insurers expectations for involvement in managing claims?
  - Legal - Data Breach Notification, Evidence Preservation, Legal Advice/Comms, Third Party Mgt
  - Regulatory - Compliance Requirements, Reporting, Audit & Documentation, Cross Border Considerations
  - How does it change between different carriers and account size or industry?

Ransomware

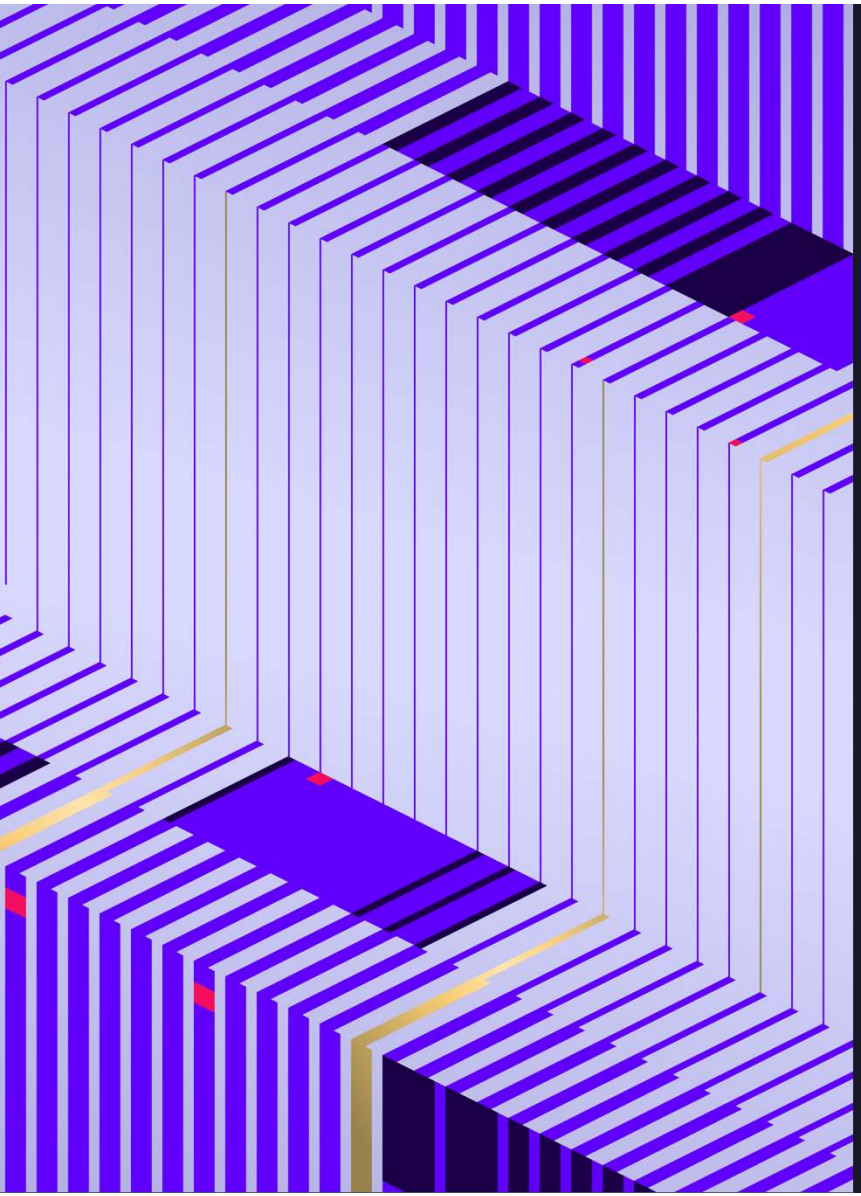
- What are underwriters' views on paying ransomware and what involvement do insurers want? Have Ransom payment bans evolved?

Liability

- Cyber and D&O suits arising from cyber events.

Government Insurer Co-operation

- How should insurers collaborate with government agencies, and how do these partnerships affect policyholders?
  - Information Sharing
- Supply Chain Security and Vendor Assessments
- Data Privacy/Security and Software Liability
- How are the participants evaluating systemic risk?
- What level of support should businesses anticipate from government agencies?
  - Federal Cyber Insurance Program and "Backstop"



SentinelOne
Secure Tomorrow

Thank You

Sentinelone.com

Chris Keegan

Sr. Managing Director, Brown & Brown

Brown & Brown

Chris places network, privacy, technology and media E&O insurance for a wide variety of companies including financial institutions, authentication providers, manufacturers, healthcare, retail and telecommunications companies. Christopher has also executed Cyber Information Risk Assessment projects and worked with regulators on evaluation of E-Business risks. Prior to joining Beecher, Christopher was a National Resource at Willis for Cyber and E&O and a leader of the Information Risk Advisory Practice at Marsh focusing on Privacy, Technology, Media, Network Intellectual Property and Professional Liability insurance products.

Tiffany Calhoun

Deputy Head of Cyber, Tech & Media, Allianz

Tiffany Calhoun is the Deputy Head - Regional Product Leader of Cyber, Tech & Media for Allianz Commercial in North America. Based in Atlanta, Tiffany is a passionate Cyber and E&O-focused insurance professional with experience on the commercial carrier and captive sides of the insurance industry. Tiffany has 15 years of insurance industry experience focused on Cyber, Tech, Media and traditional E&O throughout this time. In addition to insurance placements, Tiffany has experience with global fronting and reinsurance structures. Prior to joining AGCS, Tiffany recently was the Underwriting Manager for L&F Indemnity, Ltd., PwC Global's Bermuda-based captive overseeing the cyber, E&O, D&O and EPLI placements. She has also held positions at Sompo International and ACE USA. Tiffany has a dual major from Temple University with a focus on Actuarial Science and Risk Management and Insurance.

Sezaneh Seymour

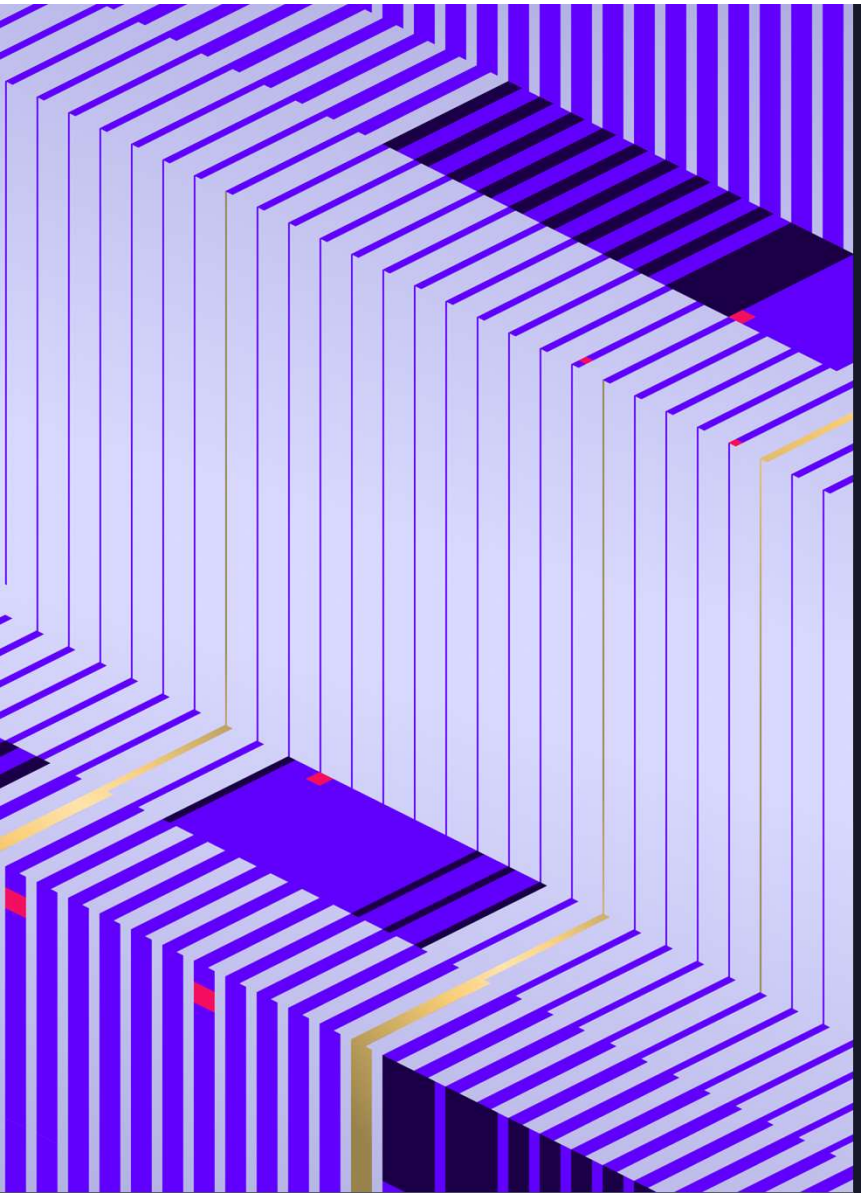
VP and Head of Regulatory Risk and Policy, Coaltion

Ms. Sezaneh Seymour is the Vice President and Head of Regulatory Risk and Policy at Coalition, a leading provider of cyber insurance and security services. For nearly twenty years, Sezaneh has held various roles in domestic and foreign policy at the intersection of national security, emerging technology, sustainability, and trade. She is the former Senior Advisor to the Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology on the National Security Council. She also served as Deputy Assistant U.S. Trade Representative at the Office of the U.S. Trade Representative in the Executive Office of the President, where she negotiated and enforced trade agreements. Before these roles, she served at the U.S. Department of the Treasury and the U.S. Department of State. She is a member of the Aspen Institute's U.S. Cybersecurity Group, a Nonresident Fellow of the Center for Strategic and International Studies, a distinguished graduate of the National Defense University's Eisenhower School, and earned her Ph.D. from Virginia Tech, where she still serves as a Professor of Practice.

Brandon Russ

Cyber Claims Specialist - USA

Brandon Russ is a licensed attorney and claims professional at CFC USA. Brandon has been in the insurance industry for several years handling claims stemming from all professional lines of business, as well as coverage disputes for international and domestic carriers. At CFC, Brandon handles a vast portfolio of first-party and third-party cyber and privacy claims, as well as media and technology claims.



SentinelOne
Secure Tomorrow

Appendix

Sentinelone.com

Appendix - Coverage & Premiums

Coverage:

- Process: securing coverage is a highly dynamic process and tailored to ensure that companies receive appropriate coverage that aligns with their specific risk exposures.
- Terms: terms are also customized, and the result of a detailed underwriting process

Premiums: Cyber insurance premiums are a function of risk and coverage

1. Risk Assessment:
   - What specific cyber risks does a company face? Answering this question involves evaluating the company's industry, size, security posture, risk management practices, existing security controls, history of compliance with relevant regulations, and historical data on cyber incidents.
   - Insurers may look to established cybersecurity frameworks to determine necessary controls and coverage levels, like those issued by NIST or ISO standards.

1. Coverage:
   - cyber insurance is not one-size-fits-all - coverage limits, exclusions, premiums, and deductibles may be tailored.
   - Coverage terms are tailored to address the specific needs and risks of the insured. Policies can cover a variety of cyber risks like data breaches, ransomware attacks, business interruption, regulatory fines and penalties, and more.

Appendix - Data Breach

1. **Legal Dimensions**:
   - Data Breach Notification, other incident disclosure requirements: Understanding victim obligations to notify affected parties and regulators, which vary depending on jurisdiction and the nature of the data involved. This is a RAPIDLY changing environment, with legislation and model laws under deliberation at the global, federal, state level.
     1. Federal Examples: GLBA, CCPA/CPRA, HIPAA, SEC 8k, CIRCIA coming online. Also under consideration: American Privacy Rights Act introduced in Congress.
     2. State level laws: this is a good resource to pull specifics from if you want them: https://www.itgovernanceusa.com/data-breach-notification-laws#TX
   - Evidence Preservation: Collecting and preserving data that may be required for legal proceedings or forensic investigations. Depending on the threat actor, there may be value in inviting FBI, CISA to the table
   - Legal Advice and Communication: Legal counsel engaged early to navigate compliance, liability, and potential litigation, while managing communications with stakeholders. Identifying a breach counsel is among the very first steps a cyber insurer assists a victim with.
   - Third-Party Management: Addressing contracts and agreements with third-party vendors who may be involved or impacted by the incident.

Appendix - Regulatory

Regulatory Dimensions:

- Compliance Requirements: Ensuring that incident response processes adhere to applicable laws and regulations such as GDPR, HIPAA, or industry-specific mandates.
- Reporting Obligations: Meeting regulatory requirements for reporting incidents within specified timeframes to authorities, which can vary widely. (CIRCIA, NYDFS, et alia.)
- Audit and Documentation: Maintaining detailed documentation of the incident response process to satisfy regulatory audits and demonstrate due diligence.
- Cross-Border Considerations: Navigating the complexities of international regulations if the incident affects data or operations across multiple jurisdictions. This is a big challenge with data breach incidents that have a transatlantic dimension.

Appendix - Catch All Topics

- Supply Chain Security and Vendor Assessments: Will lawmakers impose obligations on businesses to assess their vendors' data privacy and cybersecurity measures? We already see such obligations in Europe with regulations like NIS2 and DORA. In the United States, specific expectations are emerging in sectors such as insurance, particularly relating to AI use in insurance. (See NAIC model bulletin on this issue.)

- Federal Cyber Insurance Program and "Backstop": The U.S. Federal Government is expected to release a report with recommendations on a federal cyber insurance backstop. Many questions remain open, including the purpose and scope. For more information, see the GAO report here and its summary here. For insights, consider AXA's views here and Coalition's perspective here.

- Data Privacy/Security and Software Liability: Federal agencies are exploring how subrogation functions in the context of software liability. There is significant interest in whether the insurance sector might unintentionally serve as an enforcement mechanism for "defective" software.

Appendix - Catch All Topics

Possible discussion: what does the legal system need to iron out to make product liability a possibility, what are the circumstances that encourage the "right" balance of litigation – specifically subrogation?

- Third-Party-Financed Civil Litigation: This is a concern primarily for personal and commercial lines, though cyber insurance is among the lines least affected so far. The core issue is whether plaintiffs should be required to disclose third-party litigation financing, which has historically been linked to oligarchs and foreign wealth funds, and fuels litigation that might otherwise be settled our dismissed. This remains a top priority advocacy issue for major insurance industry associations like APCIA and is contributing to increased premiums. Relevant legislative actions can be observed on Capitol Hill, incl Cong Issa.