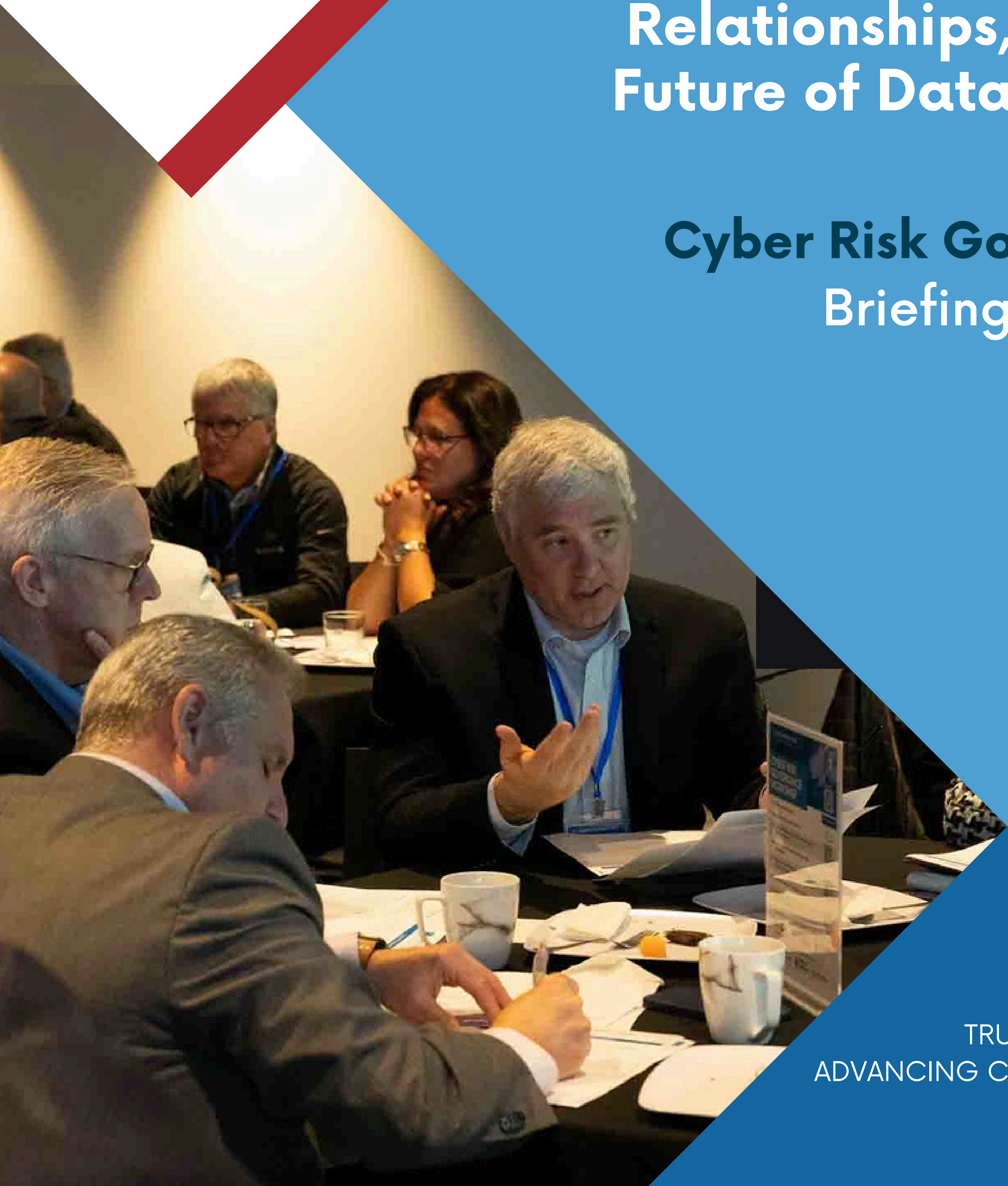
ADVANCED
CYBER
SECURITY
CENTER

Cyber Insurance: Market Trends, Provider Relationships, and the Future of Data Sharing

Cyber Risk Governance
Briefing Summary

July 2024



TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

ADVANCED CYBER SECURITY CENTER

Cyber Insurance: Market Trends, Provider Relationships, the Future of Data Sharing

After a period of stable rates, cyber insurance rates are on the rise again—and policies are getting more complex. Organizations must ensure they're not only properly covered, but also leverage broker expertise—especially when an incident hits. Cyber insurer expectations are also rising; creative organizations benefit from lower rates, better terms.

Briefing Partners

Howard Panensky
Pierson Ferdinand
ACSC Insurance Co-Chair

Lauren Crean
State Street
ACSC Insurance Co-Chair

Tom Finan
WTW

Erin Kenneally
Halcyon.ai

Executive Recommendations

In a fast-changing insurance marketplace, forward-looking executives are re-examining their risk appetite and opportunities to transfer risk, focused on actions including these:

- Lean on a strong broker relationship to help understand coverage and gaps; foster close relationships with internal and external parties ...before you need them.
- Use an insurance executive committee to support well-informed decisions.
- With AI now in mind, expand third-party security requirements to reduce risk and premiums (see ACSC's AI Vendor Assessment Toolkit link here).
- Investigate and leverage tools that streamline reporting to insurers (and for forensics).

And as real-time data and system monitoring become more transparent:

- Prepare to move from self-attestation to system monitoring reports to insurers.
- Consider opportunities for future data-sharing with insurers in exchange for discounts.

Issues to Watch

- Emergence of SEC as default cyber regulator for large firms. (read the ACSC Briefing Summary here)
- Increased involvement of procurement in insurance buying.
- Data collection risks associated with marketing programs.

View WTW's Cyber Insurance Market Trends deck.

Market Trends:
Insurers Respond to New Threats

Cyber insurance providers are responding to accelerating threats and seeking tighter relationships with internal organizational teams before, during, and after an incident.

Highlights

- Costs were already trending up; the CrowdStrike incident is expected to fuel further rate increases.
- Even as insurers pay out, many clients feel "under covered."

Ransomware Is Top Concern for Insurers

- Payouts continue to drive rising premiums, but 'events' such as CrowdStrike contribute as well.
- Ransomware remains a major challenge: "We think there are 8X more incidents than reported." From hacking systems to targeting 24/7 customer call centers, tactics and business models are getting more sophisticated.
- Increasingly, ransomware attacks are based in China and Russia.

Third Party Supply Chains: Insurers Are Asking More Questions

- 9 out of 10 orgs have done business with a breached organization, 3 out of 10 attacks are launched through 3rd parties.
- Visibility into 3rd party risk is critical to insurers.
- Reporting on vendor selection, onboarding and management will increasingly be reviewed by insurers.

Clarity On Policy Coverage Is An Ongoing Issue

Insurance providers are paying for incurred losses, but policyholders complain about incidents or costs not being covered. The disconnect leads to poor outcomes.

- 63% of respondents to a Sophos survey said they had blown through coverage.
- 58% said they didn't get a payout after incurring unapproved breach expenses. "They don't understand their policy rules."

MARKET PULSE: MEMBER POLL

- **C**overage rates, 65% said rates were same or higher, with only 10% reporting a decrease.
- Who's involved in the purchase process? Mostly legal, risk, and finance.
- Willing to trade data for better rates from insurers? Almost 40% said definitely yes, half said "I'd need to think about it."

Provider Relationships During An Incident

Take Advantage of Your Broker’s Expertise

Understanding the broker’s expertise and role during an incident is important.

- Know your team ahead of time before trouble hits.
- When an incident occurs, notifications in order should be: breach team, vendor panel, broker.
- In a ransomware attack especially, the insurance team can leverage relationships with known threat actors to mediate and negotiate on your behalf.

The Future: Insurers As Partners for Data

The Quest for More Data

As cyber insurers continually mature actuarial tables, they are on a quest for more and better data to understand customer controls, the attack surface, and threat landscape. Like auto insurers, they will look for data directly from the insured party.

Transparency around the collection and sharing of security and control data may provide better outcomes for all parties, reducing incidents and costs. Examples are still limited, and the challenge is how to get that done.

- The proposition is simple: Security transparency in exchange for reduced costs. Getting over proprietary and privacy concerns is a major hurdle though.
- Data could flow between customer, MSSP where there is one, and insurers.

An additional advantage would be the automation of the significant time spent currently on applications and renewals.

Data integrations would replace static checklists and incomplete self-assessments.

AI: On the radar but limited impact on policies to date

Most ACSC executives have not seen AI reflected yet in their policies, although questions are being raised about AI inventories and risk registers. AI continues to be managed through the traditional IT/security goals: Confidentiality, Integrity, Availability (CIA) risks.

ADVANCED CYBER SECURITY CENTER

ACSC Research Partner:

halcyon

A Proactive, Risk Value Strategy And Platform

ACSC Research Partner, Halcyon, participated as a thought leader and previewed their purpose-built platform that brings technology, best practices, and trusted advice together to help customers proactively drive better cyber insurance outcomes with a risk value lens.

Purpose-built for 360-degree protection

Moving from static assessments with occasional scan data wasn't doing enough to drive down costs. Halcyon took a different approach, combining stronger pre-breach controls with dynamic data encryption and exfiltration defenses.

- Innovative behavioral detection and blocking improves pre-breach readiness.
- The ability to capture encryption keys allow for data to be unlocked for free.
- Data protection guards against exfiltration better than traditional DLP.

Halcyon customers have experienced zero ransomware breaches or exposures to date, with plenty of proactive mitigations under their belt.

"Ideally, we create a virtuous cycle."

Done right, the right controls and data sharing combine to create a flywheel effect that drives better outcomes for insurers, brokers, and clients. Halcyon serves as a bridge to this "codependent value creation" around data.

- For insured, the cost of coverage and renewal friction should decrease.
- Carriers can benefit from claims-saved and lower loss ratios as well as gaining actionable risk information from better data.
- Brokers get lower acquisition costs and less friction at renewal.
- MSSPs and risk teams gain ransomware-specific defenses with less overhead than EDR.

Last, but definitely not least, this 'flywheel effect' can reduce incident response costs that are born by all stakeholders to different degrees.

About the ACSC

The Boston-based ACSC advances member cyber defense strategies through regional, national and global practice-sharing networks of industry leaders and provides professional opportunities for rising talent. This Executive Practice Guide reflects key takeaways, with proprietary information redacted, from this NDA-covered session.

Contact

617-485-1112

wguenther@acscenter.org