accenturesecurity

ACCENTURE CYBERSECURITY FORUM

THE EVOLVING ROLE OF CYBER INSURANCE IN ADDRESSING RISK

VIRTUAL ROUNDTABLE SUMMARY
DECEMBER 3, 2019

On December 3, 2019, the Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "The evolving role of cyber insurance in addressing risk." CISOs from multiple industries and organizations joined the call to discuss the role of cyber insurance in an overall cyber resiliency program. As the costs of cyber crime continue to rise, CISOs are increasingly adding cyber insurance to their portfolios of cyber protection.

Our two subject-matter experts for the call were an executive of a diversified insurance services company and a cyber leader of an insurance and risk services company. The session was hosted by ACF Chair Andy Vautier, Accenture CISO.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

What role can cyber insurance play in overall risk management? What are the costs and benefits of cyber insurance? Who in the enterprise should be involved in adding cyber insurance to the risk management portfolio? Are there best practices? Participants shared their experiences with cyber insurance and examined the myths and realities of this risk management tool.

Deploying cyber insurance as a risk management tool

Vautier began the discussion by noting that while cybersecurity skills and technologies are evolving to contend with a shifting threat landscape, the actuarial calculations associated with insurance rely on historical data. This can make it difficult for insurers to keep pace with changing threats. Nevertheless, cyber insurance has an important place in a cyber protection portfolio. In fact, many of Accenture's clients demand it as a contractual requirement.

DISCUSSION

An insurance expert outlined the evolution of cyber insurance over the past five years. Previously, protection focused on privacy risk, and enterprise cyber insurance decisions were typically the purview of the treasury and risk management functions. Only a small percentage of CISOs had an active role in cyber insurance decisions. Today, CISOs and other leaders in the organization have generally joined forces to address the issue. Cyber insurance policies have expanded in scope, often covering systems failures, business interruption, ransomware and other cyber extortion.

Participants raised questions about how cyber insurance can help protect against third-party risks across complex information ecosystems characterized by greater numbers of third parties and more extensive data sharing. The conversation yielded several suggestions:

1. Recognize that third-party providers may not have experienced breaches and thus are not fully aware of the consequences. Early and frequent conversations are important.
2. Require documentation from third parties that they have adequate coverage. Evaluate coverage annually to clarify risks and responsibilities.
3. Document vendor mitigation strategies and the specific approaches they will take in case of a breach.
4. When relying on third parties to mitigate risks, focus on incident response readiness. Set contract terms before an event occurs.

Members reported that candid conversation with their ecosystem partners before an incident occurs is critical in making the right cyber insurance decisions.

Myths vs. realities

A participant challenged the myth that insurers do not pay claims on ransomware attacks. In most cases, lawsuits are driven by policyholders seeking protection under older policies that do not cover the damages in question. In fact, he reported, insurers have paid out hundreds of millions of dollars for substantiated losses from system failures, service interruptions and ransomware attacks. He acknowledged that there will always be gaps between known risks and new, unknown threats.

Members discussed the value of information sharing and candid communication among CISOs, enterprise risk managers, boards of directors, and insurers. Collaboration among the CISO, CFO, legal, and risk management is critical in developing a cyber insurance strategy for the enterprise. Compared to five years ago, CISOs have greater knowledge of what is covered in policies, and risk managers have a better understanding what steps the enterprise is taking to manage cyber risks.

Greater collaboration with insurers can help reduce losses and premiums. CISOs should leverage an insurer's experience to minimize costs and business impacts. For example, a participant reported, in cases where the insurance company was actively involved, ransomware costs were significantly lower. Boards of directors are expecting more information about how the enterprise is using cyber insurance.

Best practices

Participants shared a number of best practices for effectively using cyber insurance as part of an overall cybersecurity program:

1. **Follow a four-step process in setting insurance coverage.** Start with an assessment of major risks. Second, quantify the impacts of potential events to help management and the board understand the need for and value of

cyber insurance. Third, negotiate policies that cover the greatest risks. Fourth, prepare response readiness plans with the third parties that will help you respond to a breach. Set contract terms before an event occurs. Finally, view the process as a loop that is continually refreshed, and keep the insurance policy up to date.

2. **Model attacks and the potential implications for insurance.** Develop a set of use cases based on past attacks and those suffered by other enterprises, and analyze the extent to which insurance provides appropriate protection. Together with insurers, conduct tabletop exercises of targeted attacks to anticipate each partner's response.

3. **Keep insurers apprised of your environment.** Inform carriers of relevant cybersecurity program details, including an assessment of risks in an evolving threat landscape. In order to maximize insurance value and minimize conflict, document how a breach will be managed and who will be involved, including the CISO's team and any third-party vendors the enterprise might call on to help. Include your desired providers in your policy.

4. **Communicate promptly with insurers about breaches and their impacts.** Claim disputes often occur when a company manages a breach on its own and sends its carrier a claim. Lack of communication can spark a dispute. Keeping the insurer apprised as soon as an incident occurs can ultimately help minimize the impact of a breach.

5. **Collaborate internally.** Partner with the CFO, legal, risk management and other relevant internal stakeholders to develop a cyber insurance strategy consistent with other coverage. Prepare event management teams in advance of a breach.

6. **Call on insurer expertise.** Insurers have typically seen a variety of cyber incidents. Leverage the risk management resources and experience of insurers that have dealt with ransomware attackers and other threat actors.

7. **Know your coverage.** When a breach occurs, the board and executive management will ask about exposure and coverage. The CISO should know the insurer, how much the policy costs, what it covers and what it doesn't cover.

CONCLUSION

In closing, Vautier remarked that there is an evolution on several fronts: in the threat landscape, in the ability of CISOs to respond to threats, and in the level of engagement CISOs are having with their insurers and corporate leadership. He said cyber insurance will be of greater value to CISOs as they collaborate with risk management, treasury and procurement to craft comprehensive coverage; tap into the cybersecurity experience of their insurance partners; and rehearse for the high-impact breach events that are being insured.

CONTACT

ANDY VAUTIER
Accenture CISO
Chair, Accenture
Cybersecurity Forum

ABOUT ACCENTURE

Accenture (NYSE: ACN) is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 505,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives..

Visit us at **www.accenture.com.**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently drive innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown.

Follow us @AccentureSecure on Twitter or visit the www.accenture.com/security.

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us