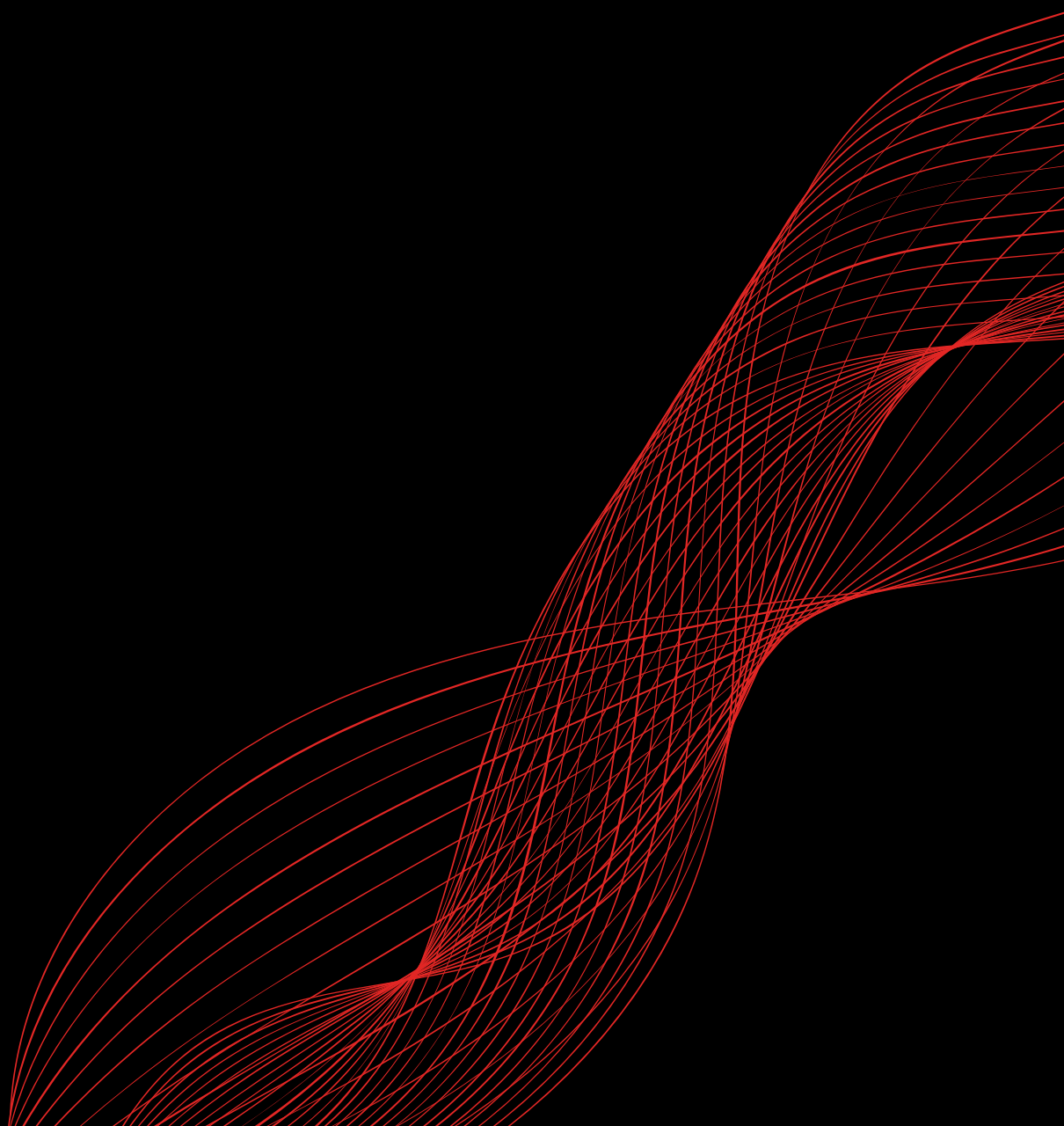
GoSec 24

CISO ROUNDTABLE: CYBERSECURITY LEADERSHIP IN THE AGE OF AI AND CYBER INSURANCE



GoSec 24

CISO Roundtable

Executive Summary

On September 12th 2024, during GoSec24 in Montreal, a roundtable discussion provided a platform for CISOs and cybersecurity leaders to exchange insights and experiences. This whitepaper focuses on the challenges posed by integrating AI technologies, the evolving role of cyber insurance, the growing importance of cyber resilience, and the complexities of maintaining privacy. Drawing on perspectives from a variety of industries, the CISOs' insights enrich thinking on practical strategies and best practices for managing these challenges while maintaining organizational resilience. As cybersecurity risks continue to grow, the need for clear governance, effective resource management, and strong incident response strategies is increasingly urgent.

Introduction

The complexity of cybersecurity challenges facing organizations continues to grow. To foster a platform where organizations can openly discuss their security challenges and share solutions, GoSecure hosted the CISO Roundtable at the GoSec24 event in Montreal on September 12, 2024. The roundtable brought together 19 CISOs and leaders from various industries, including financial services, manufacturing, and public infrastructure. Their years of experience as leaders ranged from 5 to 20 years. The wide range of organization sizes and the diverse experiences of the CISOs enriched the discussions, adding valuable depth and perspective.

The moderated roundtable was hosted by GoSecure's CTO and was held on-site in a private room. The session offered an exclusive setting for in-depth discussions and for CISOs to openly discuss key topics like AI governance, the role of cyber insurance, and building resilience into cybersecurity programs. This whitepaper highlights the key themes from the discussion, providing actionable insights to help CISOs navigate these pressing issues. The discussion was guided by three core questions, covering a range of topics from the evolving role of cyber insurance and its impact on cybersecurity programs, to challenges in maintaining privacy and managing AI usage. The questions that framed the conversation can be found in the Appendix.

GoSec 24

CISO Roundtable

Discussion Highlights

Summary Of Discussion Highlights

- **Cyber Insurance Costs and Efficacy** – Despite the high premiums and perceived limitations in coverage discussed by several CISOs, cyber insurance is recognized as necessary in certain sectors. Many organizations are now also considering alternatives like self-insurance and enhancing their risk management strategies to meet the evolving requirements of insurers.
- **Compliance and Partner Risks in Cyber Insurance** – While organizations are challenged with extensive compliance demands from insurers, these requirements drive the enforcement of rigorous policies not only internally but also among partners to secure insurance coverage. In regulated industries, where maintaining credibility and trust is paramount, adhering to best practices, including regular policy reviews and incorporating breach response services, remains essential.
- **Shift in CISO Mindset and Focus on Risk** – Cyber resilience has become a key priority for organizations post-pandemic, leading CISOs to adopt a more risk-conscious mindset. They are now more rigorous in evaluating service options and prioritizing comprehensive protection, highlighting the need for a robust incident response framework that includes clear communication with stakeholders during cybersecurity incidents.
- **Emphasis on Preparedness and Training on Resilience** – Organizations must not only be ready to respond to incidents but also maintain operational continuity. This involves leveraging cloud solutions for data safeguarding and conducting regular incident response drills that engage both technical teams and broader organizational participation. Ongoing education programs are essential to foster a culture of resilience where cybersecurity is viewed as a shared responsibility across all levels.
- **AI Governance Challenges** – CISOs express concerns over the rapid integration of AI within organizations, viewing it as a potential detriment to policy and governance. CISOs are prompted to critically evaluate the necessity of specific AI applications ensuring they align with departmental needs.
- **AI Integration Solutions** – The rise of AI necessitates robust governance frameworks to protect sensitive data and company secrets. This may involve developing in-house AI solutions and incorporating stringent clauses in partner contracts to manage AI-related risks. A proactive approach is essential, emphasizing the establishment of formal policies for AI use and comprehensive employee training to mitigate risks and ensure awareness of both opportunities and threats associated with these technologies.

Cyber-insurance: Assessing its Impact as a Relief or Burden

Cyber insurance has become a well-established component of organizations' broader risk management strategies. Several challenges and frustrations were raised regarding cyber insurance. First, the process of completing the insurance contracts demands significant organizational resources. For example, some CISOs had to allocate multiple full-time staff members for several months just to navigate the extensive and complex questionnaires. CISOs also highlighted the lack of support and tools provided to assist them through the process.

Second, if an organization is able to fulfill all the stringent requirements imposed by insurers, the concerns shift to whether the insurance is still necessary. At that point, the company may have already achieved the level of security and resilience that negates the need for such coverage.
Third, the premiums are often high, and in some cases, a single insurer may not provide the required coverage, forcing companies to engage with multiple insurers. Thus, increasing complexity.

The fourth challenge regarding cyber insurance is that organizations must now incorporate rigorous rules and policies not only for themselves but also for their partners to comply with insurance contracts and obligations. As a result, partners can potentially pose a threat to an organization's insurance coverage.

Finally, beyond the resources and costs, another major concern is the extensive list of compliance requirements imposed by insurers. The question becomes not whether you want to be insured, but whether it's even feasible given your circumstances.

Although concerns were raised about the high premiums and inconsistent coverage offered by insurers, cyber insurance remains vital, particularly in industries where it is required by contract. The objective of having cyber-insurances is sometimes directed toward maintaining credibility in front of clients, but the fact that sometimes, the coverage may not offer significant added value was raised. In other words, this external pressure reinforces the need for many organizations to retain policies, as it serves as a marker of trustworthiness and preparedness in the eyes of clients and partners.

Best practices for maximizing the value of cyber insurance include regularly reviewing policies, working with experienced brokers, and ensuring that coverage addresses both current and future risks. CISOs also recommended incorporating breach coaches and incident response services into these policies to better prepare for incidents and minimize operational downtime during a cyberattack.

The Resilience-First Approach

Cyber resilience has emerged as a critical focus in the post-pandemic landscape, defined as an organization's capacity to prevent, endure, and recover from cybersecurity incidents. CISOs noted that this shift has fundamentally changed their approach and mindset toward their roles. They have become increasingly risk-conscious, prompting them to adopt a more rigorous and inquisitive approach when evaluating service options, asking more detailed questions to ensure comprehensive protection.

The need for a comprehensive incident response framework was a recurring theme. Beyond technical recovery, organizations must also prioritize clear, transparent communication with stakeholders and customers in the event of a breach. If customer data is impacted, reputational recovery becomes just as critical as operational recovery, as losing the trust of clients can have long-lasting effects on the business. Maintaining trust is critical, especially when sensitive data is involved.

The roundtable discussions stressed the importance of developing a resilience-first approach, ensuring that organizations are not only prepared to respond to incidents but can continue their operations with minimal disruption. Leveraging cloud-based solutions that offer redundancy and scalability was recommended as a way to safeguard critical data, ensuring that businesses can recover quickly from incidents.

Resilience also hinges on regular testing of incident response plans. CISOs advocated for frequent drills that involve both technical teams and broader organizational participation, helping to ensure that every level of the business is prepared to handle cyber threats. This holistic approach should extend beyond the IT department, with cybersecurity awareness being integrated into all aspects of business operations. The inclusion of ongoing education programs for employees at all levels helps organizations build a more resilient culture, one in which security is a shared responsibility.

CISOs Remain Cautious amid AI Hype

The rapid integration of AI into the organizational landscape has been deemed detrimental by CISOs with regards to policy and governance. While their instinct may have been to stop its adoption, the pressing concern of falling behind competitors—who are all embracing these tools—has made this option increasingly untenable.

Amidst the hype surrounding AI, CISOs are compelled to ask fundamental questions. For instance, while there is interest in integrating tools like Copilot, they must evaluate whether such tools are truly necessary across all departments. Although Copilot may be highly beneficial for sales, it might not be as relevant for other areas. Consequently, for security reasons and to effectively navigate the hype, it is essential for CISOs to fully understand the tools available, their intended uses, and to assert when certain AI solutions may be unnecessary.

The role of the CISO is not only influenced by security concerns related to AI but also significantly impacted by the data privacy issues that arise with these technologies. CISOs emphasize the need for guidance in securely integrating AI. They recognize the imperative to protect personal information as well as company secrets. This situation has led some organizations to consider developing in-house AI solutions tools to alleviate the associated burdens.

Similar to the challenges posed by cyber insurance, organizational partnerships present additional risks concerning AI. While CISOs may implement robust internal policies, they must also consider integrating stringent clauses into partner contracts that mandate careful handling of AI in relation to internal information. It is crucial to ensure that the boundaries established are respected by all parties involved.

The CISOs emphasized the importance of adopting a proactive and structured approach to cybersecurity, especially as emerging technologies like AI become an integral part of daily operations. The discussions underscored the need for robust governance frameworks around AI use, ensuring that organizations can leverage these technologies without exposing sensitive data or undermining security standards. Establishing formal policies for AI usage was highlighted as a foundational step, and the second important solution raised is employee training. The former is crucial to ensure that staff understand both the opportunities and risks associated with AI. Comprehensive training programs not only mitigate risks like data leakage but also help employees recognize unauthorized access to proprietary information.

Conclusion

The CISO roundtable reinforced the need for a comprehensive, forward-thinking approach to tackling today's cybersecurity challenges. From navigating the complexities of AI governance to rethinking the value and application of cyber insurance, the conversations highlighted the critical role of strategic leadership. A resilient, adaptable security framework—built on strong governance, continuous evaluation of risk management strategies, and a proactive culture of resilience—will be essential as the threats continues to evolve. This whitepaper captures the collective expertise shared during the roundtable and serves as a guiding resource for organizations committed to fortifying their cybersecurity posture.

Appendix

Key Questions Discussed

Question 1: Cyber insurance has gone through a lot of changes since it has hit the market, going from very unstable (major changes from year to year) to stabilizing, according to certain sources, in the last 2 years.

1. How has the need for cyber insurance affected your organization
2. Do you see that as a benefit or hinderance to the overall cyber program you have been putting in place?
3. Have you received unreasonable requests from your insurers?

Question 2: Cyber resilience has become a hot topic in the post-pandemic world. It can be defined as an organization's ability to prevent, withstand and recover from cybersecurity incidents.

1. Has your organization adopted this concept?
2. How has it changed your approach?
3. Were there pandemic “lessons” that have changed things for the better for your organization?

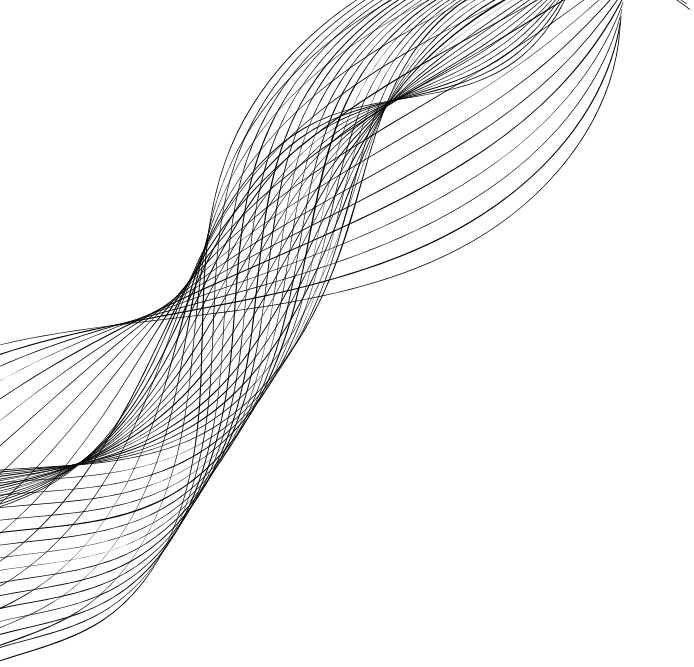
Question 3a: When it comes to privacy, as someone responsible for cybersecurity in your organizations,

1. Do you monitor your employees and is it ethical to do so?
2. With many employees using their work computers for personal matters, where is the line regarding your users’ privacy?
3. Do you concern yourself with what people put on social media (since some of it can be traced back to the organization)? If yes, how do you approach this?
4. Have you experienced sensitive information being posted?

Question 3b: Following that train of thought, more and more users are leveraging AI/ChatGPT to write, to translate, to interpret.

1. What have you done to prevent sensitive information being provided to the LLM provider?

Does your organization have a formal stance on this? Or are you simply trusting the provider?



Organizer:

Julien Turcot is the Senior Vice President of Sales at GoSecure and is based in Quebec City.

The author wishes to thank GoSecure and the CISOs for their contributions to the roundtable.

© GoSec 2024. All rights reserved.
www.gosec.net