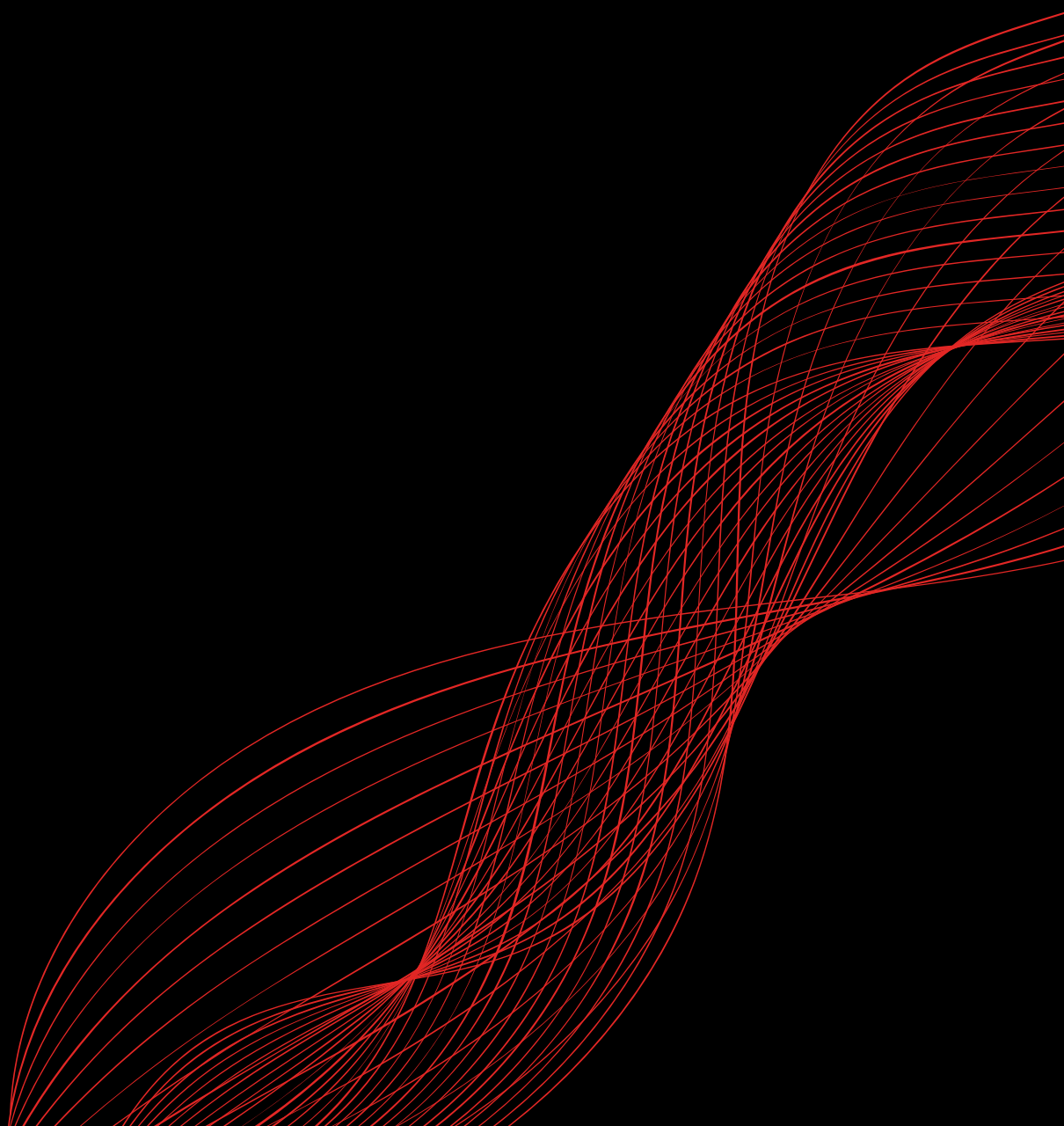
GoSec 23

CISO ROUNDTABLE: MUTUALIZATION OF RESOURCES – A CHALLENGE AND AN OPPORTUNITY



GoSec 23
CISO Roundtable

Executive Summary

At the recent GoSec 23 conference in Montreal, Canada, a pivotal roundtable session took place, bringing together 11 distinguished, anonymous CISOs from various industries across the nation. This whitepaper dives into the challenges, strategies, and best practices discussed during this session, with a special focus on navigating the cybersecurity landscape under budgetary constraints within the Canadian economic context. Leveraging diverse experiences and perspectives, this whitepaper aims to provide comprehensive insights for professionals and organizations in the cybersecurity domain, emphasizing the transformative approach of mutualization.

Introduction

In an era where cyber threats are omnipresent and constantly evolving, understanding the challenges and strategies pivotal to effective cybersecurity management is paramount. A moderated roundtable presented a platform for CISOs from a myriad of sectors, including banking, aerospace, agriculture, and entertainment, to share candid insights, challenges, and best practices. This 1-hour session was hosted during GoSec in Montreal on September 14th, 2023, on-site in a Crew Collective & Café conference room. The deliberations were steered by ten core questions, addressing aspects ranging from budget constraints, decision-making, technology adoption, to measuring the effectiveness of cybersecurity initiatives. The key questions that helped to steer the discussions can be found in the Appendix.

Participants/Participant Background

The roundtable saw participation from 11 anonymous CISOs. Industries represented include: research, manufacturing, retail, military, non-profit, aerospace, agriculture, banking and entertainment. Their years of experience as CISOs ranged from 2 to 15 years. The roundtable was a rich amalgamation of perspectives, drawing participants from diverse backgrounds and experiences. These considerations during the planning of the roundtable ensured diverse set of insights and perspectives were highlighted in the discussion.

Discussion Highlights/Trends

The discussions brought to light various themes:

- Talent Challenge - The increasing difficulty in attracting new talent, especially with losses to bigger enterprise names and the commercialization of education.
- Scope Challenge - The broad scope of security can extend beyond cybersecurity, incorporating aspects such as physical security.
- Budgeting Issues - Discrepancies in budget allocations, especially in the context of projects vs. operational needs.
- Economic State Impact - Economic downturns and rapid inflation lead to cuts in operations, regardless of their performance.
- New Technology and Regulatory Challenges - Adopting new technology introduces new risk endpoints and regulatory frameworks can impede project progression.
- Organizational Silos - The hierarchy and reporting structure of CISOs vary across organizations, leading to potential conflicts, blindspots and challenges.
- Project Budgeting - Initial phases of projects often see ample budgets, but as they transition to exploitation, funds dwindle.
- Quality vs. Quantity - The focus on quality might lead to overlooking other critical security controls.
- Knowledge Gaps - The broader organization often lacks in-depth understanding about cybersecurity.

Cybersecurity Best Practices, Recommendations and Strategies for the Future

For CISOs, the road ahead requires bold leadership. Understanding the broad scope of security is paramount; it's essential to recognize that its expanse isn't limited to just cybersecurity. It integrates wider aspects, such as physical security. Furthermore, the dynamic landscape of cyber threats necessitates continuous learning. CISOs must stay abreast of emerging threats, leveraging a gamut of informational sources, to continually refine and adjust strategies. Breaking down organizational silos is equally crucial. Ensuring a cohesive organizational structure and reporting framework for CISOs not only mitigates potential conflicts but also fosters better cooperation across departments. The future demands active CISO efforts in breaking down these silos and optimizing costs through shared resources. Adopting mutualization as a de-siloing effort requires taking calculated risks to achieve long-term benefits.

Mutualization stands as a transformative approach in the cybersecurity landscape. It empowers CIOs and CISOs to maximize their reach, distributing budgets across a wider array of priorities and projects. Beyond mere financial aspects, mutualization encapsulates the pooling of vital resources, knowledge, and talent. This is the convergence of means, skills, and talents, all channeled towards shared objectives. Such a strategy not only bridges talent gaps, allowing teams to grow exponentially, but also guarantees cost benefits, offering revenue enhancements for smaller teams and expenditure savings for larger ones.

The talent shortage issue is not new or contained to just the cybersecurity industry. Continuous learning is vital to address this issue, and its integration with a mutualization framework amplifies its effectiveness. Sharing resources allows seasoned professionals to uplift the entire team's proficiency. Such a collaborative approach enables teams to access learning opportunities that might be financially unattainable individually or infeasible for CISOs to budget. In addressing the talent deficit, organizations should focus on internal hiring, supplemented by standardized job descriptions, to retain and attract the best in the field, steering them away from more prominent names.

Incorporating new technology, especially in the cybersecurity domain, is pivotal for organizations aiming to stay ahead of potential threats. Through mutualization, teams can pool resources to collectively adopt cutting-edge cybersecurity tools and solution, such as AI and automation, at an accelerated pace. Speed is essential, as the potential of these new technologies can be harnessed to counteract relentlessly growing cybersecurity challenges, especially when resources are limited.

Mutualization's strength also lies in curbing redundant expenses, especially among similar departments. By leveraging what's already available and refraining from incessantly stacking products or solutions, firms can ensure they remain both protected and financially efficient. This, paired with the right training for decision-makers and a synchronized view of cyber and material security, ensures a holistic and robust approach to cybersecurity.

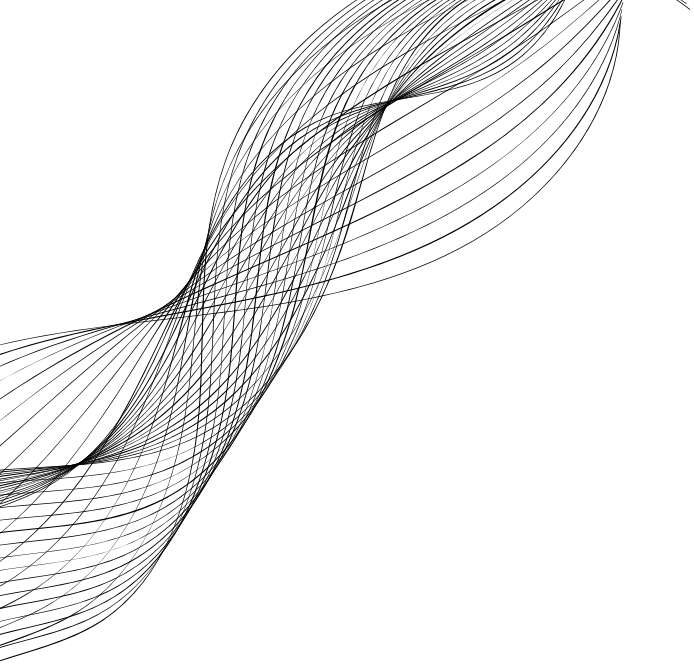
Conclusion

During the CISO roundtable, it becomes evident that a holistic, integrated approach, characterized by mutualization, which enables continuous learning, and a quicker embracing of technological advancements, is the way forward to a more collaborative and efficient future for cybersecurity. As threats evolve, so too must our strategies and practices. This whitepaper underscores the collective wisdom of industry veterans and serves as a beacon for organizations striving to strengthen their cybersecurity frameworks.

Appendix

Key questions asked to the group:

- What are the main cybersecurity challenges you've faced as budget constraints become more pronounced? How have you addressed these challenges?
- When budgets are tight, how do you decide on security priorities? What are the key considerations guiding your choices?
- Consolidating cybersecurity solutions can offer benefits in terms of efficiency and cost. Can you share specific examples of how you've managed to consolidate your solutions while maintaining a high level of protection?
- In the face of budget constraints, how do you convince management of the importance of investing in cybersecurity? What communication strategies have you found effective?
- Internal collaboration is crucial for strengthening cybersecurity posture. How have you managed to foster better cooperation between IT teams, business departments, and management despite budget pressures?
- Given limited resources, how do you manage the trade-offs between security and innovation? Can you share examples where you've found a balance between these two imperatives?
- New technologies such as AI and automation can potentially help address cybersecurity challenges. Have you explored these solutions to optimize security with limited resources?
- How do you measure the effectiveness of your cybersecurity initiatives despite budgetary constraints? What indicators or metrics do you use to evaluate the success of your strategy?
- In a budget-constrained environment, how do you keep abreast of new threats and developments in cybercrime? What are your informational sources, and how do you adjust your strategy accordingly?
- Can you share lessons learned or mistakes to avoid when consolidating cybersecurity solutions? What are your tips for other CISOs facing the same challenges?



Organizer:

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

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

www.gosec.net