GoSec 25

CISO ROUNDTABLE

2025 SEPTEMBER

SAAS BLIND SPOTS, DISASTER RECOVERY LIMITATIONS, AND THE AI CHALLENGE

GoSec25

CISO Roundtable

Septembre 2025

EXECUTIVE SUMMARY

During GoSec25 in Montreal, approximately fifteen CISOs and security leaders from diverse sectors (finance, energy, logistics, entertainment, and manufacturing) gathered for an open and confidential discussion on today’s most pressing cybersecurity challenges.

Objective: To foster peer-level discussions around concrete issues that are redefining technology governance in Canada..

The discussion highlighted a rapidly evolving landscape where three major forces are converging:

1

SaaS Proliferation and Growing Visibility Blind Spots

The participants acknowledged that critical SaaS applications (such as Salesforce, Dayforce, or Microsoft 365) often operate as blind spots: even when integrated into secure environments, they remain partially opaque.

2

The pressure created by compliance frameworks, which provide reassurance without guaranteeing continuous security.

Certifications such as SOC 2 offer only limited assurance.

Disaster recovery (DR) strategies in cloud environments also reveal a concerning reality: regardless of how robust the backups may be, the ultimate availability of systems still depends on the service provider.

3

The rapid acceleration of AI adoption, bringing efficiency gains but also new risks.

Artificial intelligence tools are being integrated at an unprecedented pace into operational workflows, including code review, fraud detection, compliance, and automation.

While the productivity benefits are undeniable, governance and ROI remain difficult to measure, and concerns around sensitive data leakage continue to grow.

| ***Cross-cutting theme:*** *governance, visibility, and security culture must evolve at the same pace as technology.*

CISOs agreed that resilience is no longer purely a technical matter.

It now relies on multi-layered governance, stronger vendor oversight, and continuous user training to turn blind spots into drivers of sustainable security.

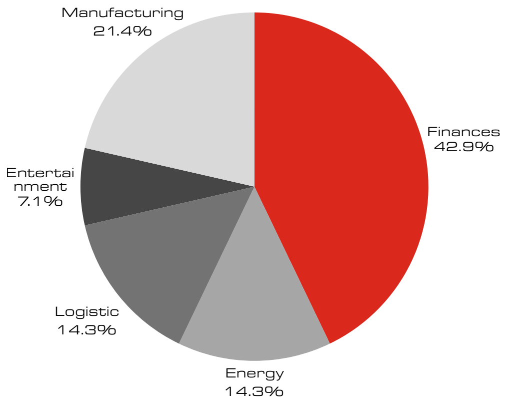
INTRODUCTION

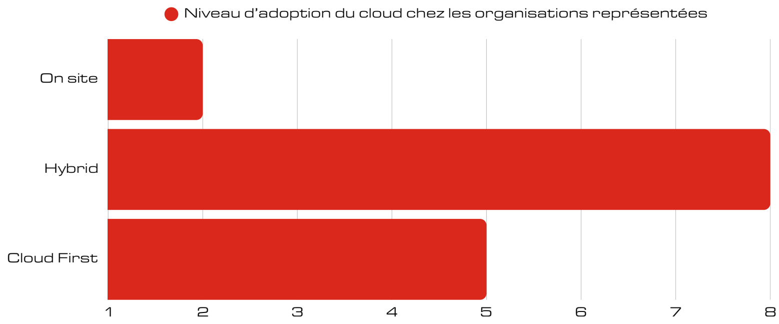
Cybersecurity is becoming increasingly complex each year as organizations rely more heavily on hybrid, distributed, and interconnected ecosystems. CISOs face a dual imperative: enabling innovation while preserving trust.

The meeting provided a space for open, peer-to-peer discussion free from vendor influence focused on real-world challenges: SaaS blind spots, the limits of compliance, disaster recovery in the cloud, and the governance implications of AI. From these exchanges emerged a shared conviction: resilience is no longer a function it is a culture. It requires organizations to continuously adapt at the same pace as digital transformation.

This white paper summarizes the key insights from this roundtable and translates them into practical takeaways for today's security leaders. The four dominant themes—SaaS security, compliance, disaster recovery, and AI adoption illustrate the delicate yet essential balance between innovation, governance, and organizational resilience.

PARTICIPANT PROFILE





Among the 15 participants, some lead "cloud-first" organizations, managing dozens of SaaS platforms and an almost entirely virtualized infrastructure. Others operate in environments where risk is not tolerated, such as the energy sector, where operational systems remain strictly on-premises.

Yet all share a common challenge: protecting increasingly complex environments with often limited resources and constant pressure to innovate. Around the table, the cumulative experience exceeded well over a hundred years of risk management, spanning technical security, organizational governance, and strategic leadership.

This diversity of profiles and risk appetites enriched the discussion. Some emphasized the speed and flexibility required to keep pace with innovation, while others highlighted the importance of resilience, continuity, and control, even if it meant slower deployments.

KEY HIGHLIGHTS AND TRENDS

- **SaaS Security: Visibility Gaps and Operational Realities**

CISOs highlighted that platforms such as Salesforce and Dayforce represent potential blind spots. Even with SSO integrations, these systems often function as black boxes where misconfigurations can lead to data leaks. Emerging SaaS Security Posture Management (SSPM) solutions provide real-time visibility but can generate an overwhelming volume of alerts. Manuals and, in some cases, external partners are required to manage this workload. The consensus was that responsibility has shifted from owning the infrastructure to overseeing vendors, but ultimate accountability for outcomes still rests with the organization, and oversight activities cannot be neglected.

- **Compliance: SOC 2 and the Trust Dilemma**

Compliance frameworks like SOC 2 are viewed as indicators of maturity rather than guarantees of continuous security. Controls assess a specific point in time and do not ensure ongoing protection; several certified companies have still experienced breaches. Best practices mentioned include requesting SOC 2, ISO, or TISAX reports, including audit rights clauses, requiring remediation plans, and using external monitoring tools provided by security rating platforms. The group agreed that compliance provides useful insights, but multi-layered trust and active governance are essential.

- **Disaster Recovery: The Reality of SaaS**

Backups alone cannot guarantee continuity if a vendor experiences a total outage, as clients cannot operate applications without the underlying platform. Some organizations now conduct business continuity tests and establish manual emergency procedures. Others noted that these plans often fail if untested. Participants emphasized prioritizing critical systems and recognizing the cost of each additional measure; SaaS disaster recovery should be viewed as a matter of processes, contracts, and proven procedures, not just data copies.

KEY HIGHLIGHTS AND TRENDS

- **Industry Perspectives: Appetite for Cloud**

Sector context strongly influences cloud strategy. Utilities and OT-intensive industries remain naturally risk-averse, keeping operational systems strictly on-premises and permitting cloud use only for productivity tools from trusted vendors. Some organizations adopt a “cloud-first” approach for HR and collaboration but maintain on-premises control for industrial systems. Many operate in hybrid environments, combining cloud-based operational units with on-site teams, particularly in critical industrial contexts where segregation is considered essential. The common thread was clear: industry dictates appetite—OT sectors remain on-premises while business functions gradually migrate to the cloud.

- **AI in Practice: Benefits, Risks, and Governance**

AI adoption is already evident across multiple functions, including policy compliance agents, pre-filled security questionnaires, SaaS vendor onboarding, extraction request reviews, insurance coverage validation, alert correlation, and fraud detection. While these applications deliver significant efficiency gains, participants acknowledged persistent challenges. Measuring ROI remains complex relative to licensing costs, and uncontrolled “ghost AI” has triggered incidents involving data loss prevention (DLP) in some organizations. Leaders emphasized the need for cultural education, balancing usability with security, and promoting safe AI usage in both personal and professional contexts. The shared conclusion is that AI offers tangible benefits, but governance, ROI tracking, and user training are critical for secure and sustainable adoption.

BEST PRACTICES AND FUTURE STRATEGIES

The roundtables highlighted a set of best practices and forward-looking strategies, reflecting both immediate needs and long-term priorities. Participants emphasized the importance of strengthening SaaS security through the deployment of SSPM solutions and the development of clear playbooks for effective alert management. For smaller teams, leveraging external partners such as Managed Security Service Providers (MSSPs), Managed Detection and Response (MDR), or Extended Detection and Response (MXDR) was seen as a practical way to scale capabilities without overburdening internal staff. Vendor governance also emerged as a recurring theme, with leaders stressing the need to standardize contracts to include SLA and disaster recovery clauses, audit rights, and mandatory report sharing to reduce ambiguity and enhance accountability.

Resilience planning was highlighted as another essential practice, requiring organizations to go beyond theoretical policies by conducting manual exercises, regularly testing backup workflows, and ensuring management understands the inherent limitations of SaaS disaster recovery. Meanwhile, a robust critical data management strategy was recommended, ensuring redundant storage of essential business data across multiple trusted vendors to minimize service disruption impact. AI enablement was also addressed, with CISOs advocating for the approval and monitoring of sanctioned AI tools, comprehensive employee training on secure AI usage in both personal and professional contexts, and tracking adoption metrics to inform licensing decisions.

Looking forward, CISOs stressed the importance of establishing multi-layered vendor trust mechanisms, going beyond compliance certifications to provide a more reliable view of current security practices. They highlighted the need to create ROI dashboards for AI initiatives to justify license investments and maintain organizational confidence in new technologies. Continuity planning should also be institutionalized, with resilience playbooks and exercises treated as evolving documents and activities rather than one-time actions. Finally, leaders recommended aligning cybersecurity adoption strategies with sector-specific risk appetites, while recognizing AI as both a productivity driver and a governance challenge requiring ongoing oversight and training.

CONCLUSION

The GoSec25 CISO roundtable highlighted a thought-provoking reality: technology may shift responsibilities, but it does not absolve leaders from accountability. Whether it concerns SaaS adoption, compliance frameworks, disaster recovery planning, or AI governance, the weight of consequences ultimately rests on the shoulders of security executives.

Blind spots, compliance gaps, and governance challenges will not disappear. However, by implementing the right solutions, negotiating stronger vendor contracts, testing continuity plans, and adopting AI responsibly, organizations can reduce uncertainty and strengthen resilience.

The path forward is not about eliminating risk entirely complete elimination is never possible. Rather, it is about managing risk transparently, ensuring leaders understand their choices, and aligning resilience strategies with organizational priorities.

APPENDIX

KEY QUESTIONS DISCUSSED

1. Cloud and SaaS Security

- Does the cloud enhance our security, or does it simply shift our blind spots?
- With the expansion of cloud adoption in enterprises, are you concerned about:
  - Multi-cloud security governance (avoiding fragmentation)?
  - “Ghost AI” and the proliferation of SaaS: how can visibility be restored?
  - Could SaaS governance become the next major blind spot in enterprise security?

2. AI and Cybersecurity

- With the global trend of AI adoption, how do you plan to leverage it to strengthen your cybersecurity?
- Are you using AI for detection, response, and automation?
- Do you delegate this responsibility to your service providers?
- Are you able to measure AI’s benefits effectively?
- Have you observed risks associated with generative AI (data leakage, hyper-manipulations, adversarial attacks)?

Organizer:

Julien Turcot, Senior Vice President of Sales, GoSecure
The author thanks GoSecure and the participating CISOs for their candid contributions to the roundtable.