BDO DIGITAL

Guardians of digital trust

Enabling a cybersecurity-driven board in the age of AI

Introduction

Rocco Galletto
Partner & National Cybersecurity Leader
BDO Canada LLP

With over 25 years of experience in technology and cybersecurity services, Rocco has been instrumental in shaping the IT and cybersecurity landscape for organizations across several industries. During the past twelve years, he has been focused exclusively on helping some of Canada's largest retail, public sector, and financial services organizations develop comprehensive cybersecurity strategies, and execute strategic cyber transformations. Rocco uses his ability to customize and enhance security programs for businesses of all sizes, across all sectors, based on their specific risk profile.

Rocco's expertise is focused on helping organizations right-size cyber risk management strategies and establish comprehensive cyber defence programs. These initiatives are designed to not only detect and counter cyber threats but also to provide critical support in the event of cyber incidents, ensuring a fast and safe return to normal operations for his clients. He leverages his lessons learned with cyber incident response services, to inform continuous improvement actions for his clients, helping them keep pace with the ever-changing cyber threat landscape. His commitment extends to educating Boards of Directors on navigating the complexities of cyber risk management effectively through education sessions, simulation exercises and breach response workshops.

Over his 25-year career, Rocco consistently demonstrates a passion for client success which has fostered long lasting partnerships and a reputation for excellence in delivery. His dedication to leadership and service has consistently driven positive outcomes, making him a trusted advisor in the IT and cybersecurity domain.

What we'll cover

1	Cybersecurity and digital transformation
2	The state of cybersecurity and current organizational gaps
3	Defining the board's role in cybersecurity oversight
4	6 strategies to improve board oversight of cybersecurity
5	Q&A

Cybersecurity & digital transformation

Techtonic States

Unprecedented demand - unparalleled opportunity

84% of business leaders* say their organisation will only survive if it significantly accelerates its technology innovation

81% of business leaders say technology is the number one critical enabler of their overall strategy

86% Say the failure to leverage technology is a risk that will impact my organisation over the next three years

75% Say the lack of technology expertise is the greatest risk to growth

"If you are a business leader and you're not already working side by side with your Technology leader - you'd better get there fast"
Ric Opal, BDO Digital

Technology drives the agenda for both risk management and business growth.

Top 5 measures to manage risk:

- ✓ Increased R&D
- ✓ Investment in AI
- ✓ Investment in innovation
- ✓ Investment in technology and digital transformation
- ✓ Increased cyber-protection

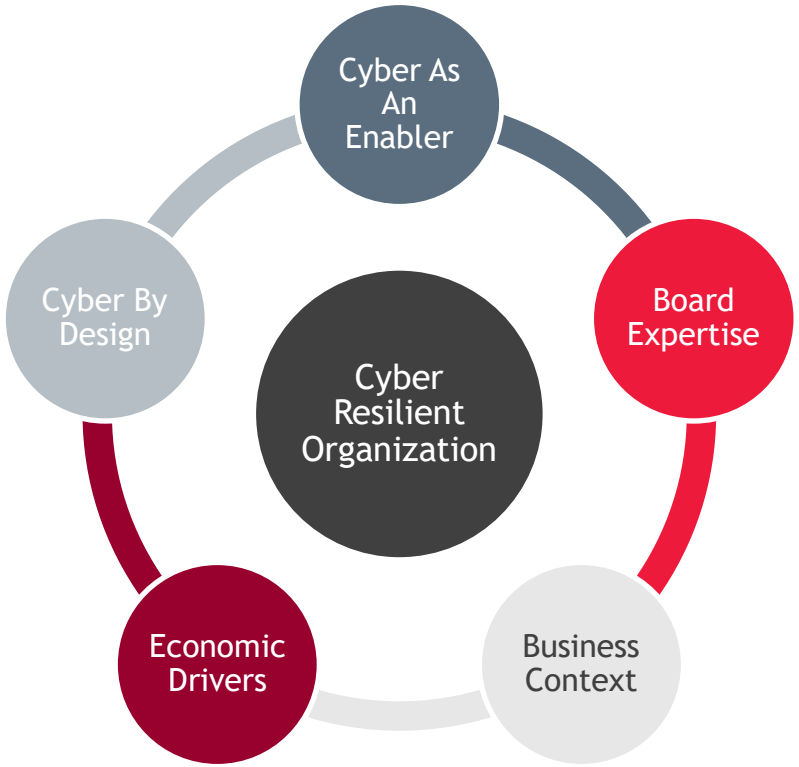
Top 5 strategies to gain competitive advantage:

- ✓ Adoption of AI & advanced digital solutions
- ✓ Data-based innovation of services, products and processes
- ✓ Shifting focus to higher value products and services
- ✓ Increased automation of tasks to improve productivity
- ✓ Supply chain restructuring and pivoting into new lines of business

** Data from a global survey of 500 C suite and C-suite-minus-one in 2023*

The critical role of cybersecurity

Protecting organizations as they adopt new technologies on their digital transformation journeys



Cyber security is about protecting the digital domain and the information available in the digital space from unauthorized access and unauthorized use.

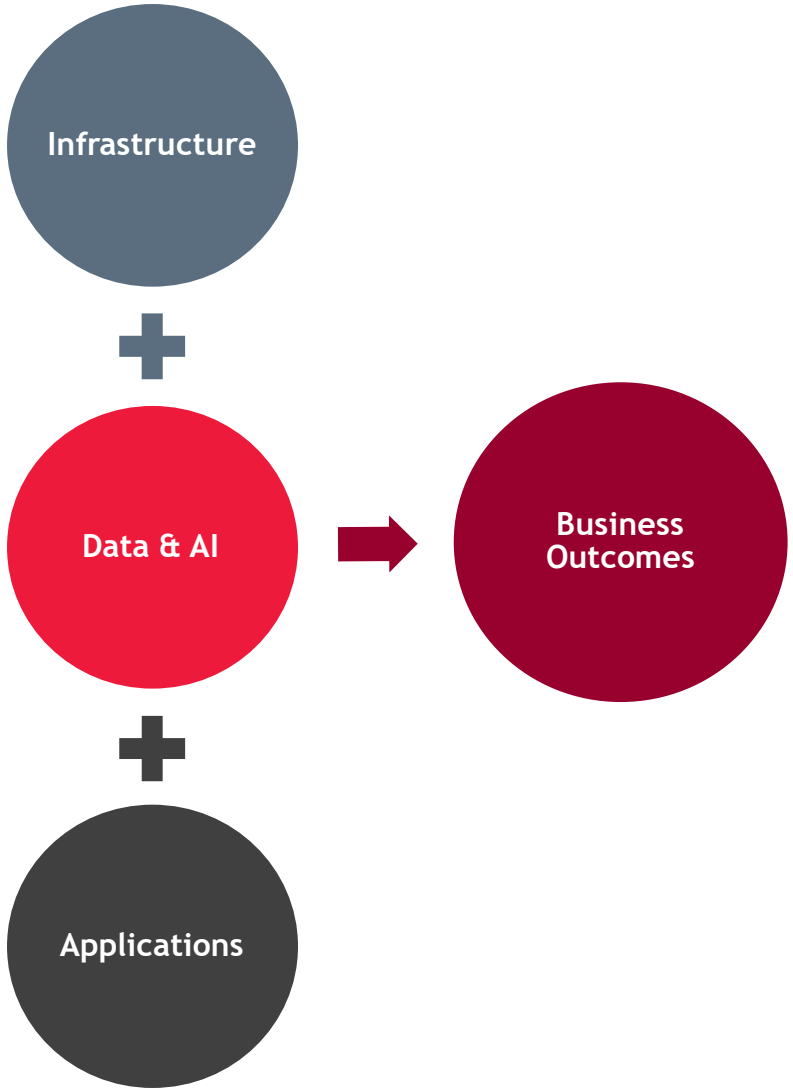
Boards, C-level executives, security & IT teams, and business units are all responsible for managing cyber risk.

“Shifting cyber left” by engaging cyber teams at the ideation phase of any digital transformation will ensure resilience.

Translating cyber risk to business risk is often a challenge for IT and Security professionals.

Business value realization

Transitioning from fear to value creation | Breaking down the barriers



Infrastructure Security: Protecting our digital pathways through access controls and ensuring vulnerabilities are quickly remediated.

Data & AI Security: Classifying and protecting sensitive data, ensuring the data remains free form tampering or unauthorized access and protecting the AI models from tampering.

Application Security: Protecting the code, software, access and logic flows from unauthorized access and use.

Uninterrupted operations for continuous positive business outcomes

Manage risk to continue to accelerate your business

Understanding and managing risks to enable acceleration

Privacy and data security

To produce sophisticated, human-like outputs, Gen AI models undergo training on vast and diverse data sets, which may contain personal, private, or proprietary information.

Sensitive data exposure or leakage.

Responsibility and accountability

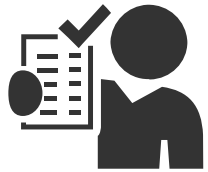
Blurred lines between the work of Gen AI models and original human creativity have sparked discussions about who should own the generated content and how to safeguard against data misuse.

Who is accountable and who owns the output?

Misinformation and inaccuracies

Generative large language models (LLM) are known to produce “hallucinations,” which are false or nonsensical claims or fabricated information.

Confidence in erroneous outputs or decisions made based on misleading information.



Bias and discrimination

AI can adopt implicit or explicit biases in its training data, including those related to race, sex, age, religion, geographic location, and more.

Biases injected or learned change the outputs.

Regulations and requirements

Industry regulations and ethical requirements may not have been factored in during training of LLM or Gen AI models.

Regulatory risks and legal liabilities continue to evolve.

Where we’re at today

Global trends

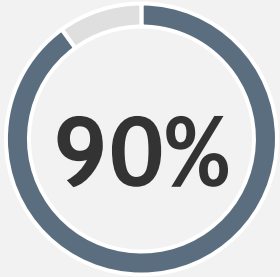
Growing cyber inequity

We are seeing a growing divide between cyber-resilient organizations and those who are not.

Contributing factors:

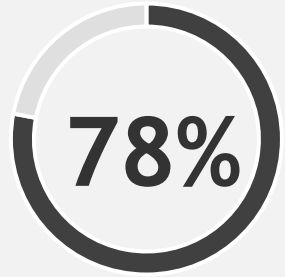
- Rising cost of cyber services and tools
- Labour/skills shortage
- Increasingly sophisticated threats
- Macroeconomic trends
- Geopolitical conflicts
- Industry regulations that vary in scope across the globe
- Early adoption of new technologies (e.g., Gen AI)

World Economic Forum
Global Cybersecurity Outlook (2024)



of cyber leaders believe that inequity within the cybersecurity ecosystem requires urgent action.

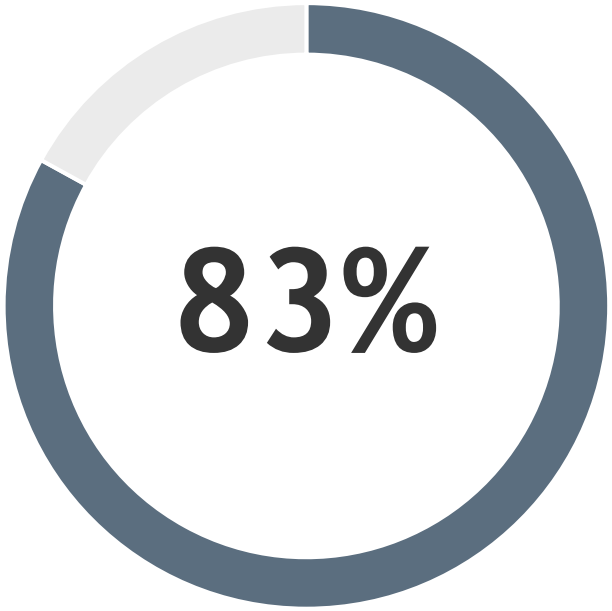
of leaders of organizations excelling in cyber resilience trust their CEO to speak externally about their cyber risk.



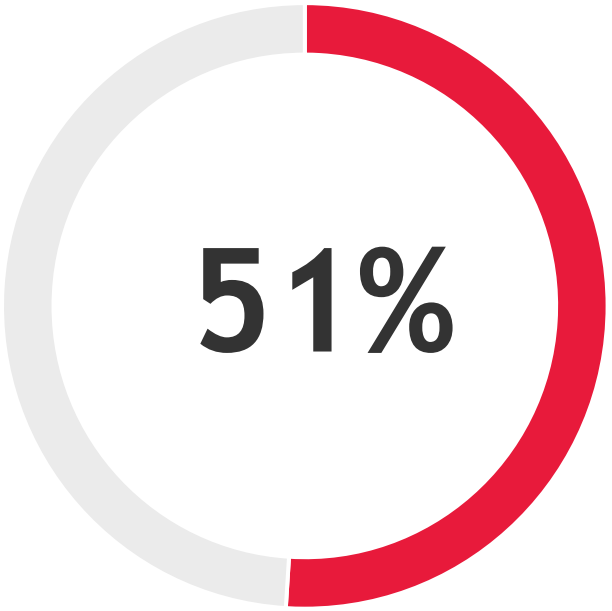
of organizations that consider themselves to NOT be cyber resilient say they don't have visibility of their third-party risk.

Will Gen AI benefit attackers or defenders?

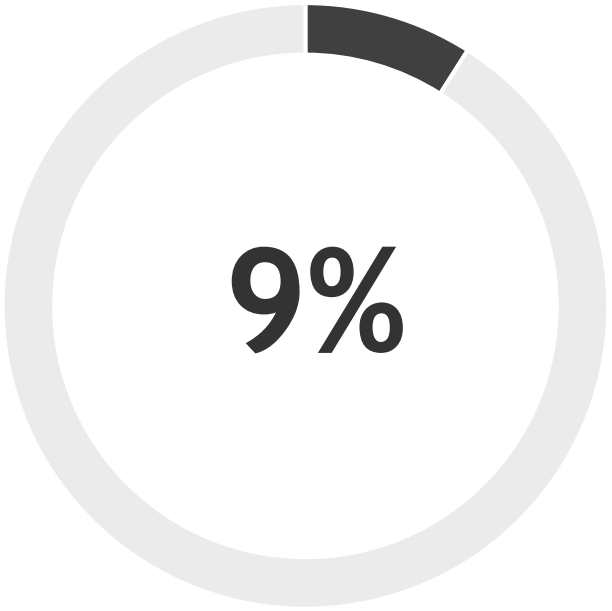
How experienced are boards in cybersecurity?



of organizations surveyed have had more than one data breach (IBM)



of Fortune 100 companies have a director on their boards with cybersecurity experience (Forbes)



of Fortune 200 and 500 companies have a director on their boards with cybersecurity experience (Forbes)

Responding to a breach is a long and intensive process for many organizations

277

Average number of days needed to identify and contain a cybersecurity breach (IBM)

100 DAYS

200 DAYS

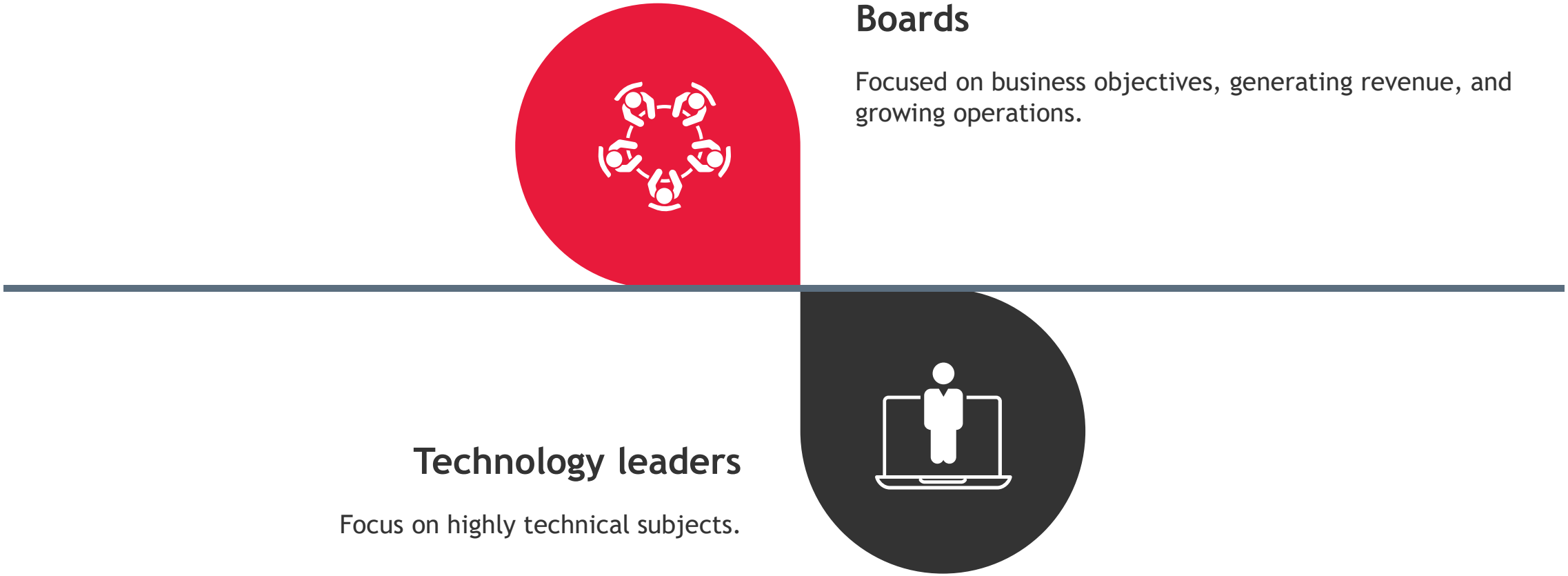
300 DAYS

Poll

Does your organization have a board of directors? If so, does your board have at least one director with cybersecurity experience?

Gaps in board oversight and how to redefine their role in cybersecurity

Boards and technology leaders often have different priorities



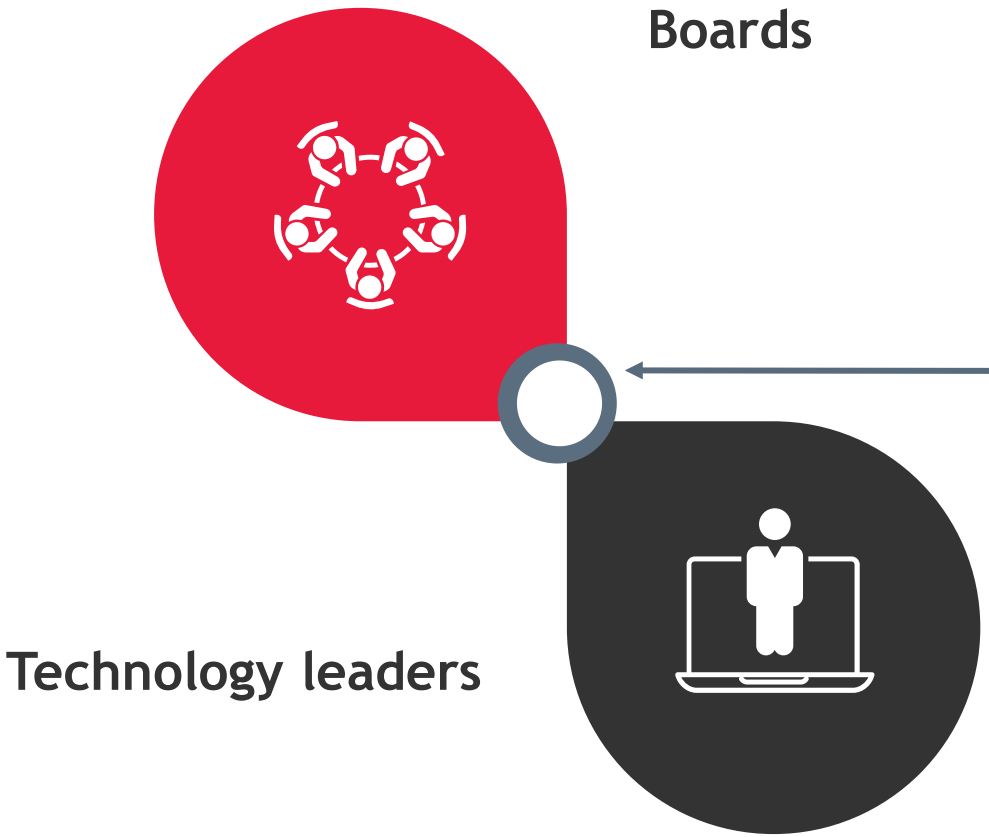
Boards

Focused on business objectives, generating revenue, and growing operations.

Technology leaders

Focus on highly technical subjects.

Shift the conversation, meet in the middle



Security conversation should focus on

BUSINESS RISK

- ☑ Translate technical issues into a business risk discussion (e.g., risk of corporate digital assets)
- ☑ Jointly assess and evaluate the organization's security posture on a regular basis using simple measures boards can understand
- ☑ Collaborate on cybersecurity governance approaches, solutions, and changes.

Strategies to deploy

Improving board oversight of cybersecurity

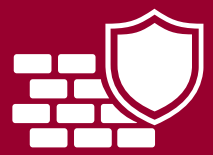
6 strategies you can follow

1. Conduct frequent board education sessions

2. Use common sense metrics

3. Create a safe environment to openly discuss risk

4. Discuss the financial impact of cybersecurity



5. Involve the board on a macro level during a security breach

6. Add a cybersecurity expert seat to the board

Contact:

Rocco Galletto
Partner & National Cybersecurity Leader
BDO Canada LLP
rgalletto@bdo.ca
416-729-2609