Cybersecurity's role in **digital transformation**: Why early engagement matters

Cybersecurity Awareness Month 2025

Rocco Galletto
Global Cybersecurity Leader
rgalletto@bdo.ca

Digital transformation is reshaping industries. Organisations are investing in cloud, AI, and data analytics to drive growth and agility. Yet, cybersecurity is often brought in too late, treated as a technical safeguard rather than a strategic enabler. According to a new BDO-sponsored report by the International Data Corporation (IDC) only **40% of organisations integrate cybersecurity during the planning stage** of digital initiatives. This delay introduces risks that can derail progress and erode trust.

Cybersecurity must be part of the foundation. When cyber teams are engaged early, they help shape secure architectures, anticipate threats, and align controls with business goals. This proactive approach strengthens resilience and accelerates time to value.

Consider a retail company rolling out a new e-commerce platform. If cybersecurity is involved from the start, the team can advise on secure payment integrations, data privacy compliance, and fraud prevention. If brought in later, these risks may only surface after launch, potentially damaging customer trust and requiring costly rework.

Bringing cybersecurity early in the digital transformation journey, and ensuring success in that journey, will require:
- aligning cyber budgets with business strategy
- refreshing cyber programmes to stay relevant; and
- building cyber maturity for resilience.

Cyber budget optimisation: Align spend with strategy

Cyber budgets are increasing, but performance gains remain uneven. IDC data shows that even organisations with flexible budgets report an average of five incidents annually. The issue isn't lack of funding, it's how that funding is applied.

Effective cybersecurity investment starts with strategic alignment. Budgets should support capabilities that reduce risk and enable transformation. This includes proactive detection, automation, and collaboration across departments. Organisations that embed cybersecurity into planning report fewer delays and stronger stakeholder confidence.

For example, when a private equity firm and their portfolio companies invest in cloud migration, they typically consider application redesign, data migration, modernisation, operational efficiency and system availability.

However, cybersecurity is often overlooked, especially in areas like regulatory impact assessments, secure coding practices during the build phase, and the security of application interactions with other systems. Without proper controls, sensitive data may be exposed. A more effective approach is to align the budget with the transformation roadmap, embedding security into every layer and step of the process.

Late-stage engagement leads to rework, missed deadlines, and diminished returns. To maximise impact, cybersecurity must be treated as a strategic partner, not a reactive fix. This need for strategic alignment naturally leads to the next consideration: how often organisations pause to reassess their cybersecurity approach.

Cyber strategy refresh: A practice worth prioritising

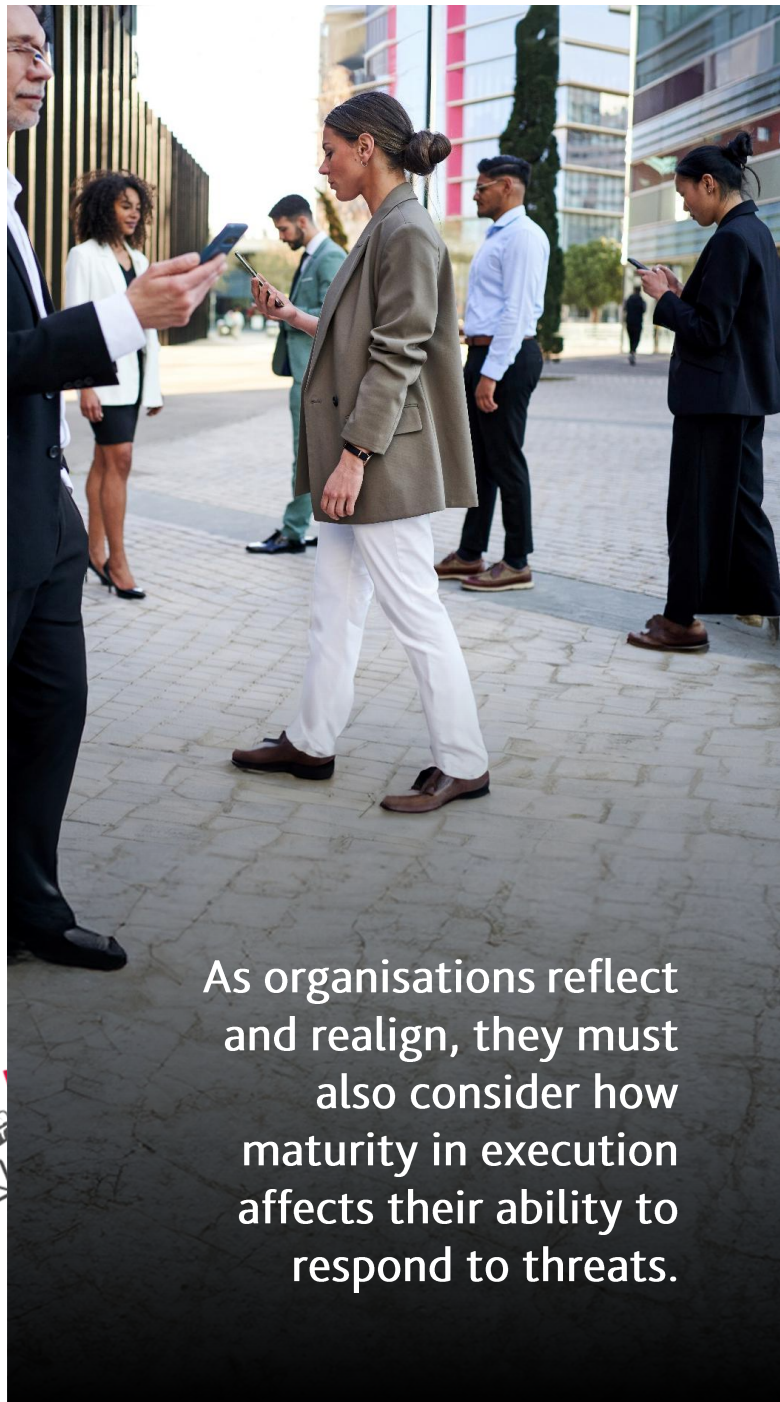
In a fast-moving environment, pausing to reflect may seem counterproductive. But it's essential. Cyber leaders must regularly reassess their strategies to ensure they remain aligned with business priorities.

Annual refreshes, outcome-based metrics, and cross-functional collaboration help teams stay relevant and effective. Reflection also reveals legacy practices that hinder progress. By shifting to agile, business-aligned approaches, cybersecurity teams can foster innovation and drive better outcomes.
This practice strengthens collaboration between cyber and business units, breaks down silos, and builds trust. It's not just about keeping pace, it's about leading with purpose.

A leading retailer, renowned for embracing technological innovation, has continually enhanced customer engagement through personalised experiences designed to foster loyalty. With several distinct business units, the organisation aimed to boost brand awareness, gain insights into spending behaviours, and deliver tailored offers that set them apart from niche competitors. Their journey of technology transformation was linked with business evolution, where security played a pivotal role ensuring that controls effectively supported new digital capabilities.

Although regular assessments were part of their routine, the latest advancements resulted in the need to reevaluate the overall strategy. This included integrating new features, aligning success measures with anticipated business outcomes, and ensuring the strategy remained aligned to changing needs. System availability was crucial for customer adoption, while safeguarding consumer information was critical for maintaining trust.

The refreshed strategy introduced ongoing collaboration with business units, improved communication channels, and the establishment of key performance indicators. These included uptime metrics and security scorecards, enabling swift identification and mitigation of risks. This proactive approach ensured optimal system availability and reinforced consumer confidence in the brand.



As organisations reflect and realign, they must also consider how maturity in execution affects their ability to respond to threats.

Cyber maturity: The true measure of resilience

Budget size doesn't guarantee security. IDC's findings show that **process maturity is the strongest predictor of resilience**. Organisations with proactive detection and investigation capabilities report fewer incidents and faster recovery times.

Mature organisations track leading indicators like time to detect, patching rates, and training effectiveness. These metrics provide visibility into operational health and help close the gap between perceived readiness and actual capability.

Boards are increasingly asking for proof of cyber-risk reduction. Without process-level metrics to complement outcome-based metrics, organisations risk overestimating their resilience. Real maturity comes from disciplined execution and continuous improvement.

A financial services firm for example, pivoted their strategy to prioritise the measurement of key outcomes aligned with specific, performance-enhancing objectives. By viewing threats through the adversary's perspective, they constructed a detailed threat model which surfaced the most prevalent threats targeting businesses within their sector. This comprehensive review encompassed a summary of potential attack vectors, alongside an assessment of the firm's ability to withstand attacks of this nature.

By collecting data on comparable organisations affected by security incidents, the security team identified common patterns in attack types and integrated these insights into a prioritised protection framework for the business. Together with business leaders, the team developed service levels tied to performance and outcomes, placing an emphasis on metrics to improve resilience against the most common attack types. This approach enabled a focused allocation of resources and budget to areas presenting the highest risk.

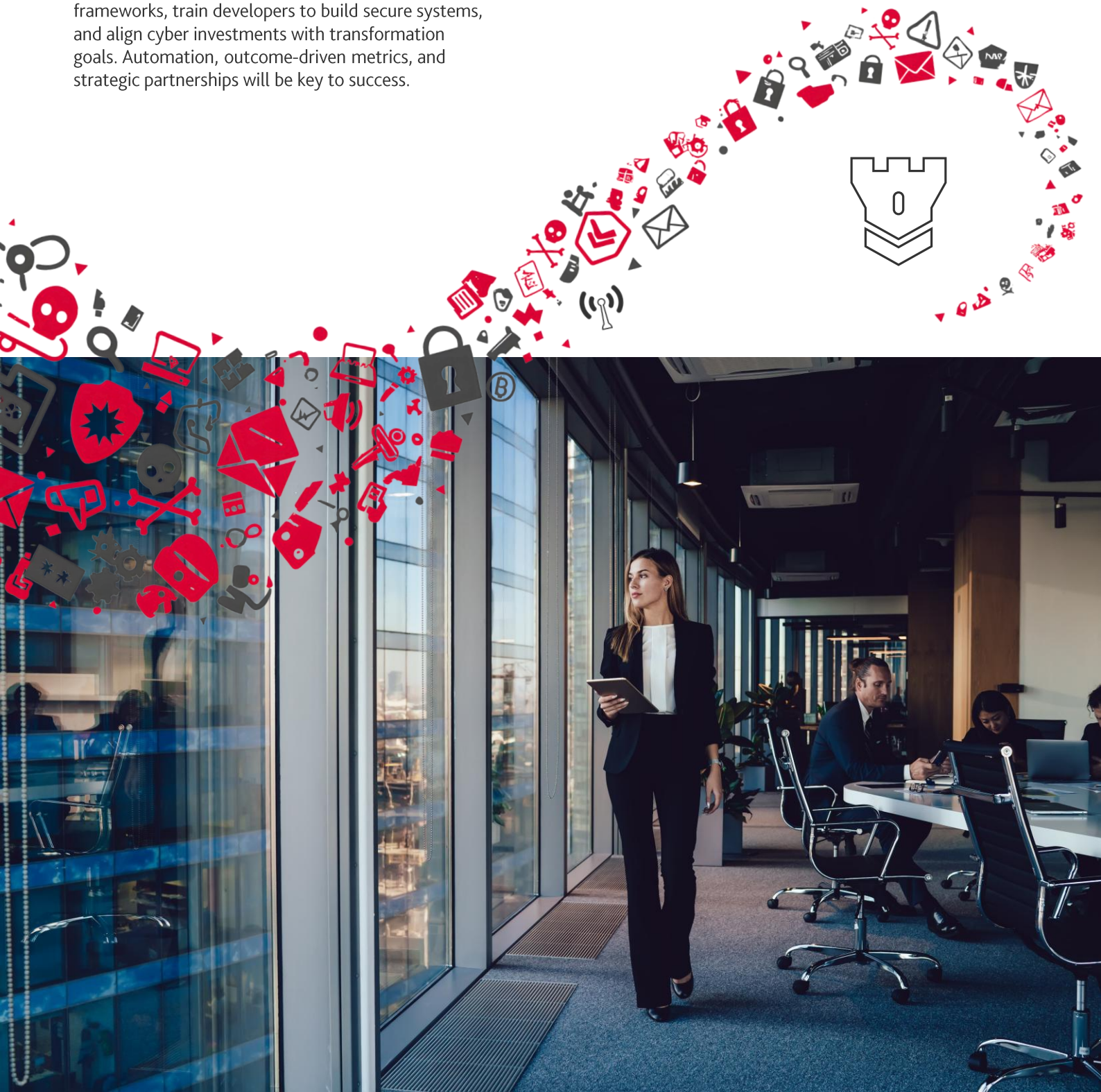
The security team elevated organizational confidence among Board members and business stakeholders, while operational efficiency was improved through a significant reduction in security incidents. This level of maturity becomes even more critical as organisations embrace emerging technologies like GenAI.

Cybersecurity as a catalyst for innovation

Emerging technologies like GenAI are transforming business functions and introducing new risks. Cybersecurity must evolve to keep pace.

Organisations should embed GenAI into governance frameworks, train developers to build secure systems, and align cyber investments with transformation goals. Automation, outcome-driven metrics, and strategic partnerships will be key to success.

Cybersecurity isn't just about protection. When integrated early and executed with maturity, it becomes a catalyst for agility, competitiveness, and long-term growth.

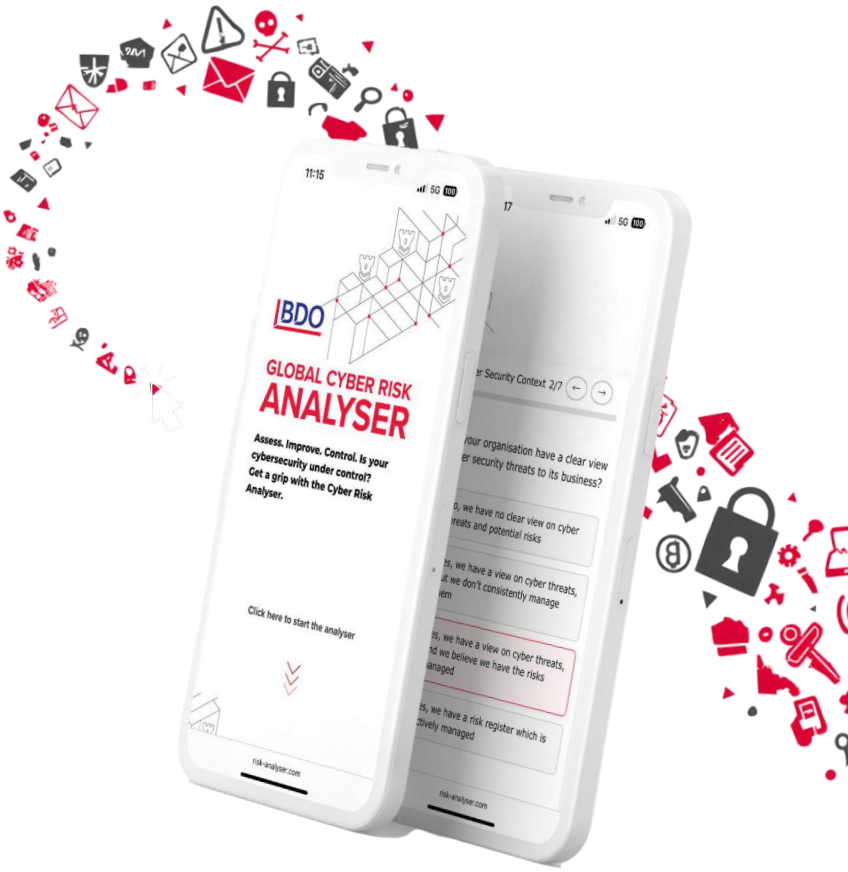


Final takeaway

Cybersecurity must lead, not follow. By embedding cyber at the core of digital transformation, organizations can scale securely, innovate confidently, and stay ready for what's next.

To explore the full findings and insights referenced in this article, we encourage you to:

- Download the IDC report to understand how cybersecurity leaders are navigating transformation and aligning strategy with execution.
- Register for our webinar to hear from our global team on building cyber resilience.
- Explore the Cyber Risk Analyzer tool to assess your organisation's current posture.



DOWNLOAD THE REPORT

REGISTER FOR OUR WEBINAR

EXPLORE THE CYBER RISK ANALYZER