How to get the best ROI from your **cybersecurity** budget while reducing risk

Cybersecurity Awareness Month 2025

Gilchrist Mushwana
Partner & National Head of Cybersecurity
BDO South Africa
gmushwana@bdo.co.za

In today's digital-first economy, cybersecurity budgets are increasing across industries. Yet despite this growth, many organisations continue to experience frequent incidents, delayed recoveries, and stalled transformation efforts.

The real challenge is not the size of the budget, but how effectively the money is being used to reduce risk and enable business performance.

Budget growth without performance gains

A global BDO-sponsored survey from International Data Corporation (IDC) reveals a telling disconnect. Nearly half of organisations have flexible cybersecurity budgets, yet still average over five incidents per year. This suggests that budget adequacy alone does not guarantee resilience.

Performance depends on how strategically budgets are allocated. Organisations that align spending with operational readiness, process maturity, and transformation goals consistently report stronger outcomes. In contrast, those who treat cybersecurity as a reactive cost center often struggle to translate investment into measurable impact.

Tips to maximise the impact of your cybersecurity budget

To make every cybersecurity investment count, organisations must adopt a performance-driven approach. This means moving beyond reactive spending and focusing on strategic execution. Here are five key strategies to help maximise the value of your cybersecurity investments.

01

Prioritise risk-based investments.

Effective budgeting begins with understanding your organisation's unique risk landscape. Identify the most critical threats—such as ransomware, insider threats, or supply chain vulnerabilities—and allocate resources to address them first. Risk assessments should guide budget decisions, ensuring that funds are directed toward areas with the highest potential impact.

Why this matters: the IDC report found that organisations with proactive risk modeling and governance frameworks experience fewer disruptions and faster recoveries. Prioritising risk-based investments helps ensure that cybersecurity spending is aligned with business priorities.

02

Invest in operational readiness.

Budget effectiveness is closely tied to operational maturity. Organisations with 24x7 threat monitoring and response capabilities detect and contain threats more quickly, reducing dwell time and limiting damage. These capabilities provide the visibility and agility needed to respond to evolving threats in real time.

Key areas to fund include:

- Continuous monitoring (internal or outsourced)
- Automated threat detection and response
- Endpoint protection for hybrid workforces
- Incident response playbooks and tabletop exercises

Organisations with optimised detection and investigation processes, often supported by AI and extended detection and response (XDR) tools, generally report significantly fewer incidents and faster recovery times.

03

Rationalise the tech stack.

Tool sprawl is a common challenge that leads to complexity, inefficiency, and wasted spend. Many organisations accumulate overlapping tools over time, creating integration challenges and increasing operational overhead. Consolidating the tech stack can improve visibility, reduce costs, and enhance overall effectiveness.

Tip: Look for platforms that offer orchestration, automation, and unified visibility across endpoints, networks, and cloud assets. Streamlined solutions not only reduce complexity but also improve response times and reduce the likelihood of misconfigurations.

04

Conduct cyber simulations.

While outsourcing can offer scale and efficiency, certain capabilities are best developed internally. These include governance, risk modeling, and employee awareness programmes. Building these capabilities in-house ensures that cybersecurity is embedded into the organisation's culture and decision-making processes.

Focus areas include:

- Cybersecurity training and awareness programmes
- Governance, risk, and compliance integration
- GenAI risk management frameworks

As GenAI adoption grows, organisations must address new risks such as phishing, data leakage, and governance gaps. Investing in employee training and AI-specific security controls is essential to mitigate these emerging threats.

05

Measure leading indicators, not just outcomes.

Boards and executives often ask for metrics like incident frequency or cost savings. While these are important, they do not provide a complete picture of cybersecurity maturity. Leading indicators, such as time to detect, patching rates, and training effectiveness, offer deeper insights into process health and operational readiness.

Why this matters: Without visibility into internal processes, organisations may overestimate their resilience. Measuring leading indicators helps identify gaps early and supports continuous improvement.

Future-proofing your budget strategy

Cybersecurity budgeting must become more strategic, with organisations shifting toward models that link funding to measurable improvements in risk reduction, recovery speed, and transformation success. To stay effective, budgets should be reassessed regularly and aligned with evolving threats and business priorities. The IDC report highlights three key areas of focus: increased automation through AI and machine learning, targeted mitigation strategies to address emerging GenAI risks, and stronger governance around third-party risk, which remains underfunded despite its role in many breaches. When cybersecurity investments are tied to clear outcomes and business goals, they become a driver of resilience, innovation, and long-term growth.

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

- Download the report to learn how cybersecurity leaders are aligning strategy with execution to drive transformation.
- Register for our upcoming webinar to hear directly from BDO's global cyber team on building cyber resilience in today's evolving threat landscape.
- Explore the Cyber Risk Analyzer tool to assess your organisation's current cybersecurity posture and identify areas for improvement.

DOWNLOAD THE REPORT

REGISTER FOR OUR WEBINAR

EXPLORE THE CYBER RISK ANALYZER

These resources are designed to help you make informed decisions, strengthen your cybersecurity strategy, and get the most value from your budget.