Deloitte.

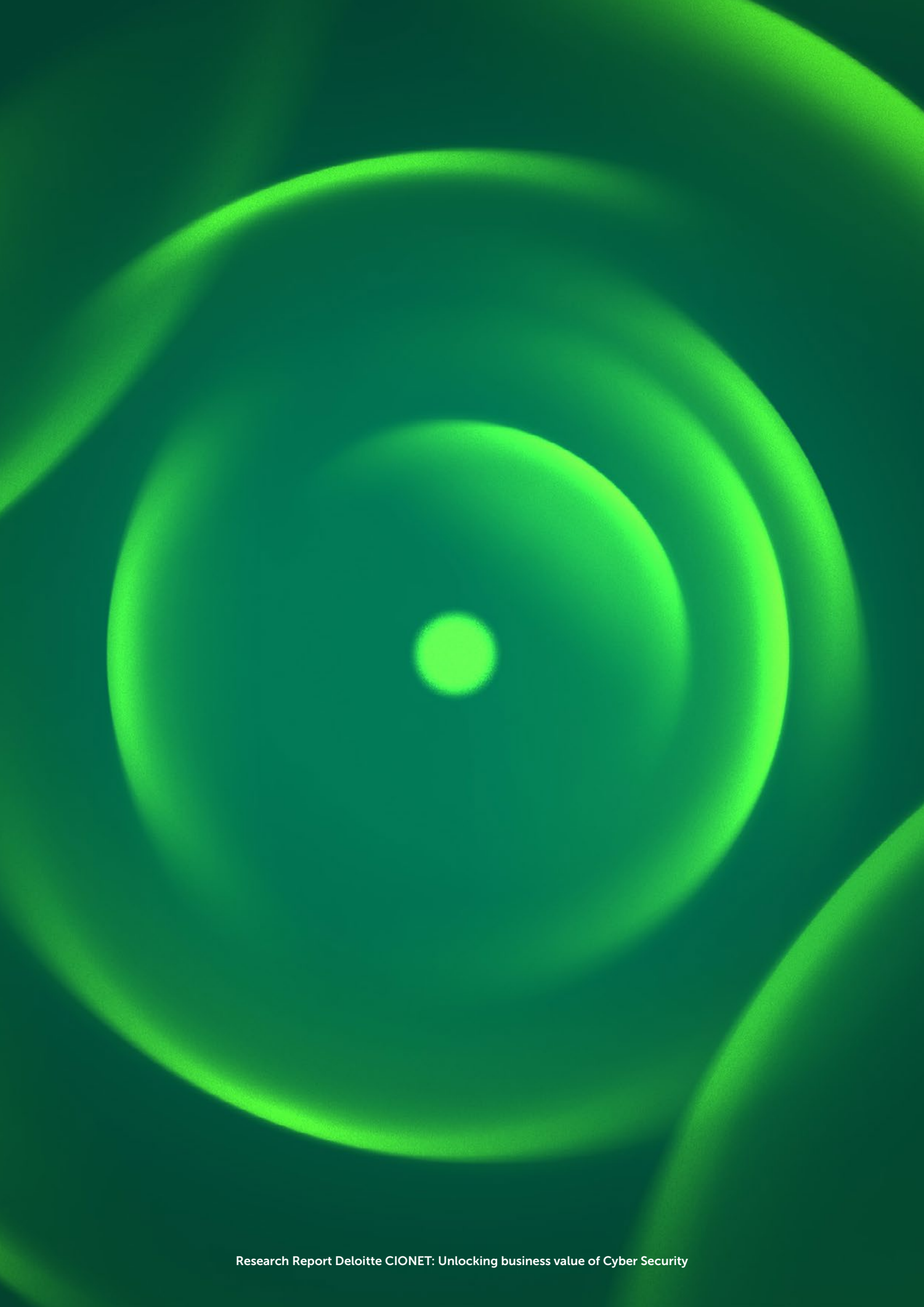
CIONET
What's next.

RESEARCH REPORT DELOITTE CIONET:

Unlocking business value of Cyber Security

Research Report

January 26



CONTENTS

INTRODUCTION

In today's increasingly digital and interconnected world, cyber security has become a critical business imperative. Organisations face a growing array of cyber threats that can disrupt operations, damage reputations, and result in significant financial losses. As cyber risk continues to evolve in complexity and scale, effectively communicating the business value of cyber security to executive leadership is essential—especially in an environment of challenging budgets and competing priorities.

The purpose of this study was to assess how cyber security leadership is articulating the business value of cyber security to senior decision-makers. Through interviews with a diverse group of organisations, the report explores how cyber risk is assessed, how budgets are allocated, and how cyber maturity is developed and communicated within the business context. It also examines the emerging impact of artificial intelligence on cyber risk and investment decisions.

By analysing current practices and future expectations, this report provides a comprehensive overview of how cyber security leaders are navigating the complexities of demonstrating value, securing resources, and advancing capabilities. The findings highlight the need for pragmatic, flexible approaches that balance ambition with feasibility, enabling organisations to build resilience and protect business value in an increasingly complex cyber landscape.

Demographics and methodology

This interview-based study involved 15 organisations across 6 sectors. We retained mid-sized to large organisations to ensure relatable context, opportunities and challenges. This diverse sample provides a broad perspective on cyber security practices across different industries and organisational scales. The qualitative methodology focused on in-depth interviews with cyber security leaders to capture insights on risk, budgeting, maturity, and emerging technologies.

Figure 1 – Sectors

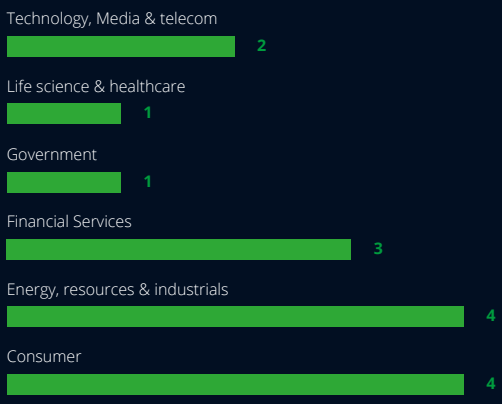
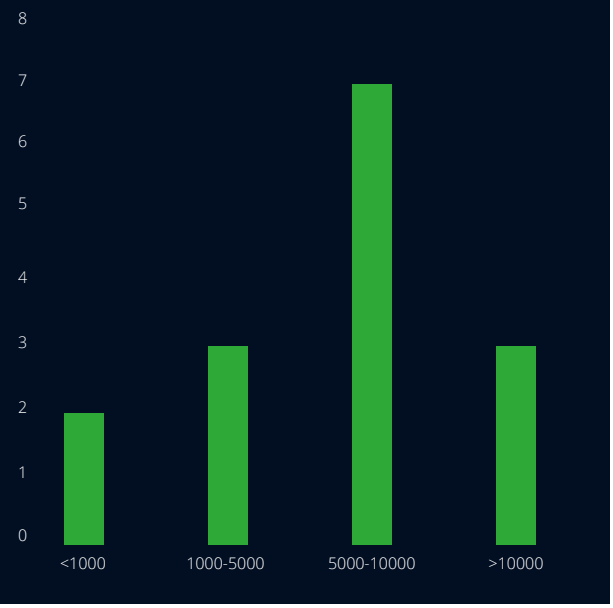


Figure 2 – Number of employees



15
organisations across 6 sectors.

Cyber risk

Interviewees generally acknowledge the significant business risk posed by major cyber incidents, though their assessments of likelihood and impact vary. All respondents agree that accurately assessing such impact is very difficult, yet most recognise that the potential financial consequences of a severe cyber event could be substantial, often reaching tens or even hundreds of millions of euros. Some interviewees are unable to estimate the impact or consider such quantification irrelevant for shaping cyber strategy. Estimating the probability of these incidents is even more challenging, with likelihood assessments ranging from very low to moderate (10-20%), reflecting the inherent uncertainty and complexity of cyber risk measurement. This variation points to differences in cyber risk management maturity and the availability of relevant data. Despite these disparities, there is a shared understanding of the critical importance of managing cyber risk as a key element of business resilience. In-depth cyber risk quantification is considered as either unachievable or prohibitively expensive.

Figure 3 – Worst case loss expectancy

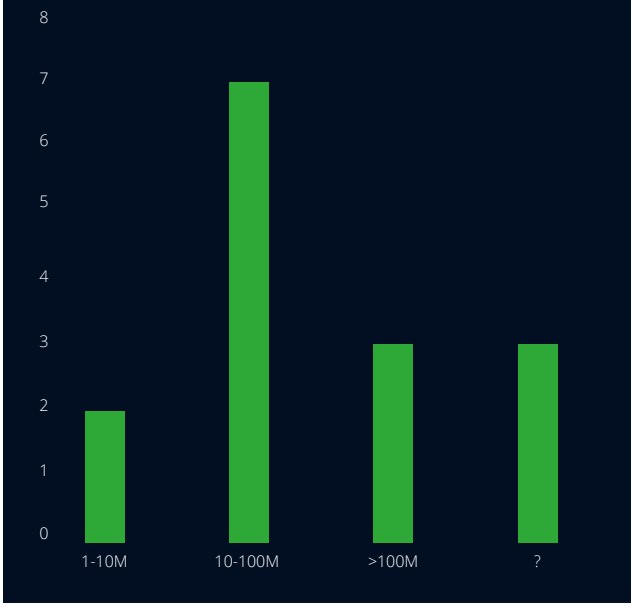
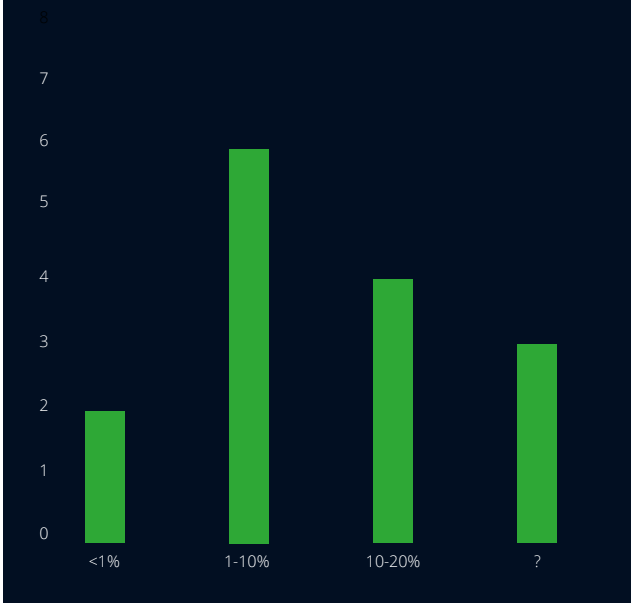


Figure 4 – Worst case likelihood



CYBER BUDGETING

Building on the complexities of cyber risk assessment, interviewees also highlighted challenges in cyber budgeting that closely reflect their perceptions of risk and organisational priorities. While cyber security is not necessarily included within the overall IT budget, comparing its size as a percentage of IT spend provides a common benchmark. Respondents noted considerable variation in cyber security budgets, alongside difficulties in accurately determining budget size due to incomplete data and differing views on which costs should be included. This underscores the broader challenge of aligning spending with an evolving cyber risk landscape. Interviewees also emphasised the difficulty of obtaining valid benchmarking data, particularly from companies within the same industry, which further complicates efforts to gauge appropriate budget levels.

The composition of cyber budgets varies notably, including in the balance between operational expenditure (OPEX) and capital expenditure (CAPEX). While some organisations allocate a significant share of their budget to ongoing operational activities such as monitoring, incident response, and cloud security services, others invest more heavily in infrastructure or technology purchases. Investments in operational technology (OT) security are sometimes considered part of the IT security budget; however, more often they are managed separately. This separation adds another layer of complexity, as OT security budgets are even harder to assess and benchmark, while they are often significant.

Looking ahead, most interviewees expect cyber budgets to increase, driven by increasing cyber threats and the growing importance of resilience. A smaller number anticipate stable budgets, while some remain uncertain about future changes. This general trend towards increased investment aligns with the recognition of cyber risk as a critical business concern. However, persistent challenges in quantifying both risk and budget requirements may continue to complicate efforts to optimise resource allocation and clearly demonstrate the business value of cyber security investments.

Figure 5 – Cyber budget versus IT budget

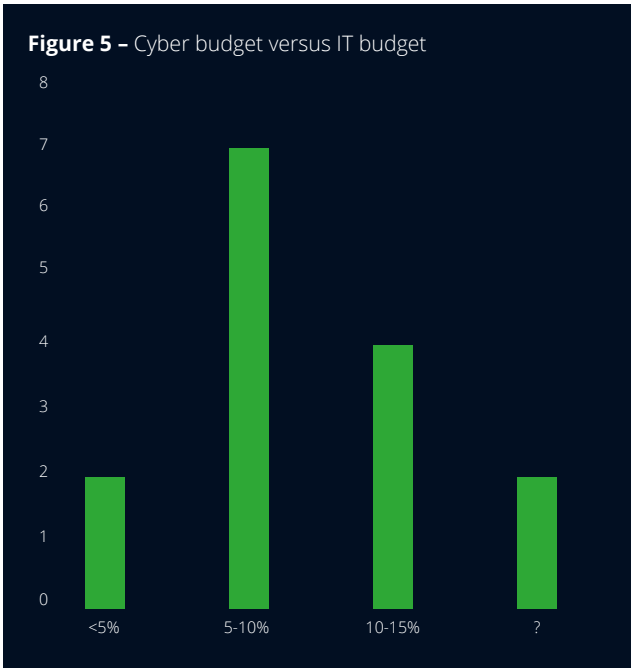


Figure 6 – OPEX % of cyber budget

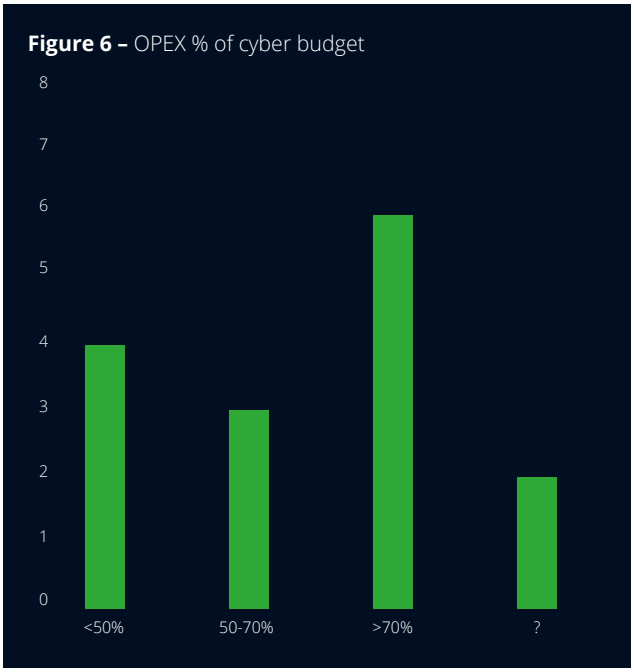
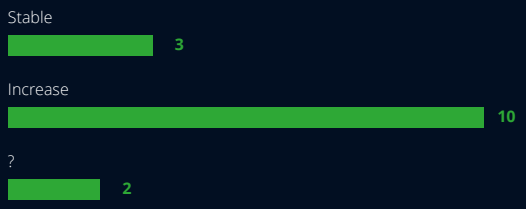


Figure 7 – Expected evolution of cyber budget



The majority of the cyber security budget is concentrated on three cyber security capabilities: Infrastructure Security, Identity & Access Management, and Detect & Respond. These areas receive the most significant investment, reflecting their critical role in protecting core systems, managing access, and ensuring timely detection and response to threats. In contrast, the remaining three capabilities—Cyber Security Management, Application Security, and Data Protection—receive considerably less budget today.

Infrastructure Security	Protection of network and IT/OT infrastructure including perimeter, on-premise and cloud systems.
Identity & Access Management	Managing user identities, authentication, authorisation, and access controls.
Detect & Respond	Day-to-day security monitoring, threat detection, incident response, and SOC activities.
Cyber Security Management	Governance, risk management, compliance, policy development, and security awareness training.
Application Security	Securing software applications through development lifecycle and runtime protection.
Data Protection	Safeguarding sensitive data at rest, in transit, and in use, including backup and recovery.

The largest share of the cyber security budget is devoted to Staffing, reflecting the critical role of skilled personnel in maintaining effective defence. Outsourcing also accounts for a significant portion, highlighting the reliance on external providers for monitoring, incident response, and specialised services. Cloud security services receive substantial investment, driven by the increasing use of cloud-based security tools and platforms. Spending on Security Software and Hardware is relatively low, indicating a shift from on-premise cyber security solutions to cloud security services. This budget distribution emphasises the priority placed on human expertise and flexible service models over purely technological investments, illustrating how organisations balance resources to address evolving cyber threats effectively.

Staffing	Salaries and benefits for cyber security staff, including SOC analysts, incident responders, security engineers, compliance teams, management, and support staff.
Outsourcing	Managed security service providers for monitoring, incident response, vulnerability management, and consulting services.
Cloud security services	Subscriptions for cloud-based security tools (SaaS SIEM, EDR, IAM, threat intelligence), cloud monitoring, and analytics platforms.
Security software	Licences for on-premises security software such as SIEM, IAM platforms, endpoint protection, application security tools.
Hardware	Firewalls, IDS/IPS appliances, servers for security operations, authentication devices, encryption hardware (HSMs).

CYBER MATURITY

The organisations surveyed are generally below level 3 on the CMMI scale, indicating that many are still developing or implementing defined and standardised cyber security processes. This suggests that while foundational practices may be in place, there is significant room for improvement in establishing consistent cyber security capabilities.

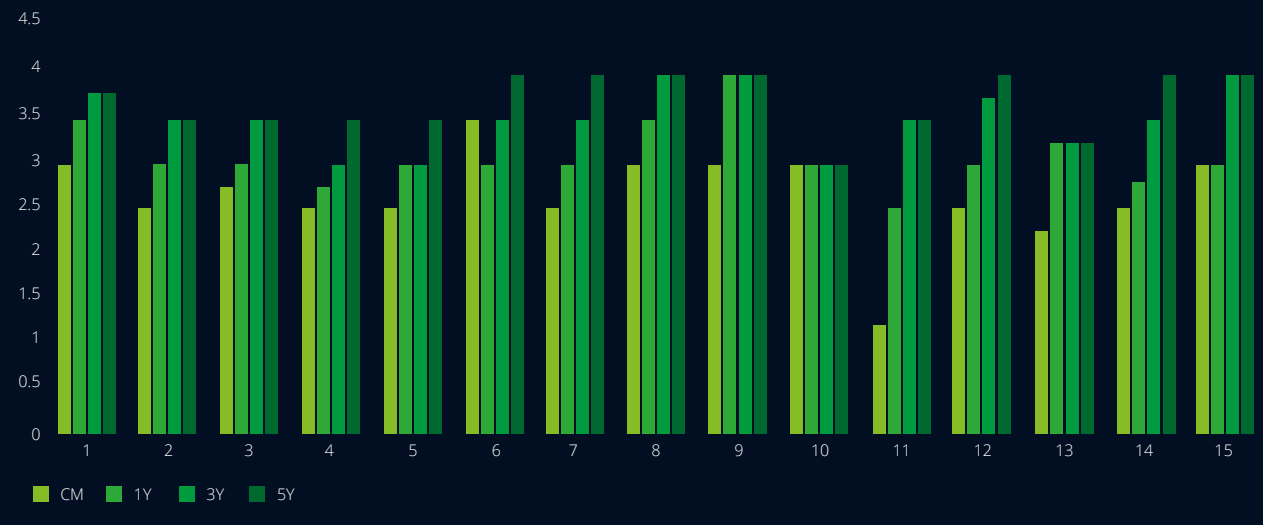
Looking ahead, the expected maturity levels show a gradual increase over one, three, and five years, but notably, there is little ambition among organisations to reach the highest maturity levels of 4 or 5. Most interviewees consider achieving level 5—characterised by optimised cyber risk management processes—as neither realistic nor affordable. This reflects a pragmatic view that the resource intensity and complexity required to reach the top maturity levels may outweigh perceived benefits.

Business leadership may still question the overall realism of the stated ambitions. Despite several years of investment in cyber security, many organisations have yet to fully achieve their target maturity levels. This indicates that progress is often slower than expected, potentially due to evolving threat landscapes, organisational challenges, or constraints in skills and funding. Furthermore, maturity levels might even decline despite ongoing investments if the changing cyber threat environment demands new, more advanced capabilities that organisations have yet to develop or implement, potentially levering AI (see next section).

Furthermore, there is uncertainty about what the ambition will be once target maturity levels are eventually achieved—if at all. It remains unclear whether organisations will seek to push beyond their current targets or if they will accept a certain maturity plateau as sufficient for their risk appetite and business needs. This uncertainty highlights the need for ongoing reassessment of cyber maturity goals in light of changing risks, technologies, and organisational priorities.

In summary, while there is a clear intent to improve cyber maturity over the coming years, current levels remain modest and ambitions are tempered by practical considerations. The gap between aspiration and achievement underscores the complexity of advancing cyber security maturity and calls for realistic, flexible strategies that balance ambition with feasibility.

Figure 8 – Expected evolution of cyber maturity



THE IMPACT OF AI

The impact of artificial intelligence (AI) on cyber security is viewed with a mix of caution and cautious optimism among interviewees, reflecting both potential risks and opportunities. Most respondents anticipate that AI will lead to an increase in cyber risk, driven by concerns over more sophisticated attacks, automated exploitation of vulnerabilities, and the rapid evolution of threat actors' capabilities. This underscores the dual-use nature of AI technologies, which can enhance both defensive and offensive cyber operations. However, a minority of interviewees do not expect AI to significantly change the cyber risk landscape, suggesting confidence in existing controls or uncertainty about AI's disruptive potential. Some remain unsure about the overall impact, highlighting ongoing ambiguity in this area.

When it comes to cyber budgets, opinions vary. While a few expect budgets to remain stable or even decrease due to potential efficiencies gained through AI automation, others foresee an increase in investment. This anticipated growth is linked to the need for new AI-enabled tools, enhanced skills development, and expanded monitoring capabilities to address emerging threats. The diversity of views reflects uncertainty about how AI will reshape resource allocation and whether organisations will prioritise AI-related spending within their broader cyber security budgets.

Regarding cyber maturity, perspectives are evenly divided. Some interviewees believe AI will have little to no impact on maturity levels, viewing maturity as primarily dependent on organisational processes and culture rather than technology alone. Conversely, others expect AI to drive improvements in cyber maturity by enabling more proactive threat detection and other cyber security capabilities (see table below). This split highlights differing expectations about how quickly and deeply AI will be integrated into cyber security practices.

In summary, AI is recognised as a transformative force with the potential to both increase cyber risk and enhance cyber maturity. Organisations face the challenge of balancing these dynamics by investing strategically to leverage AI's benefits while managing its risks. The evolving nature of AI's impact calls for ongoing vigilance and adaptability in cyber security strategies.

Figure 9 – Impact of AI on cyber risk

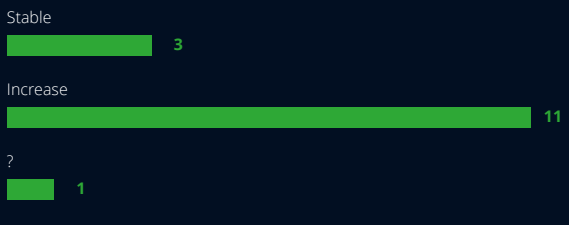


Figure 10 – Impact of AI on cyber budget

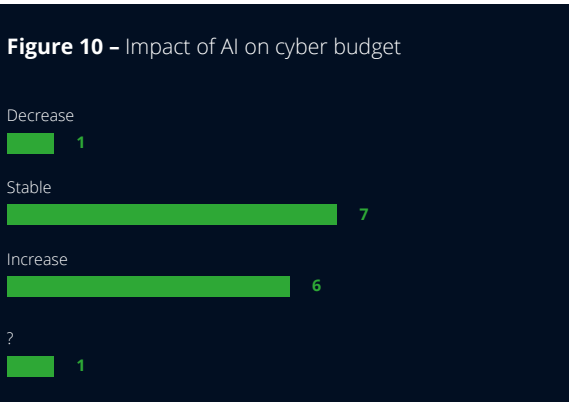


Figure 11 – Impact of AI on cyber maturity

The highest expected return on investment from AI in cyber security is seen in advanced threat detection and response, which enables faster identification of sophisticated threats and more proactive incident management—capabilities already present in current cyber security technologies. Interviewees also expect routine security tasks to be increasingly automated, allowing organisations to streamline repetitive processes and free up skilled staff for more strategic work. Policy and standards automation is valued for its role in keeping security frameworks aligned with evolving risks and regulations (although it remains important to make sure the policies and standards are realistic and achievable). Enhanced user behaviour analytics is recognised for improving detection of insider threats and compromised accounts. Overall, interviewees remain cautious about the overall benefits, emphasising that staff expertise will continue to be critical in realising AI's full potential.

Advanced Threat Detection and Response	AI-driven analytics enable real-time identification of sophisticated threats and anomalies, reducing detection time and enabling proactive incident response.
Automation of Routine Security Tasks	AI automates repetitive processes such as vulnerability scanning, patch management, and log analysis, freeing skilled personnel to focus on strategic security initiatives.
Policy and Standards Automation	AI can assist in the creation, continuous updating, and optimisation of cyber security policies and standards by analysing evolving threat landscapes, regulatory changes, and organisational risk profiles
Enhanced User Behaviour Analytics	Uses machine learning to establish baseline behaviours of users, devices, and applications, then detects deviations indicating insider threats or compromised accounts.
Compliance Assessment and Monitoring	Leveraging operational data and audit reports, AI systems can automatically assess adherence to policies and standards in near real-time, identifying gaps and compliance risks more efficiently than manual processes. This continuous compliance monitoring supports proactive risk management and audit readiness.
Predictive Risk Modelling	Machine learning models forecast emerging risks and potential attack vectors, allowing organisations to prioritise controls and allocate resources optimally.


Z-FOUR
WILMINGTON DE

CONCLUSION

The Challenge:

- Organizations acknowledge cyber risk but struggle to quantify it in business terms
- This gap between risk awareness and financial justification complicates budget allocation
- Most organizations operate at modest maturity levels with limited ambition to advance

The Reality:

- Cyber budgets vary widely (5-15% of IT spend) with no clear benchmarking standards
- Investment concentrates on Infrastructure Security, IAM and Detect & Respond
- Staffing costs dominate cyber budgets, yet talent shortages persist across the industry
- Progress toward maturity targets is slower than expected, often due to evolving threat landscapes

The Opportunity:

- AI presents increased risk from sophisticated attacks AND enhanced detection/response capabilities
- Pragmatic, achievable maturity goals resonate better with business leadership than ambitious targets

The Path Forward:

- Articulate the business value of cyber security through “business impact scenarios” that executives understand
- Establish realistic, industry-specific maturity targets
- Selectively invest in AI-driven automation to address staffing constraints and improve operational efficiency

KEY CONTACTS

Maarten Mostmans

Partner

Cyber Strategy & Transformation

mmostmans@deloitte.com

Wim Hermans

Partner

Cyber Strategy & Transformation

whermans@deloitte.com

Diederik Van Der Sijpe

Partner

Cyber Strategy & Transformation

dvandersijpe@deloitte.com

About CIONET

CIONET is the leading community of IT executives in Europe and LATAM. With a membership of over 10000 CIOs, CTOs and IT Directors, CIONET has the mission to help IT executives achieve their aspirations. CIONET opens up a universe of new opportunities in IT management by developing, managing and moderating an integrated array of both offline and online tools and services designed to provide real support for IT executives, so they can do more than just keep up with change but ultimately define it.

www.cionet.com

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms. Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 312,000 professionals, all committed to becoming the standard of excellence.

www2.deloitte.com