ECONOMIST IMPACT

Procurement and cybersecurity: a strategic disconnect

SUPPORTED BY SAP Ariba

As the severity and scope of external threats have escalated in recent years, the procurement function has come under increasing scrutiny for its role in safeguarding operations and maintaining business continuity. Cybersecurity has rapidly moved up the list of concerns, with cyberattacks rising 47% year-on-year in the first quarter of 2025.[1]

The SolarWinds attack in 2020, which saw over 30,000 public and private organisations' data compromised, and the MOVEit hack in 2023, which affected personal and financial data of organisations ranging from the BBC to the US Department of Energy, are just two cases in point.[2,3,4] In April 2025, hackers infiltrated computer systems at Marks & Spencer (M&S), a UK supermarket and retailer, causing an estimated GBP300m (US$405m) in disruption. While the overall cost of cybercrime is hard to determine, the European Commission estimated around EUR5.5trn (US$6.5trn) in 2021.[5] In the US, the FBI reported a 33% year-on-year increase in direct losses, totalling US$16.6bn in 2024, while the UK estimates current annual losses at over GBP27bn (US$35bn).[5]

In procurement, the cyber challenge is made harder by the fact that many leaders fail to carry out regular supplier security assessments. According to a Risk Ledger survey, 36% of firms do not conduct a business impact assessment for suppliers, 33% skip IT assurance checks, and 32% do not issue any supplier security policy.[6]

The Economist Impact survey[7] highlights an intriguing paradox. While aware of the growing cyber threat, procurement teams are neither prioritising cybersecurity nor developing the skills to manage it. However, this may stem less from deprioritisation, than a misalignment between perceived risk and procurement's response. Unclear ownership of cybersecurity risk across the supply chain and a tendency to overlook cyber training accentuate the severity of this discrepancy.

1 Check Point Research. April 16, 2025. "Q1 2025 Global Cyber Attack Report from Check Point Software: An Almost 50% Surge in Cyber Threats Worldwide, with a Rise of 126% in Ransomware Attacks". [https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/] Accessed July 16, 2025.
2 The Guardian. June 16, 2023. "US Energy Department and Other Agencies Hit by Hackers in MOVEit Breach". [https://www.theguardian.com/technology/2023/jun/16/moveit-transfer-hack-department-of-energy] Accessed July 16, 2025.
3 TechTarget. November 03, 2023. "SolarWinds Hack Explained: Everything You Need to Know". [https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know] Accessed July 16, 2025.
4 BBC News. June 05, 2023. "MOVEit Hack: BBC, BA and Boots Among Cyber Attack Victims". [https://www.bbc.com/news/technology-65814104] Accessed July 16, 2025.
5 The Economist. May 29, 2025. "The Uber of the Underworld". [https://www.economist.com/international/2025/05/29/the-uber-of-the-underworld] Accessed July 16, 2025.
6 Risk Ledger. April 18, 2023. "Cyber Security Supply Chain Insights 2023". [https://riskledger.com/resources/cyber-security-supply-chain-insights-2023] Accessed July 16, 2025.
7 Economist Impact. February 2025. "Economist Impact survey of C-suite executives on procurement 2025". Accessed July 16, 2025.

High stakes, low priority

The majority of procurement leaders in our survey (65%) rank cybersecurity and emerging technology risks as having the most critical impact on their organisations. However, cybersecurity ranked far lower in the list of priorities for organisational risk over the short and medium terms (Figure 1). Instead, geopolitical dynamics were the biggest concern over the short term, with sustainability/ESG considerations the long-term priority.

Legacy key performance indicators (KPIs) that favour cost savings, efficiency and compliance over long-term resilience can mean cyber threats are sidelined, particularly in circumstances where procurement is involved after strategic decisions regarding technology have already been made.[8,9,10] Cited by 49% of respondents in 2024 and 27% in 2025, cost savings still feature among the top five organisational risks.[11]

At the same time, 54% of surveyed procurement leaders are somewhat confident and 28% are highly confident in their teams' ability to deal with AI-associated risks, including data privacy and cyber threats. However, this may reflect misplaced optimism, driven by limited incident history, improved IT protocols and increasingly robust cybersecurity frameworks.

While these factors represent reasons for optimism, an organisation's cyber resilience strategy is highly dependent on the ability of departments to collaborate, share and exchange critical information. That, in turn, demands targeted skills, which are often a neglected area of development.

Talent blind spots

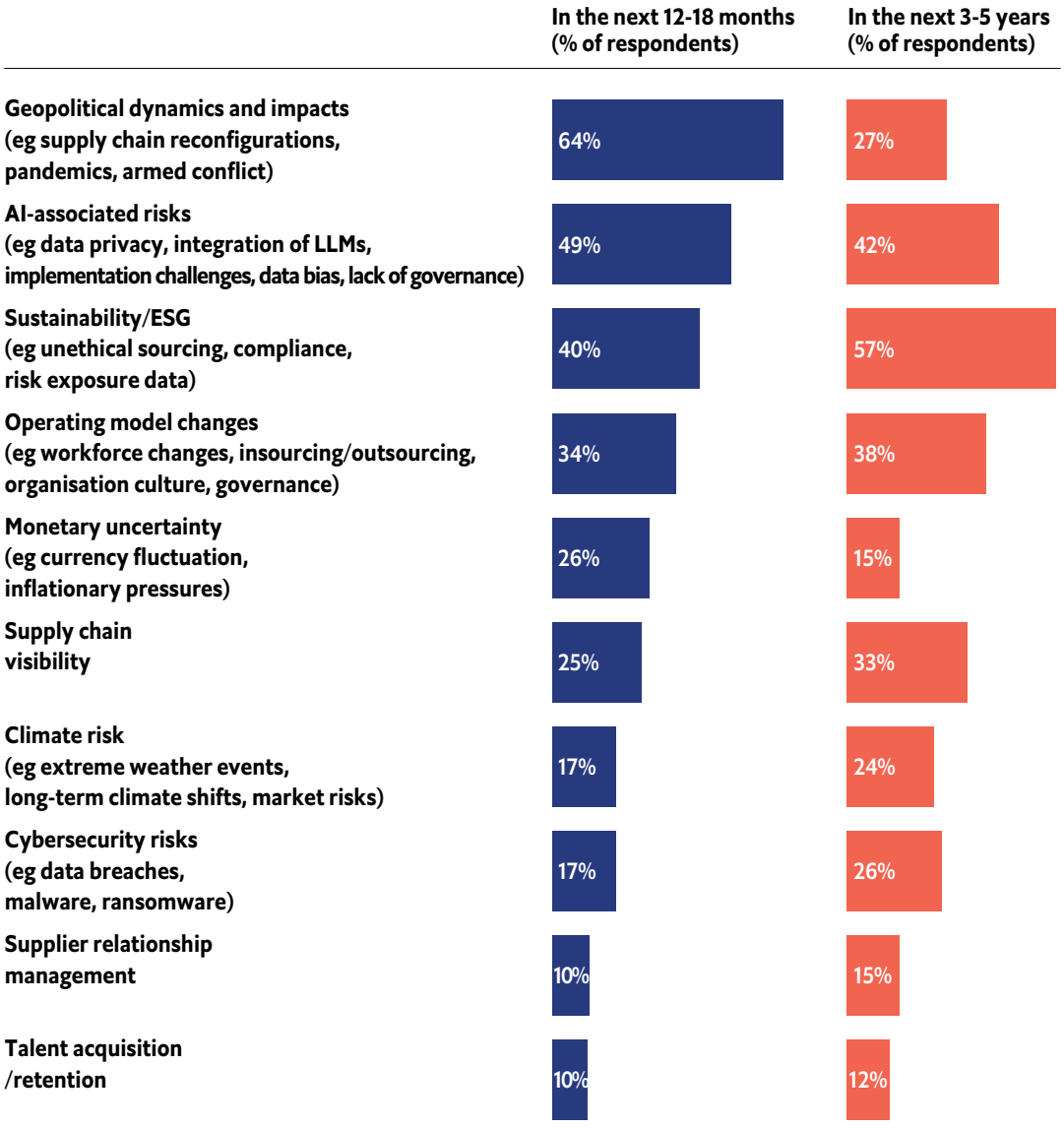
Only 18% of business leaders cite cyber skills as a priority for the next 12-18 months, with that number growing to just 22% over a 3-5 year horizon.[12]

Instead, according to David Loseby, Professor, Leeds University Business School and Editor-in-Chief, Journal of Public Procurement, Emerald Publishing Group, more traditional procurement capabilities are preferred over efforts to nurture T-shaped skill sets, where procurement professionals amass deep cyber expertise alongside more general domain-agnostic proficiencies.

Part of the reason for this inertia is a lack of understanding when applying cyber skill sets to a procurement context. Use of cyber maturity assessments, data protection clauses, risk-based tier analysis, risk questionnaires and supply chain mapping are just some of the tools at procurement teams' disposal, but many are failing to deploy them effectively.[13,14,15]

8 Computer Fraud & Security. December 2023. "Procurement's vital role in mitigating cyber security risks". [https://computerfraudsecurity.com/index.php/journal/issue/view/71/71] Accessed July 16, 2025.
9 Spend Matters. March 31, 2022. "It's Time to Change the Culture of Procurement – Part 1". [https://spendmatters.com/2022/03/31/its-time-to-change-the-culture-of-procurement-part-1/] Accessed July 16, 2025.
10 Proqsmart. February 26, 2025. "Procurement KPIs That Matter: Measuring Success Beyond Cost Savings". [https://proqsmart.com/blog/procurement-kpis-that-matter-measuring-success-beyond-cost-savings/] Accessed July 16, 2025.
11 Economist Impact. February 2025. "Economist Impact survey of C-suite executives on procurement 2025". Accessed July 16, 2025.
12 Economist Impact. February 2025. "Economist Impact survey of C-suite executives on procurement 2025". Accessed July 16, 2025.
13 American Express. n.d. "Supply Chain Mapping – Definition, Importance, and Benefits". [https://www.americanexpress.com/en-us/business/trends-and-insights/articles/supply-chain-mapping-definition-importance-and-benefits/] Accessed July 16, 2025.
14 Optiv. February 18, 2021. "Cybersecurity Risk Assessment Tiering". [https://www.optiv.com/insights/discover/blog/cybersecurity-risk-assessment-tiering] Accessed July 16, 2025.
15 SentinelOne. April 01, 2025. "Cyber Maturity Assessment: Definition and Best Practices". [https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-maturity-assessment/] Accessed July 16, 2025.

Figure 1: Top priorities for organisational risk to focus on for the procurement function



Source: Economist Impact 2025 survey of C-suite executives on procurement

Moreover, cybersecurity has long been regarded as an IT responsibility, suggesting that procurement perceives threats to be episodic rather than systemic in nature.[16,17]

This adds to a growing sense that procurement functions are failing to understand why cyber skills are needed throughout their organisation, not just among those in IT roles.

16 World Economic Forum. January 18, 2023. "Global Cybersecurity Outlook 2023". [https://www.weforum.org/publications/global-cybersecurity-outlook-2023/] Accessed July 16, 2025.
17 ProcureAbility. n.d. "Bold Procurement Prediction #4: Hyper Cybersecurity". [https://procureability.com/bold-procurement-prediction-4-hyper-cybersecurity/] Accessed July 16, 2025.

A neglected enabler of cyber resilience

Change management, a key enabler of a successful cyber risk adaptation strategy, remains widely neglected. Only 10% of survey respondents identify it as a training priority in the short term, falling to 7% over the long term. The reasons are familiar, with procurement teams often viewing change management as a finite project-based process, rather than a permanent and continuous organisational capability.

The evolving regulatory landscape underscores the need for strong change management, given that many procurement teams struggle to embed compliance across complex global supply chains. Part of the challenge lies in poor communication from leadership, which often leaves procurement unclear on its role in driving change.[18,19]

As a result, change is too often seen as a purely technological process, rather than one that also demands shifts in skills, behaviours and culture. A preference for immediate KPIs and visible return on investment can also sideline these softer, strategic competencies.

Bridging the gap

To confront the new cyber reality, procurement must move beyond its traditional cost- and target-oriented mode of operation. Embedding cyber resilience into procurement's core mandate should be regarded as a foundational competency and business continuity imperative. Placing cyber preparedness, monitoring and mitigation at the heart of third-party risk management frameworks is a matter of strategic importance. It will require diligent planning, investment and the cultivation of cyber skills at all levels of the procurement function. Only then can procurement fulfil its strategic role in safeguarding business operations while delivering value, resilience and innovation.

18 Una. February 02, 2023. "Change Management in Procurement". [https://una.com/resources/article/change-management-in-procurement/] Accessed July 16, 2025.
19 DeskAlerts. April 25, 2025. "Why Change Management Fails Without Communication – And How to Fix It". [https://www.alert-software.com/blog/change-management-fails-without-communication] Accessed July 16, 2025.