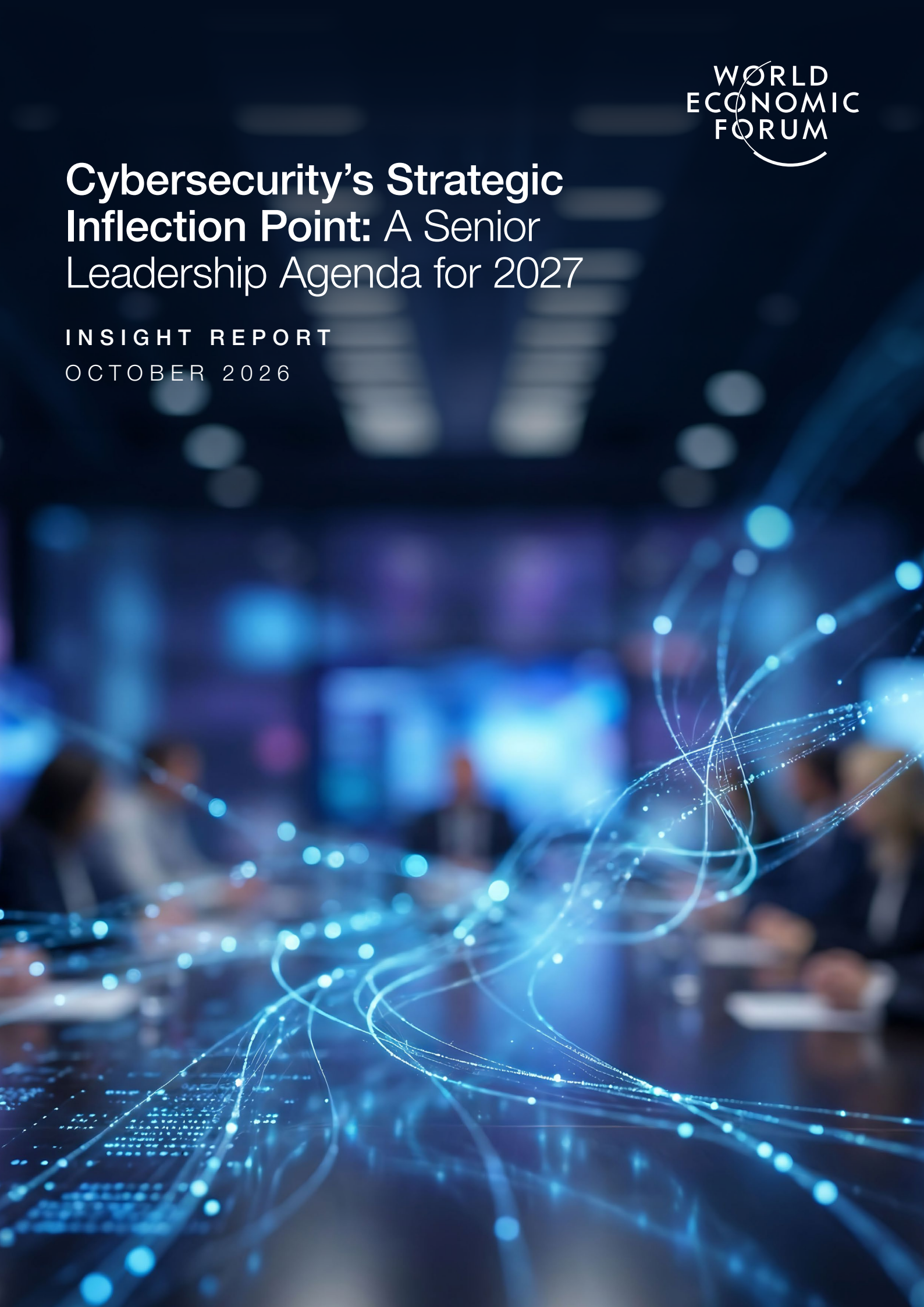
WORLD ECONOMIC FORUM

Cybersecurity's Strategic Inflection Point: A Senior Leadership Agenda for 2027

INSIGHT REPORT

OCTOBER 2026



Images: Adobe Stock

Contents

Preface		3
Executive summary		4
Introduction: Governing cybersecurity as an economic risk		5
Pillar 1	Building a common language for cybersecurity	7
Pillar 2	From cost centre to business value enabler	10
Pillar 3	Cybersecurity as an economic stabilizer	13
Pillar 4	Financing digital resilience	17
Pillar 5	A call to action for senior leaders	19
Appendix: Methodology		22
Contributors		23
Endnotes		25

Disclaimer

This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Generative AI tools were used to support aspects of drafting after analysis was completed. All outputs were independently reviewed, verified and approved by the authors.

© 2026 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Preface

The World Economic Forum's Global Future Council on Cybersecurity brings together leading thinkers from business, government, academia and civil society to examine how cyber risk is reshaping the global economy.[1] The Council translates that understanding into direction for the boards, governments and capital allocators responsible for responding to it.

Over the 2025–2026 term, its 20 members from around the world have focused on a growing mismatch: cybersecurity increasingly determines whether economies and institutions can continue to function, yet too often it is still governed primarily as a technical function. Drawing on their discussions and individual expertise, Council members have explored how this gap can be addressed. The analysis and recommendations in this report reflect their collective insights as subject-matter experts.

The stakes are increasingly clear. Cyber posture affects whether payments clear, factories operate, public services remain available and citizens trust the institutions that serve them. Yet governance has not kept pace with this dependence: cybersecurity is still frequently budgeted, governed and debated as a cost to be contained rather than an investment in resilience and value; boards lack a common vocabulary for making decisions about it; supervisors lack consistent metrics for comparing resilience across firms and jurisdictions; capital does not flow towards digital resilience in the way it does towards physical infrastructure; and there is no standing senior political constituency with clear ownership of the agenda.

The Council organized its work around five workstreams, each addressing a different dimension of this gap:

- **A common language for cybersecurity** asks whether boards, executives, regulators and practitioners share the vocabulary needed to make decisions together, drawing on the Survey on Cyber Language and Executive Decision-Making conducted in April 2026.
- **Cyber as a value-creating opportunity** draws on organizational cases to identify the mechanisms through which cybersecurity investment can produce measurable business value.
- **Cyber as a global stabilizer** examines how cyber incidents can create macroeconomic disruption and proposes an approach for tracking that exposure across countries and sectors.
- **A global sustainable finance mechanism for cyber** addresses the financing gap facing organizations that are both highly exposed to cyber risk and under-represented in the discussions where rules and priorities are set.
- **A call to action for senior leaders** translates the Council's analysis into proposals directed at institutions that already exist and have the capacity to act.

Taken together, these workstreams point to a common conclusion: the next step is not to build new institutions, but to mobilize the leaders and institutions already positioned to respond. That is the task for 2027, and it begins now.

Executive summary

Cybersecurity is now an economic imperative, requiring leaders to rethink how it is governed, measured, valued and financed.

Cybersecurity has become a condition of economic resilience. Digital systems now underpin payments, production, public services, supply chains and, increasingly, the infrastructure on which economic growth depends. When those systems fail, the consequences extend beyond individual organizations. Disruption can and has spread across sectors and borders, interrupting essential services, weakening public trust and, in severe cases, affecting national economic performance.

Recognition, however, has not yet translated into how institutions make decisions. The Survey on Cyber Language and Executive Decision-Making conducted in April 2026, found that while 42% of respondents recognized cybersecurity's measurable effects on economic output, markets and supply chains, only 9% said their institutions view it as an economic stabilizer. Investment patterns reveal a similar gap: more than half reported that cyber investment is driven primarily by crisis events, while only 8% cited demonstrated returns as a trigger for investment. The challenge is therefore increasingly one of conversion – turning an understanding of cyber dependence into the governance, investment and measurement practices needed to manage it.

The Global Future Council on Cybersecurity's work identifies the following areas for making that conversion possible:

1. **Decision-makers need to align on a common language.** Boards, governments, investors and technical leaders need to translate cyber risk into outcomes they already govern: resilience, continuity, trust, economic risk and stability. This is particularly important during crises, when unclear translation between technical and executive teams can delay decisions and weaken response.

2. **Cybersecurity should be understood as productive capital, not only as protection against loss.** Evidence gathered by the Council shows how cyber investment can create measurable value by reducing financial and operational exposure, strengthening trust across business ecosystems, enabling digital transformation and improving governance and organizational culture. Cyber capability should therefore inform strategic planning and capital allocation alongside other inputs to enterprise value.

3. **Cyber resilience needs measures that can travel across institutions and economies.** Six measures – service continuity, recovery credibility, dependency concentration, tail-loss exposure, value preserved and the effect of cyber posture on the cost of capital – would give boards, supervisors, finance ministries, insurers and investors a more comparable basis for assessing resilience and pricing cyber posture into economic decisions.

4. **Greater attention must be paid to financing resilience where vulnerability is greatest.** Under-resourced economies and organizations often face high level of risk exposure with limited capacity to absorb cyber shocks. The Council argues that a sustainable cybersecurity finance mechanism could align philanthropy, corporate giving, development finance and pooled funding around long-term investment in foundational cyber capability.

The priority for 2027 is to turn recognition into action. Senior leaders have the opportunity to embed cyber resilience more firmly in the decisions that shape economic performance – from how organizations allocate capital and pursue digital transformation to how governments assess stability and how institutions direct investment. Progress will depend on coordinated leadership across the public and private sectors, using existing institutions and decision-making levers to strengthen resilience across the digital economy.

Introduction: Governing cybersecurity as an economic risk

Cybersecurity has become essential to economic resilience, but the way institutions govern, measure and invest in it has not kept pace.



> Cyber incidents have become an important source of operational and economic disruption.

Modern economies are increasingly dependent on the digital systems that connect businesses, infrastructure, public services and financial markets. As that dependence has grown, cyber incidents have become an important source of operational and economic disruption. A ransomware attack can halt production at a major manufacturer for weeks, while a faulty software update can disrupt commercial aviation across multiple countries. Yet cybersecurity continues to be governed in many institutions primarily as a technical or compliance matter rather than as an issue of organizational and economic resilience. The gap between this growing dependence and the way cybersecurity is understood and governed by boards, governments and capital allocators is the central concern of this report.

Recent cyberattacks have underscored how deeply cybersecurity is intertwined with the broader economic landscape, inflicting tangible financial damage on businesses and national economies alike.[2] According to United Kingdom government research, the average significant cyberattack costs businesses nearly £195,000 ($250,000). Scaled nationally, this equates to an estimated £14.7 billion ($19.4 billion) in annual economic losses.[3] This is the operating reality the International Monetary Fund (IMF) had already warned about: that major cyber incidents are now capable of transmitting acute stress to the wider financial system through service disruption, confidence shocks and cross-firm contagion and that extreme cyber losses are now several multiples of their 2017 levels.[4]

The Survey on Cyber Language and Executive Decision-Making conducted by the Global Future Council on Cybersecurity in April 2026 highlights the persistence of these gaps. More than 60% of respondents reported communication breakdowns during high-stress cyber incidents (see Appendix: Methodology for additional details). While 42% recognized that cybersecurity has measurable effects on economic output, markets and supply chains, only 9% said their institutions view it as an economic stabilizer. More than half reported that cyber investment is driven primarily by crisis events rather than strategic considerations, while only 8% cited demonstrated returns as a trigger for investment. The responses, gathered from senior business leaders across leading global and regional institutions, point to a continuing disconnect between the recognized economic significance of cybersecurity and the extent to which it is treated as a strategic investment at the highest levels of organizational decision-making.

The response to these challenges does not necessarily require new institutions; it requires making more deliberate use of those that already shape economic policy, financial stability and investment: finance ministries, central banks, prudential supervisors, infrastructure investors, multilateral lenders and the political forums that convene their leaders.

Against this backdrop, the Global Future Council on Cybersecurity organized its work around five interconnected areas:

1. Proposing a framework for shared vocabulary for decision-makers
2. Framing cybersecurity as a value-creating strategic capability
3. Developing a measurement architecture for global digital stability
4. Designing sustainable financing mechanisms for under-resourced environments
5. Providing a strategic call to action for 2027

This report sets out the findings of each workstream and concludes with five concrete asks for 2027.

Pillar 1

Building a common language for cybersecurity

A shared cybersecurity vocabulary enables leaders to translate technical risk into clearer decisions on resilience, investment and crisis response.



Cybersecurity has long been treated as a technical discipline and described in technical terms. As cyber risk has become a strategic and economic concern, however, the language used to discuss it has not evolved. This section sets out what a common language for cybersecurity would need to do: who it must serve, which decisions it must support and where the current gaps are most costly. The definitional work itself belongs with the standards bodies, regulators and industry groups already engaged in this process.

The governance cost of a vocabulary gap

The vocabulary gap becomes expensive at the point of decision-making. Boards, ministers and investors are increasingly expected to decide how much to invest, when to disclose and how to coordinate across borders without a shared vocabulary to support those decisions. The result is more than a communication challenge, it is a barrier to effective governance.

A senior leader who cannot translate cyber risk into business, operational or economic terms cannot make a confident decision, and that delay has measurable consequences. In the Council's 2026 survey, 75% of respondents identified the gap between technical language and business impact as the dominant source of conflict across cyber frameworks. Nearly two-thirds deliberately avoid technical language in senior discussions, and one in five avoids using the word "cybersecurity" when speaking with peers and executives. These show not only a preference for simpler conversation but also indicate that translation is already happening informally, ahead of decisions on investment, regulation and incident response.

The Council's survey suggests that gaps in shared cyber terminology become particularly consequential under pressure: 62% of respondents reported that communication challenges had delayed or weakened their organization's response during cyber incidents, with more than a third specifically identifying language gaps during high-stress situations. One respondent from a critical infrastructure organization described an incident in which multiple attempts to brief the chief information officer (CIO) using technical terminology failed to convey the situation clearly, requiring the team to reframe the explanation in business terms.

The broader challenge is one of translation between different decision-making contexts. Technical teams may focus on containment and remediation, while executive leaders need to understand the implications for business continuity, legal exposure and reputation. Without a shared vocabulary, that translation can slow escalation, complicate coordination and delay communication with regulators, partners and the public. What appears to be a communication problem can therefore become a governance and operational issue.

The vocabulary for decision-makers

The foundations of a shared vocabulary already exist. In the Council's survey, senior leaders gravitated towards a small set of outcome-oriented terms: "resilience", used by 77% of respondents; "continuity" (61%); "trust" (55%); "economic risk" (37%); and "stability" (33%). These terms connect cybersecurity to outcomes that boards, governments and investors already consider in other areas of decision-making, providing a more accessible basis for discussions of cyber risk and resilience.

Framework names, architectural acronyms and defence-specific terminology did not feature in the same way. Such terminology remains essential at the operational level, where technical precision matters. At the governance level, however, it needs to be translated into language that enables leaders to understand consequences, assess trade-offs and make decisions.

The Council's aim therefore is not to create an entirely new vocabulary but to build greater consistency around terms already used across institutions and sectors. Technical concepts should translate into a common governance language without losing their underlying meaning. A senior leader encountering "resilience" in a risk committee briefing and "cyber resilience" in a security report, for example, should be working from a shared understanding of what resilience means, rather than reconciling definitions developed in separate institutional silos.

The terms that most urgently need clarity

Two areas of terminology emerged from the survey as priorities for greater clarity. The first is the distinction between **cyber risk** and **cyber resilience**, identified by 62% of respondents as a source of misunderstanding at the senior level. Cyber risk describes the potential for loss or disruption arising from cyber threats and vulnerabilities; cyber resilience describes an organization's capacity to anticipate, withstand, adapt to and recover from cyber disruption. The concepts are closely related, but they are not interchangeable.[5]

62%

of respondents reported that communication challenges had delayed or weakened their organization's response during cyber incidents.



> Treating risk management and resilience as equivalent can leave important gaps in preparedness, investment and accountability.

This distinction matters for decision-making. An organization may have robust processes for identifying and managing cyber risk without having sufficient capacity to maintain or restore critical functions when disruption occurs. Treating risk management and resilience as equivalent can therefore leave important gaps in preparedness, investment and accountability. A clearer distinction, grounded in established frameworks but expressed in language accessible to senior decision-makers, would provide a stronger basis for governance and investment decisions.

The second area is the definition of **critical infrastructure**, identified by 34% of respondents as a source of inconsistency across regulatory frameworks. Definitions of criticality vary across jurisdictions, sectors and legal regimes, meaning that the same or similar digital assets may be treated differently depending on the framework applied. These differences can complicate cross-border coordination, regulatory alignment and decisions about where resilience investment should be prioritized.

A second complication is the unit of analysis. Critical infrastructure is usually discussed in terms of organizations, but the fundamental unit is a function or service. Even within an organization formally designated as critical infrastructure, only some functions are genuinely critical; others could be lost for an extended period with limited consequences. Designating whole entities therefore both over-includes and under-includes: it extends obligations to activities that do not warrant them, while missing critical dependencies that sit inside organizations no framework designates as critical.

Greater consistency does not require a single global definition. A more practical approach is to establish common criteria for assessing criticality at the level of functions and services, including factors such as economic substitutability, concentration and the time required to restore essential functions. Such criteria could provide a more consistent basis for regulatory coordination and investment decisions while allowing jurisdictions and sectors to account for their different circumstances.

What effective crisis language looks like

The survey also provides insight into the forms of communication senior leaders find most useful once an incident is under way. Respondents highlighted three in particular: quantified economic impact, including costs, sectoral disruption and effects on national output (59%); clear recovery indicators, such as the expected time to restore operations (55%); and human-centred framing that describes consequences for people rather than systems (53%).

The common thread is not more technical detail but greater clarity about consequences. During a crisis, communications to boards, ministers and other senior decision-makers should therefore translate technical developments into information they can act on: the scale of financial and operational exposure, the expected path to recovery and the implications for citizens, customers and partners. Technical precision remains essential, but at the governance level it needs to be accompanied by a clear account of what an incident means and what decisions it requires.

Why language is the foundation

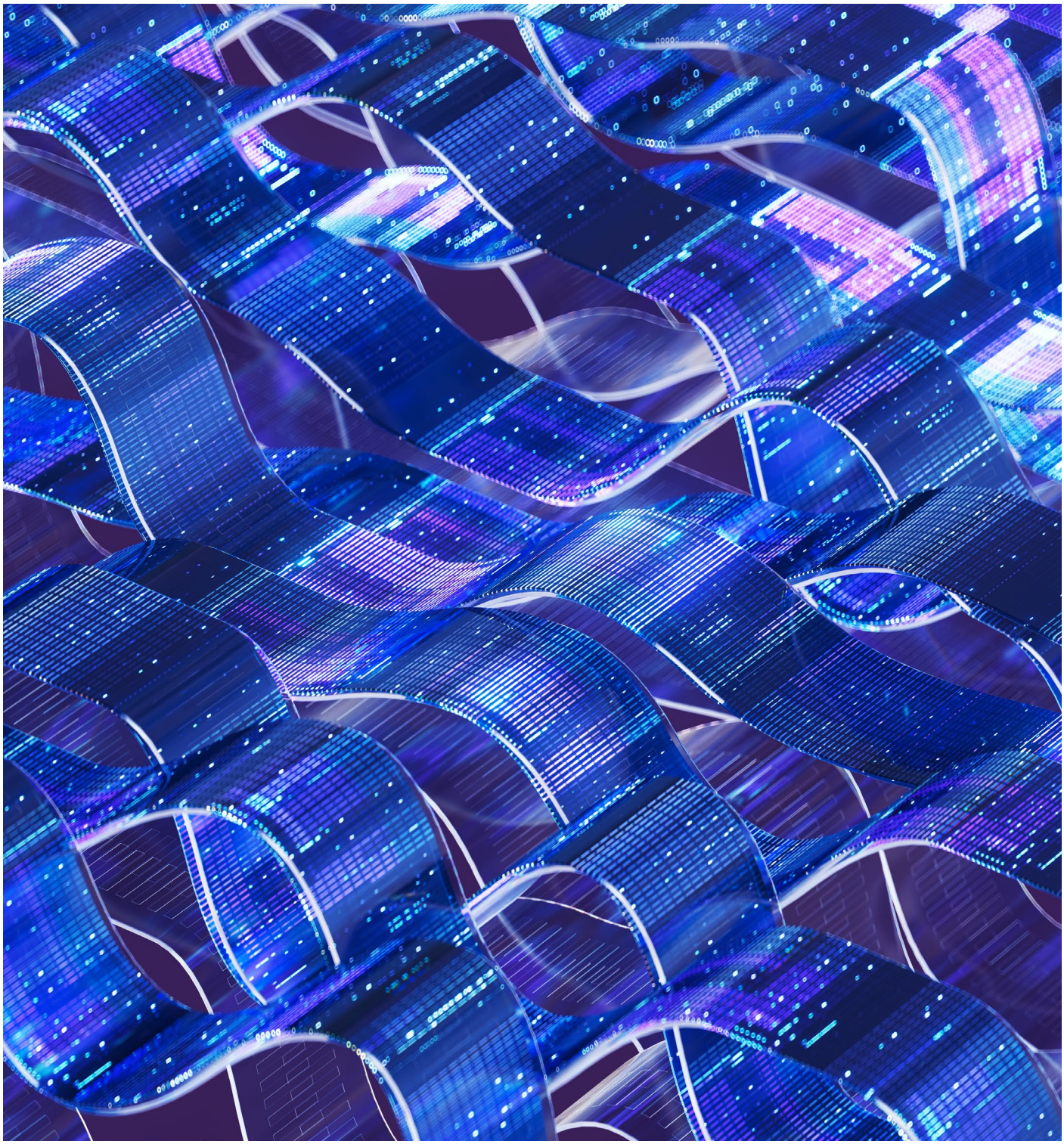
Without a shared vocabulary, efforts to strengthen cyber resilience become more difficult to coordinate and evaluate: valuation models cannot readily compare firms if resilience is understood differently by chief information security officers (CISOs) and chief financial officers (CFOs); stability metrics are difficult to aggregate across economies when definitions of criticality vary significantly across jurisdictions; financing decisions are harder to align when funders and recipients use different measures of resilience and impact; and political commitments can lose clarity as they move across technical, institutional and national contexts.

A common language for cybersecurity is therefore more than a communications tool; it provides part of the foundation for more consistent governance, investment and coordination across institutions and borders.

Pillar 2

From cost centre to business value enabler

Cybersecurity becomes a value enabler when organizations translate security investments into financial, operational and strategic business outcomes.



Cybersecurity as a value enabler: Evidence from the field

The value case for cybersecurity is most often stated defensively: cyber investment protects against loss, reduces downside exposure and reassures markets. That framing is analytically incomplete as cybersecurity is also an input to value creation in its own right. In the Council's survey, 39% of respondents identified clear economic valuation models as the most significant unmet need for positioning cybersecurity as a strategic investment rather than primarily a cost. Boards and CFOs already know where they want those models to point: 67% want metrics tied to revenue and productivity, 58% to financial loss avoided, 50% to downtime reduction and 48% to a risk-adjusted return such as cyber-adjusted return on investment (ROI). The vocabulary of finance is ready, yet it is challenging to find empirical evidence and case studies that may standardize the approach. Recognizing both the imperative and the opportunity to address the economic dimension of cybersecurity, the World Economic Forum launched the Centre for Cyber Economics in collaboration with the Global Cybersecurity Forum to explore the economic dimension of cybersecurity in detail and complement the Council's own workstream in this area.[6]

Reframing cybersecurity from a cost centre to a source of business value is easier to advocate for than to demonstrate. To move beyond anecdotal evidence, the Council collected structured case submissions from organizations that have begun to make this shift, asking each to identify how cybersecurity investment translated into business value. Four distinct mechanisms emerged: create economic value, build ecosystem trust, enable digital transformation and strengthen governance and culture. These are illustrated by the examples below.

The cases suggest that there is no single path to positioning cybersecurity as a value enabler. Some organizations translate cyber risk into financial terms, treating resilience as a measurable economic consideration. Others use their security posture as a business credential, which can accelerate partner onboarding, meet regulatory requirements or enable access to markets and ecosystems. Still others treat cybersecurity as a foundation for digital transformation, enabling initiatives that might otherwise carry greater risk or cost.

While the mechanisms differ, the cases share a common feature: cybersecurity investment is connected explicitly to business outcomes in a language that senior leaders can understand and act on. This connection, supported by sustained senior leadership engagement, helps move cybersecurity beyond a primarily technical or compliance discussion and towards a broader consideration of its contribution to organizational value.

39%

of respondents identified clear economic valuation models as the most significant unmet need for positioning cybersecurity as a strategic investment rather than primarily a cost.

Cybersecurity as an economic value discipline

The clearest pattern in the sample is the shift from compliance spending to a risk-informed model. The case of a state-owned investment holding company in the United Arab Emirates (UAE) is representative of the compliance-triggered version of this shift: a Dubai Electronic Security Center (DESC) directive pushed cybersecurity from an audit-driven checklist into a capital-allocation conversation. As a result, leadership now approves cloud migration and identity investments on ROI and risk-reduction grounds rather than best practice alone. Their clearest metric, a maximum two-hour downtime tolerance for critical system outage, shows how a compliance threshold was repurposed as a business continuity commitment.

Banco do Brasil, a financial institution, illustrates the same discipline at a more structural level. Rising regulatory pressure and the move to remote working driven by the COVID-19 pandemic pushed cybersecurity from IT into enterprise risk management. The distinctive change was organizational: the bank's first line of defence (the business units that own risk day-to-day) and second line (independent risk oversight) jointly defined a shared set of key risk indicators (KRIs), rather than each party tracking cyber risk separately. These KRIs translate cyber exposure into financial-loss and service-disruption terms and are now debated alongside financial and operational risk within senior governance committees. The bank estimates exposure reductions in the order of tens of millions in potential losses per year.

Cyber resilience strengthens ecosystem trust

Cybersecurity creates economic value not only by reducing expected losses but also by reducing uncertainty across business relationships. Organizations that demonstrate continuously monitored readiness, including visibility into critical dependencies, may strengthen customer confidence, preserve contracts, accelerate partner onboarding and improve their position as trusted participants in digital ecosystems.

The case of global energy technology organization Schneider Electric shows how cybersecurity can create value by turning security posture into externally recognized evidence of trustworthiness. Drawing on independent certifications, the company reports faster partner onboarding and fewer duplicative third-party security assessments sustained over the past two to three years. It points to its published transparency reporting as a standardized assurance reference for customers and partners, illustrating how external validation can reduce the cost and time required to demonstrate trust.

> Cyber capability should be reported and evaluated as an enabling input to value creation and not only as a cost or risk category.

Cyber resilience unlocks digital transformation

A third mechanism emerges when cybersecurity enables a transformation that would not otherwise be possible, rather than simply supporting one already under way. The UAE's Ministry of Cabinet Affairs illustrates this in its simplest form. By bringing cybersecurity into planning discussions in the early stages, the entity changed the function's role from technical control to strategic partner, allowing it to move cloud, data and AI-enabled initiatives forward with clearer security conditions set in advance and fewer unresolved risks surfacing late.

SwissPost, a public logistics company in Switzerland, adopts a similar mechanism. Its shift to a zero-trust, identity-centric architecture was the precondition for exiting its own data centres. Without it, the company judged, the business case for moving to the cloud would have been cost-negative; with it, they estimated recurring costs to be roughly CHF 9 million ($11.2 million) lower.

Governance and culture amplify security outcomes

A fourth mechanism runs through all the others: governance and culture as multipliers. Absa Group, a South African-based financial services group, rebuilt its security function after Barclays reduced its shareholding, and the decisive moves were structural. The board created a dedicated IT subcommittee for cyber risk and restructured the CISO's reporting line into a dual model spanning the Group CIO and the Group chief risk officer (CRO), preventing cyber risk from being deprioritized when technology delivery and risk management compete. Culture was measured rather than asserted: with board and executive backing, simulated phishing click rates fell from roughly 24% to below 10%, while suspicious-email reporting rose from around 1% to above its 20% target.

An anonymous Israeli bank reached similar conclusions under Bank of Israel Directive 364, which reinforced senior-management and board accountability. It refined cyber-related key performance indicators (KPIs) for executives, integrated cyber and technology risk into enterprise risk management and built a network of cybersecurity champions that grew from zero to 40 between 2022 and 2026 to embed secure-by-design practices. Both cases make the same point: technology alone did not move the numbers; governance and shared accountability did.

Four distinct value-creation mechanisms hold up under scrutiny: cybersecurity as a quantified economic discipline embedded in enterprise risk management; as a trust credential that reduces friction within a value chain; as the enabling precondition for digital transformation; and as a governance and culture discipline that multiplies the ROI. For boards and investors evaluating cyber as a category of productive capital, the lesson is less about which single metric to adopt than about ensuring some translation discipline exists at all. Cyber capability should therefore be reported and evaluated as an enabling input to value creation and not only as a cost or risk category, and should be included in strategic planning, capital allocation and mergers and acquisitions (M&A) due diligence as a factor of production alongside human capital and physical infrastructure.

TABLE 1 **Recommendations to peers**

Sector grouping	Condensed recommendation to peer organizations
Financial services and banking	Treat cyber and technology risk as a business risk not a technical function. Translate cyber exposure into financial, operational and service-continuity terms through a small set of executive-level KRIs. Ensure the CISO has sufficient independence, direct access to senior governance and the authority to escalate uncomfortable trade-offs. Make minimum security and resilience controls mandatory validation prior to release for new technologies, third parties and architectures.
Public-sector and government digital transformation	Bring cybersecurity into digital transformation at the beginning and not at the approval stage. Use cybersecurity to define safe adoption conditions early for cloud, AI, data sharing, third parties and sensitive information, so that security becomes a strategic partner in delivery rather than a late-stage blocker.
Digital infrastructure, telecommunications and platforms	Engineer security into platforms and infrastructure as a product capability, not as a bolt-on risk function. As cloud, AI and networked services expand the attack surface, organizations that remove the trade-off between innovation and risk can use secure-by-design platforms to increase trust, adoption and growth.
Industrial, energy and critical infrastructure ecosystems	Treat cyber resilience as a strategic trust credential for participation in critical ecosystems. Invest in interoperability, transparency, external assurance and structured evidence of readiness to reduce due-diligence friction, build credibility with partners, customers and regulators, and strengthen resilience across the wider value chain.

Pillar 3

Cybersecurity as an economic stabilizer

Cyber incidents now transmit disruption into the wider economy; such exposure can be measured, compared and priced.



> Cyber resilience is no longer only a question of preventing losses within individual organizations; it is becoming integral to how economies preserve continuity.

Digital systems now carry the routine operating load of the economy: the clearing of payments, the administration of public services, the running of production lines and the records on which citizens' entitlements depend. Where those services have no offline substitute, continuity is no longer only a private operational concern; it becomes a condition of economic stability.

That reframing matters because cyber resilience is no longer only a question of preventing losses within individual organizations; it is becoming integral to how economies preserve continuity, investor confidence and public trust when digital infrastructure fails.

The scale of that dependence is measurable. The digital economy is estimated to account for roughly a quarter of global gross domestic product (GDP)[7] and is expected to generate more than two-thirds of new value creation over the next decade.[8] Severe cyber incidents can therefore become macroeconomic events: modelled effects on national output range from 0.2% to 2% of GDP in the year of the event, and econometric analysis has found a persistent drag on total factor productivity across high-income economies.[9] Cyber posture is a determinant of economic performance rather than a subsidiary risk category.

How cyber disruption reaches the economy

Cyber incidents reach the wider economy through four channels: financial systems; the real economy and supply chains; government services; and trust in information and institutions.

The first is financial systems. Disruption to payment, settlement and market infrastructure is amplified by shared dependencies: when many institutions rely on the same cloud provider or clearing house, a single failure becomes a source of correlated stress across a sector. The February 2024 ransomware attack on Change Healthcare caused widespread disruption across the US healthcare system and resulted in approximately $3.1 billion in costs and business disruption impacts for its parent company, UnitedHealth Group, over the course of 2024.[10]

The second is the real economy and supply chains, where disruption moves through logistics, industrial control systems and manufacturing. This was seen in 2024 when a faulty update to CrowdStrike's cloud-based security software resulted in a global IT outage, affecting businesses and governments around the world.[11]

The third is government services: the identity, welfare, tax and customs systems for which there is rarely an alternative provider. Disruption to these systems can delay entitlements, interrupt revenue collection and slow cross-border trade.

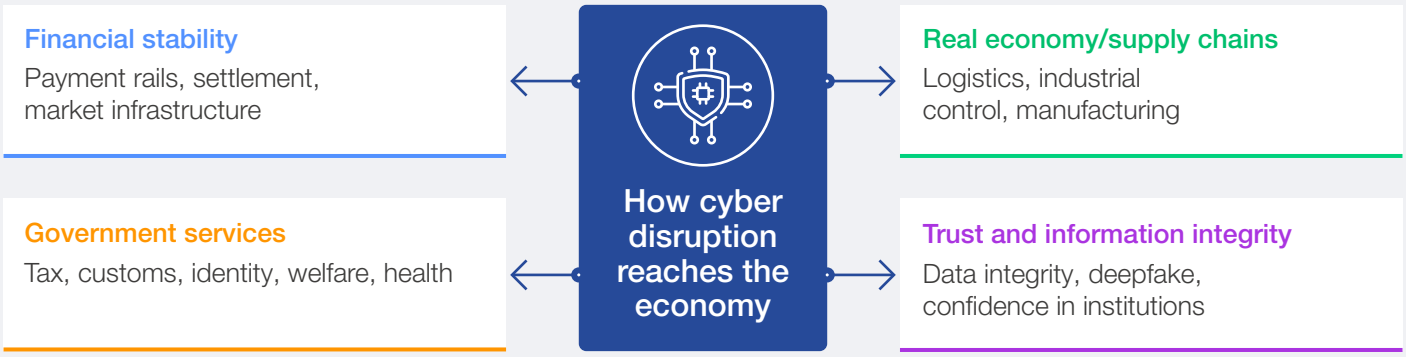
The fourth is trust and information integrity, where compromises to data and to public information systems reduce confidence in institutions and accelerate risk aversion, most sharply in fragile governance environments.

Senior leaders identify the same four channels. In the Council's survey, 61% selected supplier and third-party disruption as a primary route through which incidents spread, 59% selected public trust and societal stability, 54% selected internal operational disruption and 46% selected sector-wide disruption. The prominence of third-party disruption carries a governance implication: critical dependencies, including non-technology suppliers and shared service providers, require monitoring and credible substitution arrangements, not acknowledgement alone.

FIGURE 1 **The four channels through which cyber incidents transmit disruption into the wider economy**

Four transmission channels: How cyber shocks propagate into macroeconomic disturbance

Each channel is independently observable and anchored to a verified incident of micro-scale impact



Source: World Economic Forum

What economic decision-makers need to measure

Understanding how disruption travels is not the same as being able to price it. Boards, supervisors, finance ministries and insurers work largely from measures built for technical audiences, which are difficult to aggregate across institutions and to compare across jurisdictions. Six questions would address much of that gap (see Table 2).

TABLE 2 **A set of measures expressed in terms already used by decision-makers**

What to measure	The question it answers	Who needs the answer
Service continuity	✓ Do essential digital services remain available under stress?	Boards, prudential supervisors
Recovery credibility	✓ How wide is the gap between planned recovery and proven recovery?	Boards, regulators
Dependency concentration	✓ How many critical functions rest on the same providers?	Supervisors, finance ministries
Tail-loss exposure	✓ What would a severe incident cost over a defined horizon?	Insurers, chief financial officers
Value preserved	✓ What economic value has resilience investment protected?	Boards, finance ministries, investors
Cost-of-capital effect	✓ How does cyber posture affect financing, insurance and market access?	Investors, ratings agencies, ministries of finance



> In frontier and developing markets a cyber incident can escalate into a national emergency.

This is close to what senior leaders ask for. Measurement that captures only damage avoided understates the case for investment because it records what did not happen and omits what was created. Measurement that also captures value preserved and value enabled – reduced cost of capital, expanded market access, credit-rating uplift and lower insurance cost – allows cyber capability to be appraised as productive capital. This is where this pillar and the value mechanisms in Pillar 2 converge.

Comparing resilience across countries and sectors

Measures that cannot be compared cannot support policy. The Council proposes a benchmark scoring cyber capacity across countries and sectors on four dimensions:

- Concentration of critical dependencies
- Preparedness capacity
- Demonstrated ability to sustain and recover essential services
- Assurance of data integrity and transparency; two design choices distinguish it from existing indices

It scores sectors alongside countries, because national aggregates conceal concentration within a single sector or provider, and it weights demonstrated recovery above declared resilience, on the principle that a capability which has not been exercised has not been established. A pilot across two sectors and five countries would establish whether the scoring travels.

Supervisory measurement already works at national scale

The Bank of England's CBEST framework, launched in 2014, subjects systemically important UK financial institutions to intelligence-led testing calibrated to real threat actor tactics. Results feed the Prudential Regulation Authority's supervisory assessment and shape sector-wide practice.[12] CBEST moved cyber posture from a self-declared attribute to a supervised prudential category using existing mandates, threat intelligence and accredited providers. The benchmark proposed here applies the same logic at country and sector level: measurement integrated into supervisory practice rather than layered on top of it.

Why the same incident costs more in developing economies

Cyber shocks do not distribute evenly. In frontier and developing markets, an incident that an advanced economy with parallel processing capacity could absorb within hours can escalate into a national emergency. The causes are structural: dependence often concentrates on a single national payment switch, identity system or telecommunications provider; offline fallbacks are thinner; insurance penetration is below 10%; and recovery doctrine is less established. Costa Rica's 2022 ransomware campaign illustrates the risk: it produced a declared national emergency and roughly two months of disruption to tax and customs functions.[13]

Preparedness financing in these markets is therefore not solely a development question; it reduces fragility in a system where exposure is shared across borders. Where benchmarking identifies a specific deficiency, it also identifies what financing should address. That is the subject of Pillar 4.

What this pillar asks of the institutions that already assess economic risk – finance ministries, prudential supervisors, ratings agencies and reinsurers – is narrower than a new mandate. It asks for cyber resilience to be measured in a form that can be compared across borders and priced into judgements those institutions already make. Pillars 4 and 5 set out how that capacity is financed and who is asked to adopt it.

Pillar 4

Financing digital resilience

The interconnected nature of the digital ecosystem means that it will never be secure if many people and organizations cannot afford basic cybersecurity.



> The economies and organizations that face the greatest cyber risk relative to their capacity to absorb it are the least protected.

If everyone used a common language, recognized cybersecurity's value-creating opportunity and measured cybersecurity well, the digital economy would still have a security problem. Even with the standards, policy frameworks and technical know-how to secure the digital economy in place, what is missing is financial resources. Many organizations do not have the resources to access existing cybersecurity capabilities and, when they do, these resources do not flow to where exposure is greatest. The Council's review of 28 existing funds suggests private and corporate philanthropy together contribute in the order of $100–200 million a year to cybersecurity-specific causes. Government grant programmes, such as the State and Local Cybersecurity Grant Program in the United States, the Integrated Security Fund in the United Kingdom and the European Union's Digital Europe Programme, have begun adding millions in their own jurisdictions, but little funding reaches emerging economies, least-developed countries or civil society. Against the $885 billion given to charitable causes in 2023[14] or the $580 billion that flowed into corporate AI investment in 2025, cyber philanthropy is a rounding error.[15] The AI engine is being scaled without funding the guardrails.

The economies and organizations that face the greatest cyber risk relative to their capacity to absorb it are the least protected, most exposed and least present in the governance discussions where the rules are set. Yet a small fraction of existing giving, directed deliberately, would be enough to change that. That's why the Global Future Council on Cybersecurity recommends creating a Sustainable Cybersecurity Finance Mechanism (SCFM) structure. The SCFM would not operate as a single fund but rather as a coordinated ecosystem of individual philanthropy, corporate giving, multilateral funds and pooled mechanisms aligned under shared principles. A coordinated base of this kind provides the stability needed to unlock further resources and to fund under-resourced but critical internet functions. To maximize impact, the mechanism would bound its scope using five parameters:

- Cybersecurity as the primary objective
- Acceptance of the overlap with disinformation
- Civil resilience and victim-centred capacity-building rather than military or defence applications
- Foundational capability ahead of compliance in digitally nascent regions
- Global equity, political neutrality and differentiated contributions throughout

Design principles: The SCFM's purpose is not just to get more resources to beneficiaries but also to ensure that those resources improve security. The SCFM should adhere to three principles to achieve this goal. The mechanism should fund broad capabilities and core infrastructure rather than narrow programme silos: it should favour predictable, long-term allocations over large, volatile, one-time grants, and it should legitimize mixed funding models, including cost recovery from capable users such as law-enforcement agencies while subsidizing those who cannot pay.

Economic viability: Government resources are not allocated to problems policy-makers do not understand, capital does not flow to problems it cannot price and treating cybersecurity for under-resourced organizations and economies purely as a "charitable cause" will keep funding limited, donor-dependent, fragmented and hostage to political cycles. The adoption of a common language, the shift to treating cybersecurity as a source of value and rigorous measurement would provide the foundation for getting more resources for cybersecurity. The SCFM should build on that foundation and:

- Adopt rigorous avoided-loss modelling
- Develop credible risk-adjusted return estimates
- Standardize resilience accounting that makes digital health visible on balance sheets
- Embed outcome measurement on the part of recipients as a routine requirement
- Reclassify cybersecurity from "military/defence" to "civil resilience" in Organisation for Economic Co-operation and Development (OECD), development-finance and pension-fund categorization systems, a misclassification that currently locks significant pools of capital out of the sector

The interconnected nature of the digital ecosystem means that it will never be secure if many people and organizations cannot afford basic cybersecurity. A sustainable, transparent and impactful financing mechanism is the baseline requirement for securing the technical infrastructure of the global economy and protecting the organizations and people least able to protect themselves.[16] Realizing the full upside of AI and emerging technology depends on it.

Pillar 5

A call to action for senior leaders

The agenda for 2027 is to set cybersecurity as a core condition of economic resilience.



> Senior leaders must govern cyber resilience as economic resilience.

Cybersecurity has reached the point where senior leaders can no longer treat it as a specialist concern delegated to technical teams. The digital layer now carries the continuity of firms, markets, governments and communities. When it fails, the consequences are not confined to networks: they appear as halted production, delayed or disrupted public services, disrupted payments, supply-chain fragility, reduced trust and, in the most exposed economies, national instability. The analysis in the previous four pillars points to one obligation: senior leaders must govern cyber resilience as economic resilience. The question is no longer whether cybersecurity matters, but rather who will act on that obligation through the institutions and governance levers they already control.

The first four pillars establish the conditions for action. This fifth pillar, in its turn, asks boards, governments, investors and financial-stability institutions to turn those conditions into an operating agenda. By 2027, senior leaders should commit to the following five moves:

1. Adopt a common executive vocabulary for cyber resilience

Boards, national leaders and investors cannot govern what they cannot discuss in common terms. The first act of leadership is to move cyber conversations out of isolated technical vocabulary and into the language already used to make consequential decisions. The practical test is the board paper: every escalation, ministerial briefing and incident report should make clear what is at risk, which services may be affected, how long recovery will take, what economic value is exposed and who is accountable for the decision. This is not simplification, it is translation for governance, and the obligation sits with cybersecurity practitioners as much as with the leaders they brief.

2. Require cyber value and recovery metrics in board and public-sector reporting

Technical maturity scores alone are insufficient for boards, finance ministries, reinsurers and ratings agencies. The measurement set out in Pillar 3 is expressed in terms these audiences already use, and adopting it is a reporting decision rather than a technical one: leaders can require it of their own organizations without waiting for a standard to be agreed. Measurement that records only damage avoided understates the case for investment, because it captures what did not happen and omits what value was created. These measures need not be perfect to be useful, but they must be consistent enough to compare, credible enough to disclose and practical enough to inform decisions before a crisis occurs.

3. Price cyber posture into investment, insurance, ratings and financing decisions

Consistent measurement makes cyber capability something that can be priced. Pillar 2 shows what would be priced: organizations that invested in security protected revenue, cleared partner due diligence faster and moved to the cloud on schedule rather than stalling on unresolved risk. Those are ordinary business outcomes, and they belong in the same discussions as any other capital decision such as budget rounds, strategy reviews or acquisitions. The bigger shift comes from outside the organization. If investors, insurers and ratings agencies take cyber capability into account when setting borrowing costs, premiums and market access, boards no longer have to argue for security funding on its own terms.

4. Support a sustainable financing route for under-resourced environments

The countries, public-interest organizations and small enterprises most exposed to cyber shocks often have the least access to sustained funding, yet their failure creates spillovers through payments, identity systems, health services, logistics, telecoms and digital public infrastructure. Cyber preparedness in these environments should be financed as civil resilience rather than categorized narrowly as national security or defence. This reclassification is what opens the door to philanthropy, development finance and corporate giving, and is a decision for the leaders who set funding mandates rather than for the recipients.

5. Make cyber resilience a standing item in economic and financial stability forums

The first four moves each depend on someone convening them. Cyber resilience is discussed extensively in technical and security forums and only episodically in the bodies that govern economic stability, which is why attention rises after a major incident and recedes before the next. Placing it as a standing item on the agendas of finance ministries, central banks, prudential supervisors and international financial institutions would give the issue what it currently lacks: continuity of political attention between crises. This requires no new mandate; it asks existing forums to treat digital dependence as within their remit.

FIGURE 2 | **Elements of a senior leadership agenda for 2027**



Source: World Economic Forum

This agenda does not require senior leaders to become technologists; it requires them to govern dependence. The institutions that act first will not simply reduce cyber risk, they will protect continuity, strengthen trust, preserve value and help stabilize the digital foundations of growth. The leaders who define cybersecurity in those terms will shape whether 2027 becomes another year of reactive spending after preventable disruption, or the year cyber resilience becomes part of the operating model of the global economy. Cyber resilience will become a foundation of economic stability only when senior leaders choose to govern it that way.

Appendix: Methodology

This report is supported by primary and secondary research conducted by the Global Future Council on Cybersecurity. The quantitative findings in the report draw on the Survey on Cyber Language and Executive Decision-Making developed by the Global Future Council on Cybersecurity. Administered in English from 9 to 30 April 2026, the survey received 110 anonymous responses following open distribution through Council members' professional networks and contacts. It combined structured multiple-choice questions with optional open-text fields, asking respondents how cybersecurity is described within their organizations, which terms are most often misunderstood at senior level and where language gaps affected decisions or incident response. Respondents included executives, directors and managers from private- and public-sector organizations, critical infrastructure operators, multistakeholder and international organizations, and academic and research institutions across six regions. Responses were analysed and reported only in aggregate. As participation was voluntary and self-selected, and 60% of respondents were based in Latin America and the Caribbean, the findings reflect self-reported perceptions of institutional practice and should be interpreted as directional rather than statistically representative of the global cybersecurity community.

Alongside the survey, the report draws on structured mini-case submissions from organizations across five sectors and five regions. Using a common template, contributors identified mechanisms linking security investment to business value, the point at which cybersecurity became a business conversation and realized outcomes. Participation was self-selected, and outcomes were validated largely through organizations' own internal or external audit processes rather than independently by the Council. The cases are therefore presented as substantiated illustrations of reported effective mechanisms, rather than as a generalizable sample.

This report also draws on 13 semi-structured expert interviews conducted between January and March 2026 across cyber policy, public and private finance, philanthropy and related fields, as well as a desk review of 28 cyber and cyber-adjacent funds using publicly available information. Interview participants were selected purposively, while the fund mapping covered size, recurrence, scope, geography and source of capital. Coverage is strongest for North America, the European Union and the United Kingdom, and some fund sizes are approximate or bundled with adjacent programmes. Findings are therefore directional rather than statistically representative. The estimate of annual private and corporate philanthropic contributions to cybersecurity is derived from this mapping and presented as a range where dedicated cybersecurity budgets were unavailable.

Contributors

Global Future Council on Cybersecurity 2025–2026

Co-Chairs

Öykü Işık
Assistant Professor of Global Digital Transformation, Thunderbird School of Global Management, Arizona State University

Sami Khoury
Former Government of Canada Senior Official for Cyber Security

Council Members

Bushra AlBlooshi
Executive Director, Governance and Risk Management, Dubai Electronic Security Center (DESC)

Hoda Al Khzaimi
Associate Vice-Provost for Research Translation and Entrepreneurship, New York University Abu Dhabi

Christophe Blassiau
Senior Vice-President and Group Chief Information Security Officer, Schneider Electric

Cristina Camacho
Director for Human Rights and Peace, Ministry of Foreign Affairs and Human Mobility of Ecuador

Ann Cleaveland
Executive Director, Center for Long-Term Cybersecurity, UC Berkeley

Anna Maria Collard
Senior Vice-President, Content Strategy and Chief Information Security Officer Advisor Africa, KnowBe4

Belisario Contreras
Executive Director, Digi Americas Alliance

Michael Daniel
President and Chief Executive Officer, Cyber Threat Alliance

Humberto Luiz Ribeiro da Silva
Head, Center for Cyber Incident Prevention, Ciberlab, University of Brasilia

Shih Yen Lee
Deputy Chief Executive, Cyber Security Agency of Singapore (CSA)

Sameer Suryakant Patil
Director, Centre for Security, Strategy and Technology, Observer Research Foundation (ORF)

Thelma Quaye
Director, Infrastructure, Skills and Empowerment, Smart Africa Secretariat

Jamie Saunders
Oxford Martin Fellow, University of Oxford

Shlomo Serfaty
Chief Economist, Israel National Cyber Directorate

Despina Spanou
Deputy Director-General, Directorate-General for Communication Networks, Content and Technology (DG CNECT)

Confidence Staveley
Founder, Cybersafe Foundation

Rob Wainwright
Group Chief Information Security Officer, UBS (2023–2026)

Kemba Eneas Walden
President, Paladin Global Institute, Paladin Capital Group

Council manager

Giulia Moschetta
Lead, Insights, Centre for Cybersecurity, World Economic Forum

Council specialist

Ellie Winslow
Specialist, Insights, Centre for Cybersecurity, World Economic Forum

Acknowledgements

World Economic Forum

Joanna Bouckaert
Lead, Initiatives and Communities, Centre for Cybersecurity

Akshay Joshi
Head of the Centre for Cybersecurity and Member of the Executive Committee

Leandro Loss
Lead, Knowledge Communities, Global Future Councils

Nataša Perućica
Lead, Initiatives and Growth, Centre for Cybersecurity

Apisada Suwansukroj
Lead, Programming and Communications, Centre for Cybersecurity

For their contributions, the authors would also like to thank: Abdul Rahman AlBlooshi, Ahmed AlZarooni, Anton Bauman, Matas Bianchi, Zara Bruhn, Irene Corpuz, Fleur Heyns, Christopher Painter, Pavlina Pavlova, Claudio Peguero, Chua Kuan Seah, Eli Sugarman, Piyush Verma.

Production

Laurence Denmark
Creative Director, Studio Miko

Sophie Ebbage
Designer, Studio Miko

Simon Smith
Editor, Astra Content

World Economic Forum Public Engagement

Maxwell Hall
Creative Editorial Lead

Floris Landi
Design Lead

Sybile Penhirin
Head, Video and Design

Esther Pennella
Communications and Coordination Specialist

Endnotes

1. World Economic Forum. (n.d.). *Global future council on cybersecurity: Members*. Retrieved August 26, 2026, from https://initiatives.weforum.org/global-future-council-on-cybersecurity/members
2. Wise, A. (2025, December 29). Cyber attacks "tipping point" warning issued after Harrods and M&S targeted. *Independent*. https://www.independent.co.uk/news/uk/home-news/cyber-attacks-warning-harrods-b2891386.html
3. United Kingdom Department for Science, Innovation & Technology. (2025, November 12). *Summary of research on the economic impact of cyber attacks*. https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk/summary-of-research-on-the-economic-impact-of-cyber-attacks
4. Natalucci, F., Qureshi, M. S., & Suntheim, F. (2024, April 9). *Rising cyber threats pose serious concerns for financial stability*. IMF Blog. International Monetary Fund. https://www.imf.org/en/blogs/articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability
5. World Economic Forum. (2024). *Unpacking cyber resilience*. https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf
6. Riyadh Centre for Cyber Economics. (n.d.). *Centre for Cyber Economics*. Retrieved August 26, 2026, from https://www.cybereconomics.org/home
7. World Bank. (2022). *Tech savvy: Advancing GovTech reforms in public administration*. https://documents1.worldbank.org/curated/en/099400004112257749/pdf/P1754970d6c6420f00ab5905f7004ba9c2f.pdf?utm_
8. United Nations Trade and Development (UNCTAD). (2025) *World investment report 2025*. https://unctad.org/publication/world-investment-report-2025
9. Eling, M., Elvedi, M., & Falco, G. (2023). The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*, *27*(3), 429–443. https://doi.org/10.1080/10920277.2022.2034507
10. Olsen, E. (2025) *UnitedHealth hikes number of Change cyberattack breach victims to 190 million.* https://www.healthcaredive.com/news/change-healthcare-cyberattack-affects-190-million-unitedhealth/738351/
11. World Economic Forum (2025) *Global cybersecurity outlook 2025*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
12. Bank of England (n.d.) *CBEST threat intelligence-led assessment.* Retrieved August 26, 2026, from https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide
13. Associated Press. (2022, May 12). Costa Rica declares national emergency amid ransomware attacks. *Guardian*. https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks
14. Esmaeili, N., Janik, K., Lau, T., et al. (2024). *2024 Funding trends report: Climate change mitigation philanthropy.* ClimateWorks Foundation. https://www.climateworks.org/report/funding-trends-2024 /
15. Stanford Institute for Human-Centered Artificial Intelligence. (2026). *The 2026 AI Index report* (Chapter 4). https://hai.stanford.edu/ai-index/2026-ai-index-report/economy
16. Collard, A. M., Cleaveland, A., Al Khzaimi, H., et al. (2026, August 3). *Why cybersecurity needs a sustainable finance mechanism.* World Economic Forum. https://www.weforum.org/stories/cybersecurity/cybersecurity-sustainable-finance-mechanism/