uvance Wayfinders

Consulting by Fujitsu

The cyber resilience divide

Fujitsu Cybersecurity Report

FUJITSU

How leading organizations balance innovation, risk and resilience in the age of AI

News of devastating cyber security incidents is no longer unusual. The window between vulnerability discovery and exploitation has shrunk from weeks to hours, with major attacks regularly disrupting operations, damaging customer trust and wiping billions from companies' value.

The August 2025 Jaguar Land Rover cyber attack, for instance, is estimated to have cost the company £1.9 billion, and a ransomware attack on a global food and beverage group forced production and shipment shutdowns and compromised customer and employee data.

New Uvance Wayfinders research reveals that such headline-grabbing events are only part of a broader shift. Our new global survey of 400 executives shows that cyber disruption is becoming a routine operational risk for businesses of all sizes and in all sectors. As organizations accelerate digital transformation, technologies such as AI are simultaneously expanding the internal attack surface and empowering cyber criminals with new capabilities.

2/3 **of companies report experiencing at least one significant cyber security incident in the past 12 months.**

Executives are already feeling the impact. Two-thirds of companies report experiencing at least one significant cyber security incident in the past 12 months, and they say the frequency of threats has increased over the past three years.

As a result, cyber resilience – the ability to adapt to evolving threats and protect the business from significant disruption and long-term damage – is now at the top of executive agendas: 67% say it's critical to overall strategy, while just 33% see it as a technical requirement.

But despite their shared recognition of risk, organizations aren't all reacting in the same way. Our research reveals a growing divide between organizations that are building true cyber resilience through leadership, investment and innovation and the ones that are still vulnerable.

What do companies need to do to secure their futures when the threats keep multiplying? In this report, we explore what sets leading organizations apart, the technologies and tactics that are fueling true resilience and why strong cyber security is increasingly linked to business success.

AI is raising both risk and reward

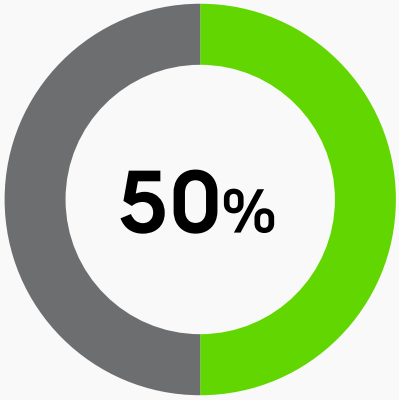
AI is transforming how organizations operate, but it's also reshaping the cyber threat landscape.

AI allows cyber criminals to rapidly detect vulnerabilities and automate malware development. It can also make their phishing campaigns more sophisticated. Once attackers gain access to company systems, AI can accelerate reconnaissance and cause maximum disruption.

Executives are aware of the scale of the threat: 61% say AI-enabled cyber attacks pose the greatest risk to their organization's security and resilience today.

The threat doesn't just come from outside the business. AI is also introducing new vulnerabilities from within organizations. As adoption accelerates, AI tools expand the internal attack surface, and many companies are innovating too fast for their governance to keep up. Half (50%) of executives say they're under pressure to accelerate AI innovation faster than their cyber security and governance frameworks can keep pace.

When governance is addressed, it's often reactive. More than half (56%) of organizations retrofit existing cyber security controls after technologies are deployed, instead of investing in targeted measures from the start. Governance frameworks that aren't fit for purpose leave gaps vulnerable to exploitation.



of executives say they're under pressure to accelerate AI innovation faster than their cyber security and governance frameworks can keep pace.

Visibility is another challenge. Many executives say they don't know where or how employees are using AI. 57% say that unmanaged or "shadow" AI tools represent a growing risk to their organization. They can't govern AI effectively without this oversight.

But the research also reveals a powerful upside to AI. When organizations get their governance right, the benefits go beyond security. Nearly seven in 10 (68%) executives say that strong AI security frameworks help to build trust with customers and partners, supporting retention and long-term business value. So balancing AI adoption with cyber risk is complex, but the rewards for organizations that get it right can be significant.

From prevention to preparation

Traditional cyber security measures were built around prevention. But as attacks become a constant threat and sophistication grows, the complete elimination of cyber incidents is no longer realistic.

Executives seem to understand this: 67% say their cyber security strategies now assume breaches will occur and aren't focusing on prevention alone.
This means that the real test of cyber resilience is no longer about whether organizations can stop every incident. Instead, the test is whether they can continue operating when an attack happens. Organizations need to prepare their security frameworks for the worst-case scenario.

Our research shows there's a clear divide between organizations in how they approach this challenge. Some executives are confident in their ability to respond to major cyber security incidents and recover critical operations without incurring significant commercial damage. These are the "leaders" in our research. But others are still worrying about the impact an attack would have on their business. These are the "laggards."

The difference in confidence between the two groups reflects the difference in their strategic choices. Here, we examine what's fueling the leader group's cyber resilience, why the laggards lack confidence and what other executives can learn from both groups.

Cyber resilience is a matter of culture

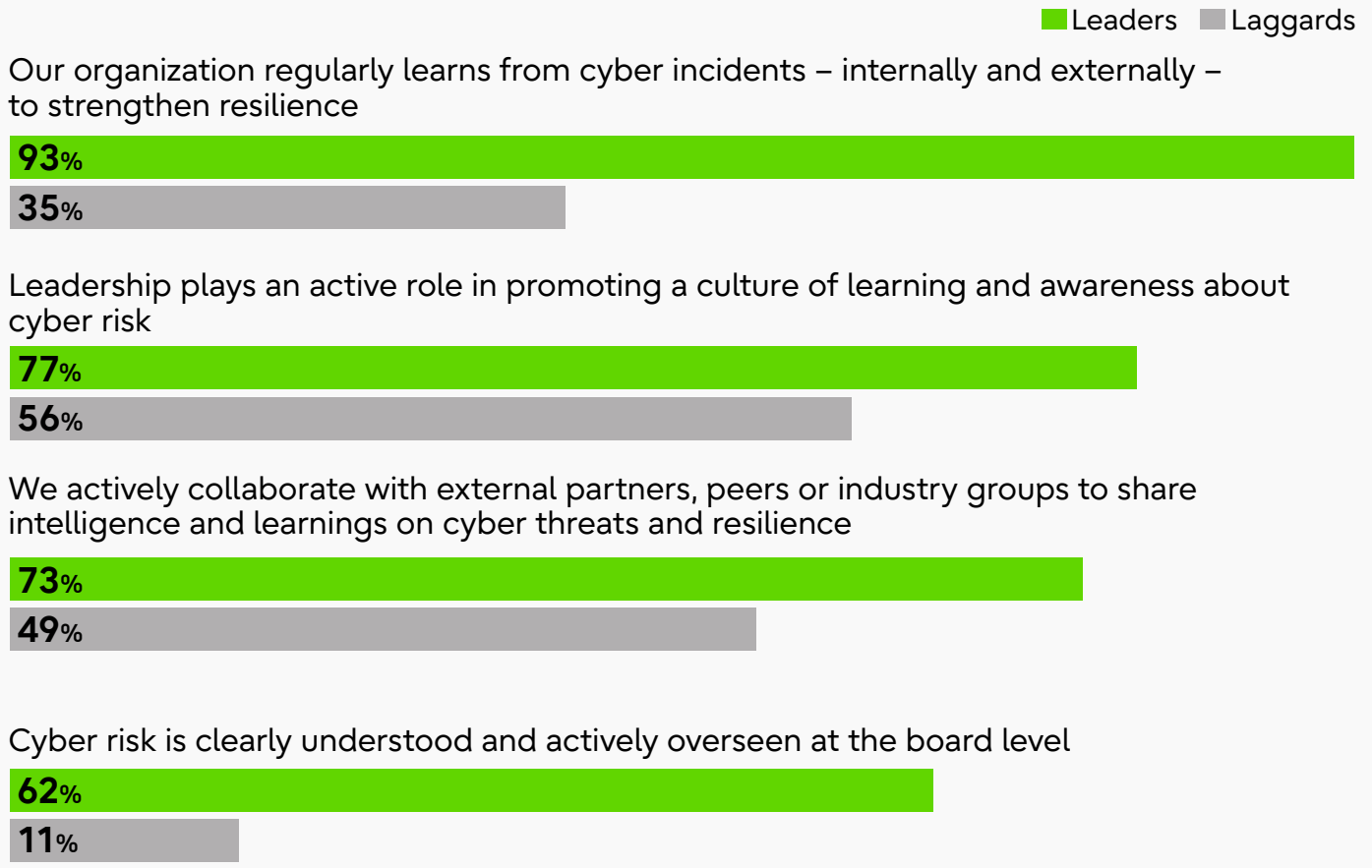
Cyber security is only as good as the weakest link. A single lapse of judgment and weak organizational awareness can compromise even the most advanced security infrastructure. So cyber resilience must become a company-wide priority.

The most resilient organizations know that cyber culture transformation starts at the top. More than three-quarters (77%) of the leader group say their leadership plays an active role in promoting a culture of learning about cyber risk, compared with 56% of laggards.

The difference is even more stark at the board level. The majority (62%) of the leader group say that cyber risk is clearly understood and actively overseen by their board, compared with just 11% of laggards. This leadership gap has real consequences: without board-level visibility and instruction, cyber resilience can't be fully integrated into broader business strategy.

The leader group makes cyber resilience a day-to-day priority

Q: To what extent do you agree with the following statements about your organization's cyber resilience?



The leader group also understands that resilience requires constant learning. Almost all of them (93%) regularly learn from internal and external cyber incidents, compared with just 35% of laggards. And 73% actively collaborate with external partners, peers and industry groups to share intelligence – less than half (49%) of laggards do the same.

For leading organizations, cyber resilience is embedded into their day-to-day culture and decision-making. It's not confined to the IT function.

Leaders prioritize responsible innovation

The most resilient organizations manage innovation responsibly. Our research shows that the leader group deliberately strikes a balance between innovation and governance: 72% say they adopt emerging technologies cautiously – only once cyber risks are well understood and guardrails are in place.

Laggards take a different approach. The majority (59%) prioritize early adoption, even when they don't fully understand the security implications. Laggards might win the deployment race, but these knowledge gaps could have devastating consequences if they expose the organization to cyber criminals.

This divide is especially apparent in AI strategies. The leader group is four times as likely to have strategies that enable AI-driven innovation without introducing unacceptable cyber risks. They have a good understanding of where and how AI is used by their employees: 56% are monitoring shadow AI use, compared with just 27% of laggards.

The leader group is also getting ahead on AI's next frontier: agentic AI. Six in 10 (61%) are embedding security controls for agentic systems, compared with 28% of laggards.

Unlike traditional AI models, which are largely confined to pattern recognition and predefined tasks, agentic systems can act autonomously and make decisions with limited human input or oversight. This difference significantly expands the threat landscape.

Internally, agentic AI can introduce vulnerabilities by interacting with multiple systems and acting in ways that are more challenging to monitor or control. Cyber criminals can use it for more frequent, adaptive and persistent attacks.

Agentic knowledge gaps are a problem for laggards: 71% say that internal agentic AI introduces cyber risks they don't fully understand yet, compared with just 37% of the leader group.

They're even more worried about how the technology will be used by cyber criminals. Eight in 10 (81%) say agentic AI-driven cyber attacks introduce new resilience requirements that they aren't prepared for, compared with 38% of the leader group.

As AI adoption accelerates, organizations need to close these knowledge gaps quickly through upskilling, hiring or partnerships.

Shift from response to resilience

Another clear difference between leaders and laggards is how they prioritize cyber resilience over time.

Most of the leader group (65%) focus on building long-term business resilience, while 68% of laggards prioritize immediate threats and short-term risk reduction. Both are important, but organizations that spend most of their time fire-fighting can fall into a reactive cycle, unable to look forward and get ahead of the next wave of threats.

What's causing laggards to be more short-termist? Our research reveals a broader maturity gap.

Many laggards still rely heavily on theoretical planning and foundational activities, such as risk forecasting and employee training. These practices are important but aren't enough on their own when threats evolve so rapidly.

Leaders are moving to the next stage of defense maturity

Q: To what extent does your company use the following solutions/initiatives to enhance cyber resilience? Frequent/fully embedded

The leader group recognizes this, and having mastered the basics, is focusing on strategy validation and refinement. More than half (56%) frequently stress-test their processes by conducting independent, real-world cyber attack simulations.

One example is white-hat hacker exercises, where security specialists apply ethical hacking techniques to identify and disclose system weaknesses. These exercises help executives identify vulnerabilities before attackers do and make sure that resilience strategies are effective.

Fight AI-enabled threats with AI-enabled resilience

There's no doubt that AI is increasing cyber risk. But what many executives don't realize is that it's also one of the most valuable tools for defending against cyber criminals.

Once again, the leader group is ahead here. Nearly eight in 10 (79%) say AI is becoming essential for defending against increasingly sophisticated cyber attacks, compared with just 44% of laggards.

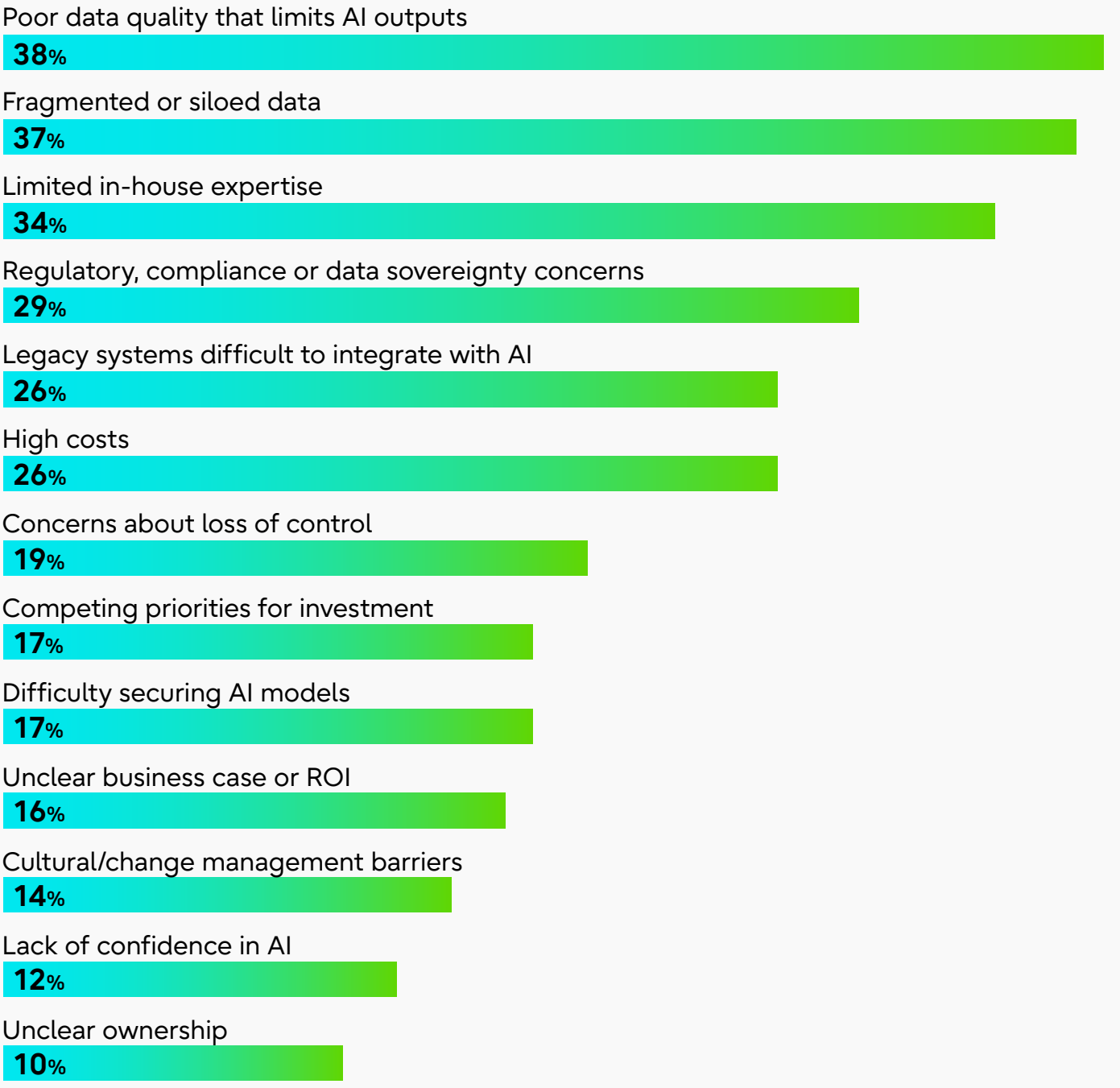
This belief is reflected in their cyber resilience strategies. The leader group is more than twice as likely to rely on AI-enabled threat detection and anomaly monitoring, more than three times as likely to use AI to support decision-making and four times as likely to use AI in incident response and containment. AI tools are allowing these organizations to identify threats earlier, respond faster and continuously adapt their defenses.

But even the organizations that recognize AI's potential face barriers. Our research highlights two major obstacles: data foundations and talent. Executives rank poor data quality and fragmentation as the greatest barriers to embedding AI in cyber resilience. Limited internal expertise follows closely behind.

Without strong organizational readiness, AI investments won't deliver their full return on investment (ROI). So organizations need to prioritize data modernization and capability development to unlock the technology's potential to improve their cyber resilience.

Data issues and skill gaps limit AI adoption

Q: Thinking about your organization, what are the greatest barriers to embedding AI into cyber resilience strategies?



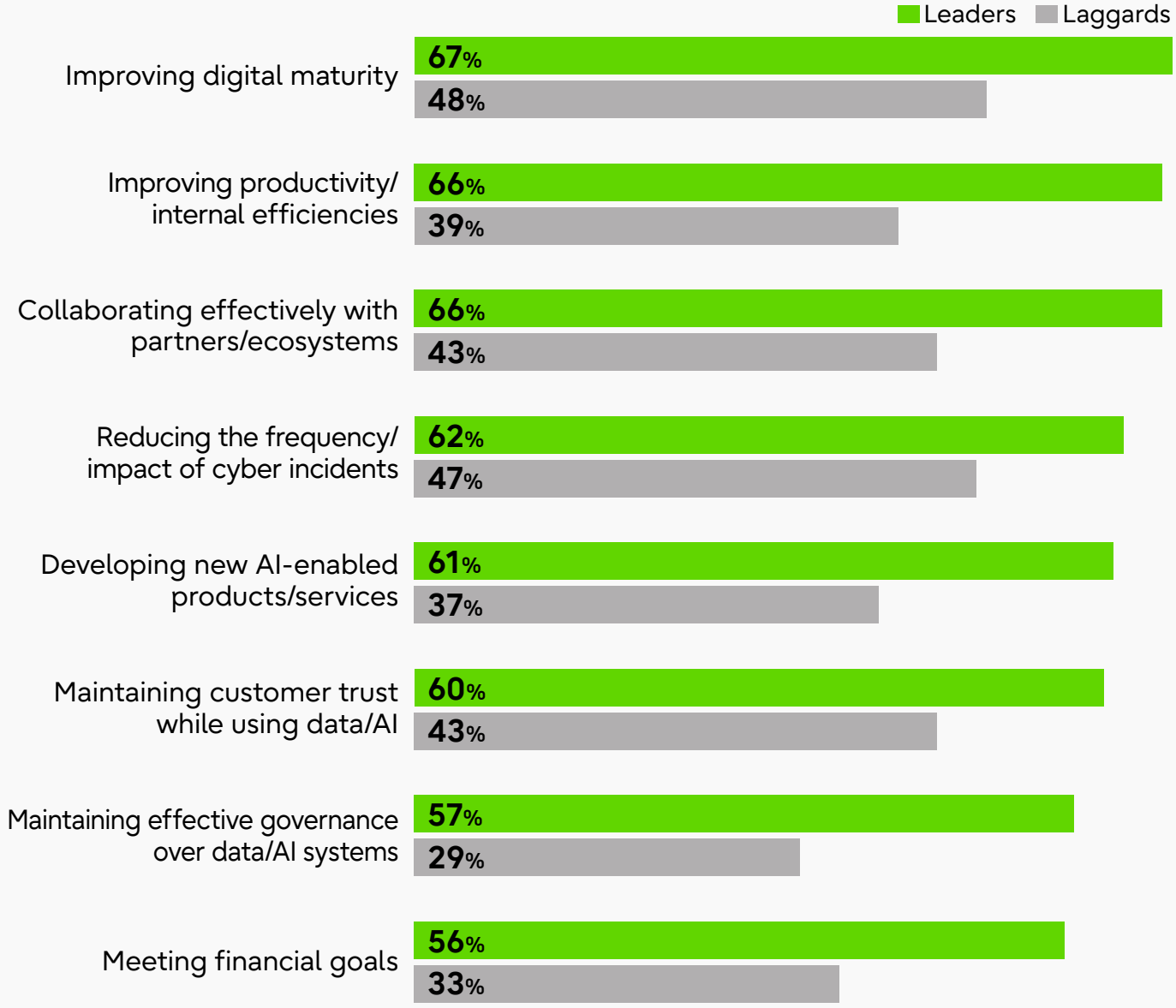
The business case for cyber resilience

Organizations with strong cyber resilience are already seeing measurable benefits. More than six in 10 of the leader group (62%) are reducing the frequency and impact of cyber security incidents, compared with just 47% of laggards.

But the advantages go beyond security improvements.

Strong cyber resilience correlates with better business outcomes

Q: How well is your organization currently performing against each of the following objectives? Performing well



By putting in place the right safeguards, governance and controls, organizations in our leader group create conditions that allow them to innovate faster and more confidently. Six in 10 (61%) are successfully developing new AI-enabled products and services, compared with just 37% of laggards. And 67% have improved digital maturity across the organization, compared with 48% of laggards.

Critically, the leader group is also better at maintaining customer trust while using data and AI, which supports retention and long-term commercial success. And they're far more likely to meet financial goals, improve productivity and collaborate effectively with partners.

These findings show that cyber resilience is no longer about simply avoiding risk. Increasingly, it's also a way to improve business performance.

How to build a resilient business

The leader group identified in our research shows that balancing AI innovation with cyber resilience isn't just possible – it's increasingly essential.

For the organizations that are struggling with cyber resilience, becoming a leader isn't out of reach. The gap between leaders and laggards isn't defined by their scale or their sector but by their strategic choices. This means an organization can change its trajectory by changing the way it approaches cyber security and shifting its priorities.

Based on our research findings and our experience supporting organizations with their cyber strategies, this is the path to leadership:

1. Design for breach, not just prevention

The most resilient organizations accept that cyber intrusions are inevitable. They move away from the "fortress" mentality and design systems, processes and governance frameworks accordingly. By prioritizing detection, response and rapid recovery, executives can ensure their organizations remain operational, even when their defenses are breached.

2. Build resilience into leadership and culture

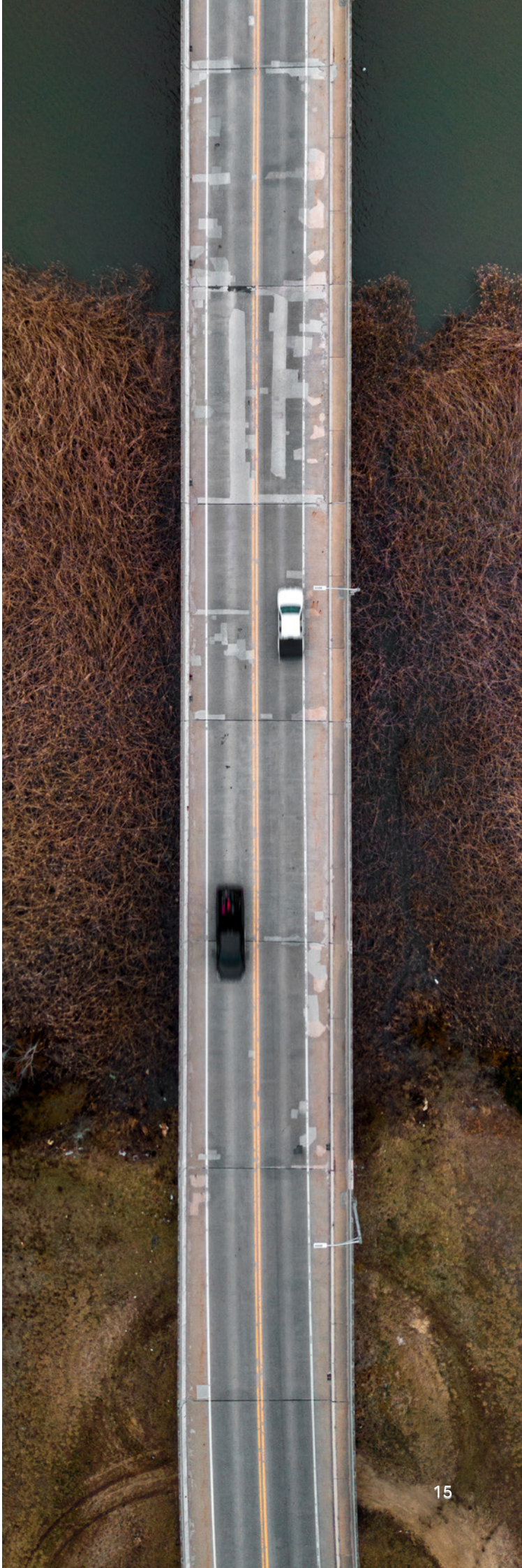
Cyber resilience starts in the boardroom – it's no longer a technical problem that the organization can delegate to IT. Organizations should assume breaches will occur and embed cyber resilience into company culture to make sure executives and employees understand their roles in protecting operations and maintaining trust.

3. Protect what matters and test it in the real world

Organizations should move beyond trying to protect everything equally. By prioritizing mission-critical assets and validating defenses against realistic attack scenarios, executives can focus resources where disruption would cause the greatest business impact. This is how to make sure resilience strategies work in practice – not just on paper.

About the research

In February 2026, Uvance Wayfinders surveyed 400 senior business leaders based in Australia, Japan, the UK and the US. They represented technology and IT, finance, strategy and operations equally and were from companies across the following sectors: financial services; manufacturing; energy, resources and utilities; logistics and supply chain; retail and consumer goods; healthcare and life sciences; the public sector, government and defense; technology and telecommunications; and professional services. About half (53%) of companies had between 1,000 and 4,999 employees, 20% had between 5,000 and 9,999 employees and 28% had more than 10,000 employees. Percentages throughout this report may not sum precisely due to rounding.



uvance
Wayfinders

Consulting by Fujitsu

FUJITSU