ncc group

The state of supply chain security

What's inside

- Global insights into supply chain security posture
- Details of the changing regulatory landscape
- Practical advice on enhancing supply chain security

nccgroup.com/the-state-of-supply-chain-security

October 2025

Contents

03 Foreword, Mike Maddison, CEO

04 Executive summary

05 Key stats at a glance

07 Critical questions to ask

08 Major risk areas

- **09** The overconfidence trap
- **14** The responsibility gap
- **19** The shadow of AI

24 Global spotlight

25 Global complexities, regional nuances

29 Five steps to enhance supply chain security

33 Final thoughts

34 Immediate actions

35 Methodology

Foreword

Mike Maddison
CEO, NCC Group

In today's hyper-connected economy, cyber attacks are no longer a distant threat, they're a daily reality. With cyber resilience rising up the boardroom agenda following recent high profile attacks, one critical vulnerability remains overlooked: the supply chain. The soft underbelly of cyber resilience.

Global supply chains are layered, complex, and sprawling, and are the engine of modern business. From global cloud providers, distributors and manufacturers to SMEs and local businesses, the delivery of one product or service may rely on hundreds of interconnected organisations. But every new supplier, vendor, or third-party service adds exposure. Each link in the chain is a potential entry point for attackers. And with that, the risk multiplies, quietly, invisibly, and sometimes catastrophically.

Your security is only as strong as the weakest link in your supply chain. A single compromise can trigger a butterfly effect rippling across operations and business continuity, draining finances, and damaging reputations.

Resilience demands more than software or siloed teams. It requires a clear understanding of your unique risk profile, a culture of openness and challenge, strong relationships with third parties, and the agility to respond to a shifting threat landscape.

When we began this report, we expected supply chain resilience to be top of mind. We assumed leaders would be deeply concerned about visibility gaps and the complexity of third-party risk.

Instead, we found something deeply concerning: a sense of complacency.

Despite recent high-profile disruptions, many organisations appear to overestimate their ability to manage third-party risk. They rely too heavily on compliance frameworks and underestimate the operational fallout of a breach.

Our experts see the reality every day. And it's clear: we may be sitting on a ticking time bomb.

The call to action is urgent. Supply chains are your problem – because they're everyone's problem. As leaders, we must own this challenge. Not just to protect our own organisations, but to raise the bar for cyber resilience across the economic ecosystems we rely on.

Mike Maddison
CEO, NCC Group

Executive summary

The tip of the iceberg

Organisations today are navigating a perfect storm: evolving global markets, increasingly complex supply chains, and a cyber threat landscape that's growing in both scale and sophistication. Our latest Cyber Threat Monitor revealed a 15% surge in ransomware attacks in 2024 alone, a record high.

To understand how businesses are tackling the challenge of supply chain cyber security, we conducted a global study exploring the key concerns, pressures, and priorities shaping their approach. The findings offer a compelling snapshot of how decision-makers around the world have perceived and responded to evolving supply chain risks.

Our research highlights that the rising tide of risk is crashing into supply chains, with 68% of organisations expecting attacks to become even more severe. At the same time, emerging technologies like Artificial Intelligence (AI) are reshaping how we operate, unlocking new efficiencies, but also introducing new vulnerabilities.

The reality? Supply chain security is an iceberg. What's visible above the surface is only a fraction of the risk. Beneath lies a vast, often unseen network of dependencies and exposures.

We've seen the consequences play out in real time:

- Critical medical procedures delayed
- Retail shelves left empty
- Flights grounded
- Organisations paralysed for weeks

All triggered by a single supplier breach. The ripple effects are economic, operational, and deeply human.

68%

of organisations expect the severity and scale of supply chain attacks to escalate further

Our research identified three critical risk areas that demand urgent attention:

1. The overconfidence trap

94% of respondents are confident in their ability to respond to a supply chain attack. 92% trust their suppliers to follow best practices. Yet only 66% regularly assess supplier risk. This disconnect suggests many may be underestimating the scale of the threat. Are organisations sleepwalking into a resilience crisis?

2. The responsibility gap

While 57% of CEOs believe they have strong visibility into supply chain security, only 30% of directors and 18% of team supervisors agree. Responsibility is often pushed to cyber security teams, with 62% saying it's their job alone. But resilience can't live in a silo. It requires shared ownership across the business.

3. The shadow of AI

AI is now the top emerging risk in supply chain security. 59% of respondents expect it to drive the greatest increase in threat over the next year. Yet many organisations lack visibility into how AI is being used, both by employees and by attackers. From data poisoning to model manipulation, the risks are real and rising.

These findings raise a fundamental question: if supply chain attacks are inevitable, what can organisations do to increase not only their resilience, but that of their supply chain?

This report offers data-driven insights and expert analysis to help you answer that question. More importantly, it provides a roadmap for action. The next wave of cyber threats is already forming. Now is the time to strengthen your defences.

Key stats at a glance

Research methodology

In 2025, we surveyed 1,010 professionals who were responsible for cyber security in organisations with over 500 employees.

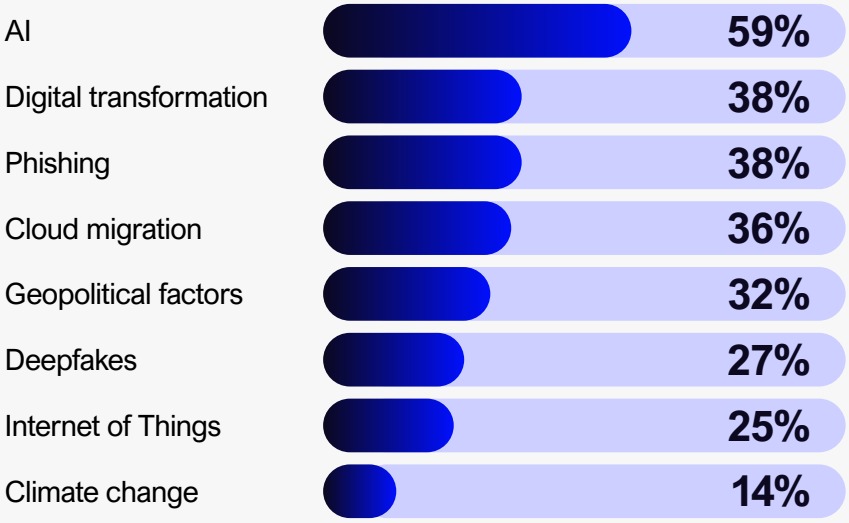
To achieve a global view, we included eight key markets: Australia, Germany, the Netherlands, Singapore, Spain, the Philippines, the US, and the UK.

Security threats

45%

of respondents experienced a cyber security breach in the last 12 months

The greatest threats to supply chain security were stated as:



Security confidence

94%

of organisations were confident in their ability to respond quickly to a supply chain attack

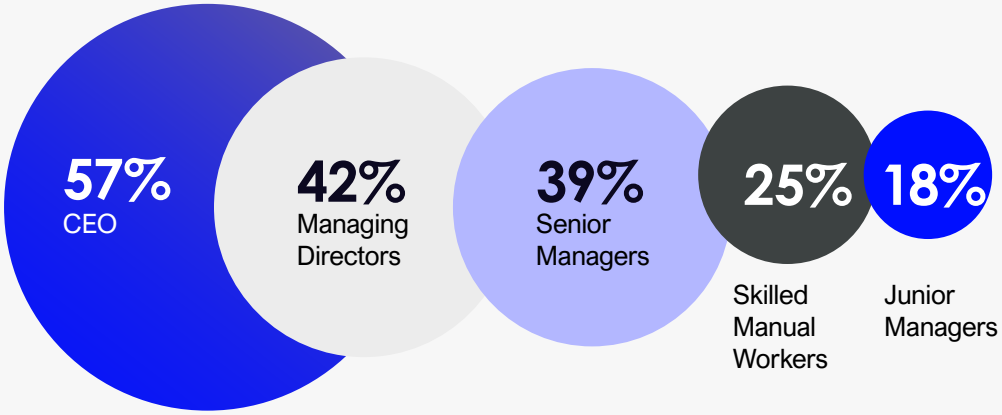
92%

of organisations trust their suppliers to follow cyber security best practice

59%

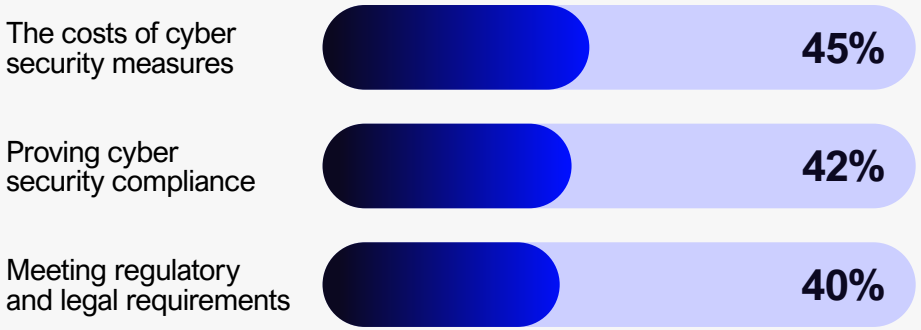
of respondents were concerned about the visibility over their supply chain

Senior leaders were more confident in their supply chain visibility than other roles, with 57% claiming they had full and detailed insight into their supply chain's cyber security.

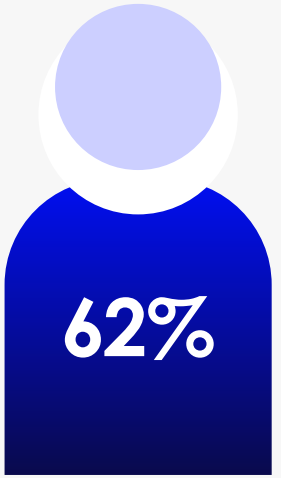


Pain points

The most common pain points regarding cyber security and compliance were:



Responsibilities



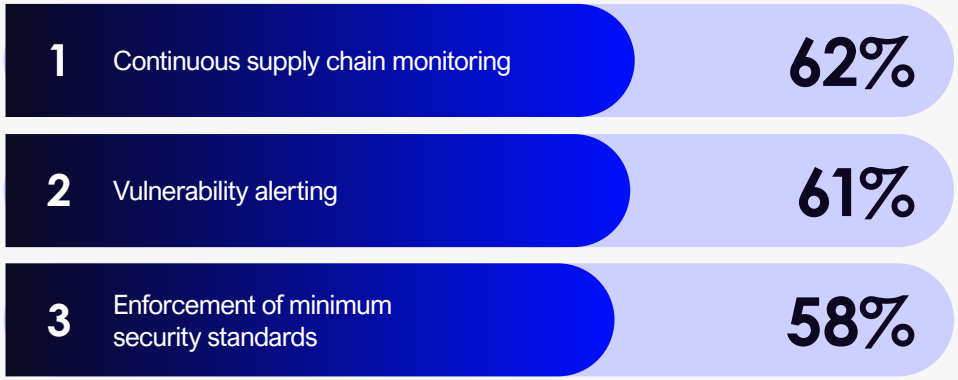
of respondents believe their cyber security teams bear responsibility for cyber incidents that affect their operations

Priorities and investments

of organisations believe that their spending on cyber security will increase over the next 12 months

of respondents said that current cyber security standards and regulations adequately reduce risks of suffering supply chain attacks

The top three services that organisations are considering investing in to improve supply chain security are:



Critical questions to ask

Executives and board members

Leaders set the tone for supply chain resilience. Their strategic choices and investment priorities determine whether their organisation takes a proactive or reactive approach to risk.

It is important that they ask themselves:

- How can we lead on supply chain security, ensuring we reduce the likelihood of an attack and mitigate the effects if one were to be successful?
- Who can help me interpret compliance reports and give frontline context at an operational level?
- Are we investing enough resource and budget towards supply chain resilience?
- Is regulatory compliance alone enough to keep us secure?

Procurement

Procurement plays a frontline role in onboarding and managing suppliers, but security isn't always central to their processes and decisions.

It is important that they ask themselves:

- Which suppliers access our different systems and data, and are they secure?
- How often are we checking that suppliers meet evolving standards and best practice?
- Are all suppliers following the minimum standard of Cyber Essentials, regardless of location?
- When should we keep working with suppliers who fall short of our security standards? And how do we do this?

CISOs

CISOs own the supply chain cyber risk strategy, from defining secure suppliers to managing compliance, contracts, and emerging tech.

It is important that they ask themselves:

- Do we have a clear, risk-based definition of a secure supplier?
- Can we audit and dictate how artificial intelligence and large language models are being used in our supply chain?
- Will enforcement of the Artificial Intelligence Act be sufficient to support our supply chain security?
- Are our contracts keeping pace with evolving threats and international compliance standards?
- Do compliance reports reflect what's really happening across our supply chain?
- How do we balance security with operational efficiency?

Cyber professionals

Cyber teams see the vulnerabilities others miss, but often lack the authority or budget to fix them.

It is important that they ask themselves:

- How can we escalate supply chain concerns and unlock budget to address them?
- How might the use of artificial intelligence in our organisation – both authorised and hidden – be impacting the security of our supply chain?
- How do we highlight the disconnect between compliance forms and real-world risk?

Major risk areas

The overconfidence trap

Organisations are confident in their ability to withstand disruption following a supply chain cyber attack – but this may not tell the full story.

94%

of respondents are confident about their ability to respond quickly to a supply chain attack

45%

of respondents said that they have experienced a cyber security breach in the last 12 months

21%

of respondents feel as though they wouldn't be affected if a key supplier was unable to operate for five days

As supply chains become increasingly complex and digitally interconnected, we are witnessing a domino effect in terms of the scale and frequency of cyber incidents.

It is creating vulnerabilities in global networks and leaving organisations around the world exposed to threats, prompting the World Economic Forum (WEF) to highlight increasingly complex supply chains as a critical risk in its latest Global Cyber Security Outlook report.

In stark contrast to the risk identified by NCC Group and global bodies, 94% of respondents feel confident in their ability to respond quickly to a supply chain attack. This is a marked increase compared to the findings in on our Global Insight Space report from March 2023, which found that only 32% of respondents were 'very confident' in their ability to respond to a supply chain attack quickly and effectively.

At first glance, this surge in confidence appears reassuring, but organisations may be overestimating their ability to respond quickly and effectively when incidents strike. We know from our Annual Cyber Threat Monitor Report that ransomware attacks are at a record high, increasing 15% in 2024 alone, therefore these latest findings suggest a troubling disconnect between perception and reality. Could a false sense of security be leading organisations to 'sleepwalk' into critical cyber incidents?

A false sense of security

An overwhelming 92% of organisations reported trusting their suppliers to follow cyber security best practices. This level of trust suggests organisations have faith that suppliers are well-equipped to prevent, detect and respond to attacks, and possibly that they would receive support in the event of a cyber attack within the supply chain.

Yet, this optimism may not reflect actual preparedness. As cyber threats become more sophisticated and supply chains more complex, the assumption that suppliers are secure and capable of effectively responding to attacks is dangerously naive.

Ade Clewlow MBE, Associate Director and Senior Advisor at NCC Group, suggests that more needs to be done to ensure that confidence in suppliers' cyber security posture is well-placed: "While it's heartening to see that organisations have confidence in the security of their suppliers, this isn't necessarily reflective of the wider security landscape when it comes to supply chains. For organisations to have these confidence levels, there needs to be an in-depth understanding of supply dependencies, something most organisations are still working to put in place."

Another factor to consider is that, while organisations often express confidence in their visibility of direct suppliers, visibility beyond these immediate relationships is frequently lacking.

Many focus primarily on direct partners, with far less insight into subcontractors and fourth-party engagements. The risk factor could increase exponentially when you consider the number of hidden organisations in your supply chains, which can impact your resilience and security posture.

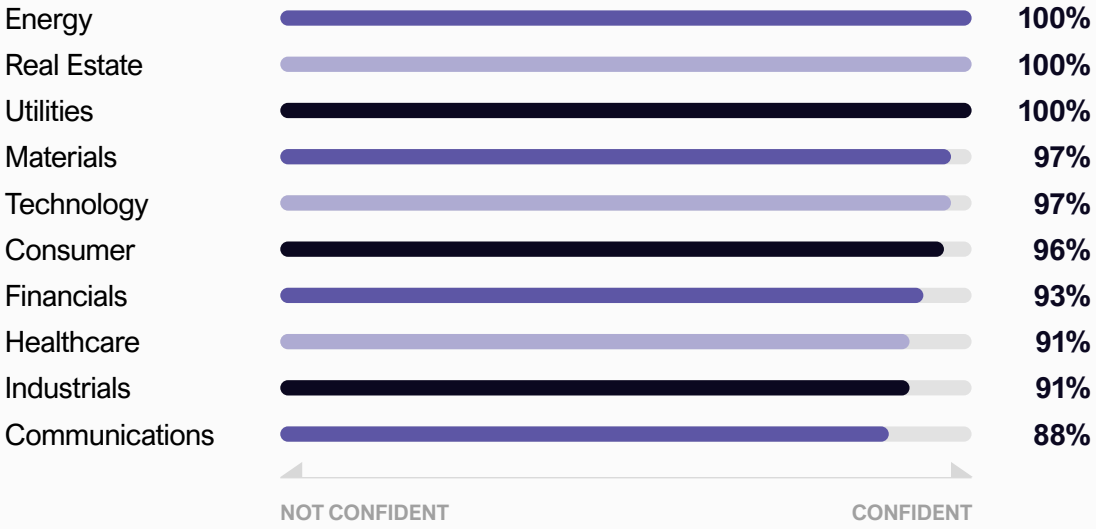
The illusion of oversight

The disconnect between confidence and actual preparedness becomes even more apparent when you investigate how organisations are protecting themselves. Only 66% of respondents regularly monitor their suppliers and conduct risk assessments – but relying on monitoring alone is not enough. Just because an organisation believes it has full supply chain visibility, does not necessarily mean that its suppliers have adequate cyber security practices in place.

And while point-in-time, tick-box assessments may satisfy compliance requirements and reassure boards, 65% of IT teams remain concerned by the lack of real-time visibility over their supply chain.

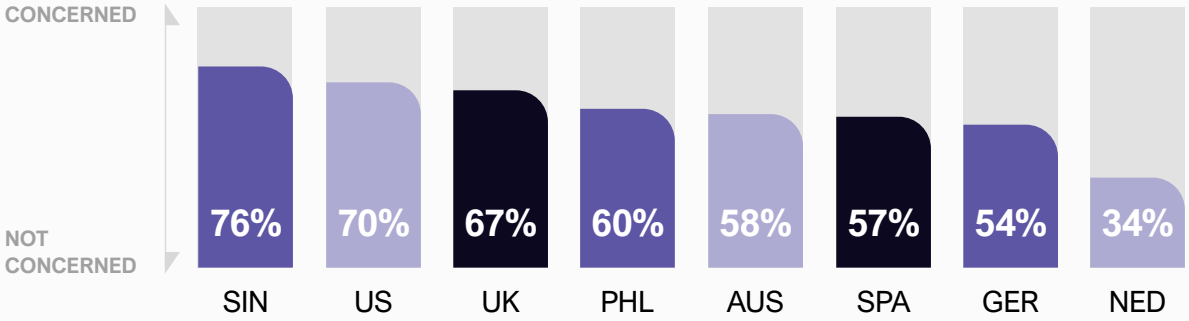
James Pearce, Commercial Director at NCC Group, cautions against over-reliance on passive monitoring, which is commonly trusted to provide confidence in supply chain security: "Organisations lack control over large third-party suppliers. If you can't take corrective action, visibility doesn't translate into security. You could spend your entire budget on monitoring, but without action, it's not a complete solution."

How confident are different sectors in their ability to respond to a supply chain attack?



Which regions are most concerned about their supply chain visibility?

Singapore (76%), US (70%) and UK (67%) respondents were most concerned about supply chain threats. Interestingly though, 50% of US respondents also claimed to have "full and detailed insight" into their supply chain security. Does this suggest that many US companies may overestimate their level of insight? Or maybe they recognise that visibility alone doesn't guarantee protection?



Overconfidence in downtime resilience

While many organisations are aware of the disruption a supply chain attack could cause, one in three still believe they would remain unaffected if a key supplier went offline for 24 hours. Concerningly, even as the length of cyber disruption increases, confidence remains high, with one in five organisations still believing they would be unaffected by five days of supplier downtime.

Based on our experience in the field, there is a mismatch between confidence in response capabilities and the real risk of downtime and disruption. As supply chain cyber incidents become more common, you cannot afford to make assumptions or hope for the best. To ensure continuity, you must have a clear understanding of how supplier downtime could affect your operations.

The impact of a supplier breach can be devastating. In the healthcare sector for example, it can risk real-world harm to patients and place significant operational pressure on staff as they work to keep services running. An overconfidence in the ability to withstand such disruption can lead to insufficient preparation and underinvestment, particularly as supply chain attacks increase and budgets tighten. In this climate, a level of arrogance and complacency becomes even more dangerous.

Pearce reinforces this, delving into why organisations may be less likely to invest in resilience measures when it comes to supplier security specifically: “Many organisations don’t truly understand the cascading effect of a supplier cyber attack and the major disruption it can cause, so they aren’t investing enough in resilience. It’s like being told to invest in fireproofing your neighbour’s house. Would you do it if you believed your own home was immune? It’s only when the fire spreads that the true cost of inaction becomes clear.”

An awareness of the threats

So, while some organisations may be overconfident in their ability to respond to supply chain attacks, there is generally a strong awareness of the growing threat landscape. And the increasing interconnectedness of global supply chains only amplifies these risks.

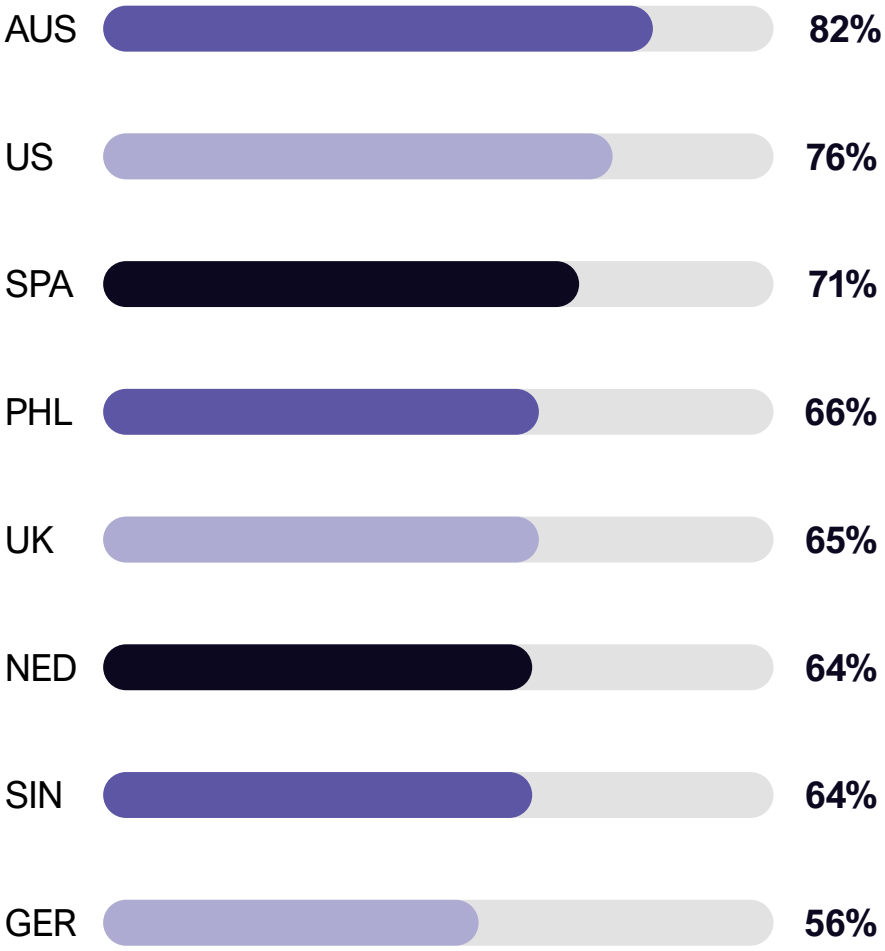
In fact, 45% of respondents reported experiencing a supply chain attack in the last 12 months, and 49% faced operational suspension as a result. Over two-thirds of organisations also expect supply chain cyber threats to become more severe over the next 12 months. This aligns with our 2023 supply chain research, which found that the number of cyber attacks on company supply chains increased by 51% in just six months.

With half of organisations suffering major disruptions due to supply chain attacks, it reinforces the critical need to address the overconfidence trap and ensure you are alive to the realities of what is at stake.

1 in 5

organisations believe they would be unaffected by five days of supplier downtime

Which regions have reported the highest expectation of increased cyber threat?



Regulatory challenges and geopolitical shifts

Regulatory approaches to supply chain security are evolving in response to recent elections, which have reshaped national cyber security policies across the world. With 95% of respondents believing standards and regulations reduce the risk of supply chain attacks, it's clear that regulations are playing an important role in strengthening resilience.

Katharina Sommer, Associate Director of Government Affairs and Analyst Relations, NCC Group: "Governments do not share the same confidence as organisations when it comes to their collective ability to withstand supply chain attacks. While deregulation is a key priority for governments around the world, supply chain risk is now too significant to ignore. As a result, initiatives to tackle supply chain risks, by using government regulatory and procurement levers, are ramping up."

Some governments are expanding cyber security rules to more explicitly capture key suppliers, such as the EU with NIS2 and DORA, and the UK with its Cyber Security and Resilience Bill. Other governments are creating new obligations for the developers and manufacturers of software and hardware products that many organisations now rely on.

Even in the US, where the Federal Government has been clear in its mission to reduce regulations, President Trump has retained his predecessor's Executive Order 14028 – which set in motion many supply chain risk policy measures.

Verona Johnstone-Hulse, Government Affairs Lead, NCC Group: "With different rules and initiatives hitting different parts of the supply chain, organisations now face the emerging challenge of working out who is responsible for what, and how can they be appropriately held accountable."

How can organisations get a reality check?

Failure to accurately assess risks and overconfidence in supplier security, combined with a lack of proactive and long-term resilience planning, could be leaving organisations open to attack. Many companies are essentially turning a blind eye to mounting supply chain vulnerabilities, leaving themselves exposed to serious financial, operational, and reputational fallout.

So, what can you do now?

Understand your risk profile

It's important to gather a deep understanding of where vulnerabilities lie throughout the supply chain, whether it is a critical dependency on one supplier or a lack of insight into a supplier's cyber security practices. Risk assessments and mapping are essential not only for uncovering weak points but also for challenging assumptions about trusted suppliers, ultimately building stronger, more resilient supply chain cyber security.

Strengthen supplier relationships

By adopting a collaborative and responsive approach, you will be able to develop real trust with your suppliers as they can detect issues earlier and coordinate faster during disruptions.

By deepening your understanding of risk and embedding resilience across your supply chains and supplier relationships, you can better prepare for potential cyber attacks in an increasingly complex threat landscape.

The responsibility gap

There is confusion amongst organisations when it comes to visibility of the threats and the responsibility for mitigating them.

84% of organisations believe that cyber security budgets will increase over the next year

83% of respondents believe they can positively impact their supply chain security posture

62% of respondents say cyber security teams would be responsible for a supply chain cyber incident

57% of CEOs believe that their organisation has full visibility over their supply chain security, compared to 30% of directors

Supply chain security is a shared responsibility that spans every level and function within an organisation. To effectively manage supply chain risk, it is essential that all employees, regardless of their role, understand the part they play and are equipped with the right tools to fulfil their responsibilities.

Despite overwhelming levels of confidence when it comes to supply chain resilience, sentiment surrounding supply chain visibility varies based on job role and seniority. Our data found that those in more senior positions were much more confident that they had full oversight of their organisations' supply chain security compared to other colleagues.

Over half (57%) of CEOs stated that they had full and detailed insight over their supply chain security. In stark contrast, only 30% of director-level respondents and a worrying 18% of team supervisors – potentially those who are working more closely with key suppliers – were completely confident in their organisation's supply chain visibility. This disconnect not only reveals a visibility gap, but also exposes a growing responsibility gap, where senior leaders may feel confident and accountable, yet those closer to day-to-day supplier interactions lack the same assurance. Left unaddressed, this could lead to critical blind spots, weakening an organisation's ability to anticipate and respond to supply chain threats.

Perhaps even more concerning than the gaps between seniority levels are the discrepancies in confidence across departments. When asked about their organisation's visibility into the cyber security posture of their supply chain, less than half (44%) of IT professionals said they had full visibility, despite being on the front line of cyber defence. A further 13% admitted they had only partial insight, lacking the comprehensive detail needed to assess risk. The figures are even starker for procurement teams, who are directly responsible for supplier vetting, onboarding and ongoing management. Only 20% said they had full visibility, while another 20% admitted to having limited detail, and 20% reported significant gaps. These findings point to a troubling misalignment in that the very teams tasked with securing and managing the supply chain do not feel adequately informed. Without cohesive, end-to-end insight across functions, organisations risk overlooking critical vulnerabilities and leaving themselves open to attack.

James Pearce, Commercial Director at NCC Group: "When it comes to supply chain security, people don't know what they don't know. For larger organisations especially, supply chains can span borders and industries, making it extremely difficult for a whole organisation to stay on top on supply chain security."

Ade Clewlow MBE, Associate Director and Senior Advisor at NCC Group: "A lack of shared insight and clear accountability signals a structural risk within organisations – one that can allow critical vulnerabilities to go unnoticed until it's too late. Strong supply chain cyber resilience requires a unified, organisation-wide approach, where visibility isn't confined to senior leadership or technical teams, but embedded across all roles involved in supplier engagement."

How culture impacts security

As supply chains become more complex and cyber threats intensify, a company's internal culture plays an increasingly pivotal role in shaping its overall security posture. How seriously cyber risk is taken, and how well aligned teams are across functions and seniority levels, can determine how resilient an organisation really is.

Our data shows that awareness of growing cyber threats is widespread across organisations, with 70% of CEOs, 73% of managing directors and 74% of junior managers expecting the number and severity of supply chain threats to rise in the next 12 months. This awareness signals a shared understanding of the risks, but it also raises questions about whether this awareness is being translated into coordinated action and shared responsibility.

Company size also appears to influence threat perception. Larger organisations (10,000+ employees) were more likely to anticipate increased threats (74%) compared to smaller organisations with fewer than 1,000 employees (66%). This may reflect differences in resources, visibility, or cultural maturity when it comes to cyber preparedness.

45% of all respondents reported experiencing a data breach in the past year, and 69% anticipated more threats in the next 12 months. This underlines the importance of embedding a culture of cyber security, where responsibility is widely understood and operationalised throughout the organisation.

As Ade Clewlow MBE, Associate Director and Senior Advisor at NCC Group, explains: "We know that board-level culture around cyber security plays a critical role in shaping organisational cohesion and building resilience. When senior leaders take a proactive interest in security posture, and engage closely with those working directly on the ground, they gain a more holistic view of the organisation's defences and the measures in place to mitigate risk. They also build trust and openness, which are vital when preparing for and responding to different threats."

In organisations of all sizes, a strong culture of cyber security is essential to building resilient, secure supply chains. Teams must collaborate across departments, senior leaders should stay connected to operational realities, and everyone needs to understand their role in reducing risk.

Where does accountability lie?

Ensuring supply chain security demands collaboration across departments and seniority levels. It is also important that everyone feels a level of responsibility for this within your organisation and is empowered to act when they need to. Without clear accountability shared across the company, critical security gaps can emerge, reducing your ability to respond swiftly.

When asked who bears responsibility if a supply chain cyber incident affects their organisation, 62% of respondents pointed to their cyber security team. Those in operational roles felt even stronger, with 80% believing that their cyber security team was responsible. Although this isn't entirely surprising, it may indicate a misplaced confidence in a siloed approach to security. Surprisingly, only 21% of all respondents selected procurement, despite their key role in selecting and managing suppliers. Even among procurement professionals themselves, just 44% believed their own team was responsible. This highlights a critical gap in shared accountability, underscoring the need for a more collaborative, cross-functional approach to security.

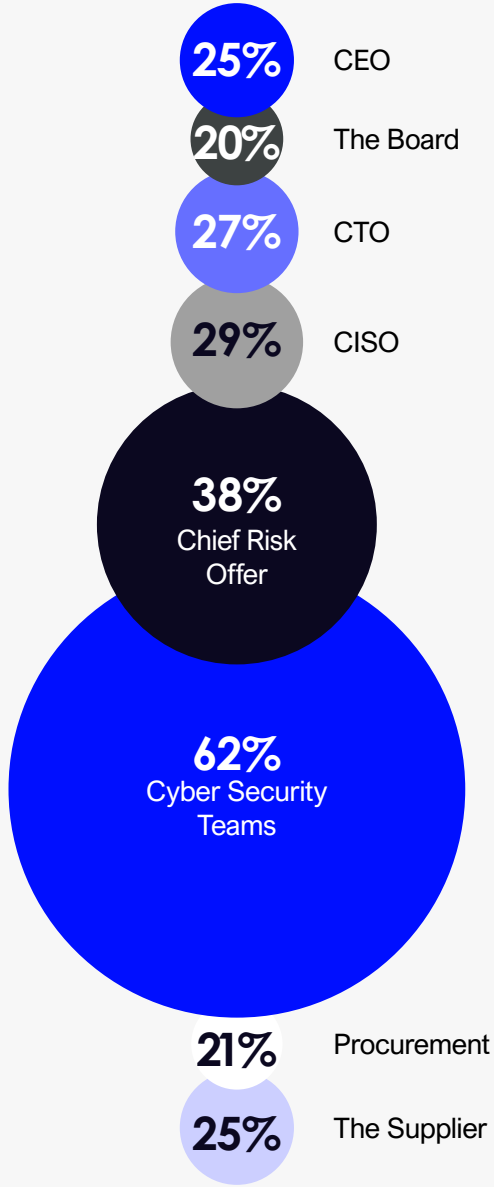
The perception of responsibility also varies at the top. Half of CEOs said their security team was accountable, while 40% cited the CISO and 39% said themselves – a higher proportion than the average, indicating that many leaders do recognise their personal role in safeguarding the supply chain.

Encouragingly, only 2% of all respondents said they thought their organisation could have no impact on improving supply chain security, but confidence in the level of potential impact differs. While 90% of CEOs and 92% of board members believed their organisation could make a difference, this dropped to 64% among procurement respondents and 40% for semi-skilled manual workers. This may reflect a lack of empowerment or understanding at different levels, particularly among those tasked with supplier oversight.

To build true resilience, you must move away from fragmented ownership of cyber security. Everyone from boardroom to back office needs to understand their role, feel empowered to act, and be ready to take accountability when it counts.

Ade Clewlow MBE, Associate Director and Senior Advisor at NCC Group: "It is important that organisations get this right and provide clarity around roles and responsibilities across the company when it comes to supplier security. People need to know how they can help to safeguard the organisation from external threats, and, if the worst should happen, they need to be able to act fast in the areas they are responsible for. Everyone has a part to play and there is no time for excuses or trying to pass the buck."

Who did respondents think would bear responsibility for a supply chain cyber incident?



From awareness to action

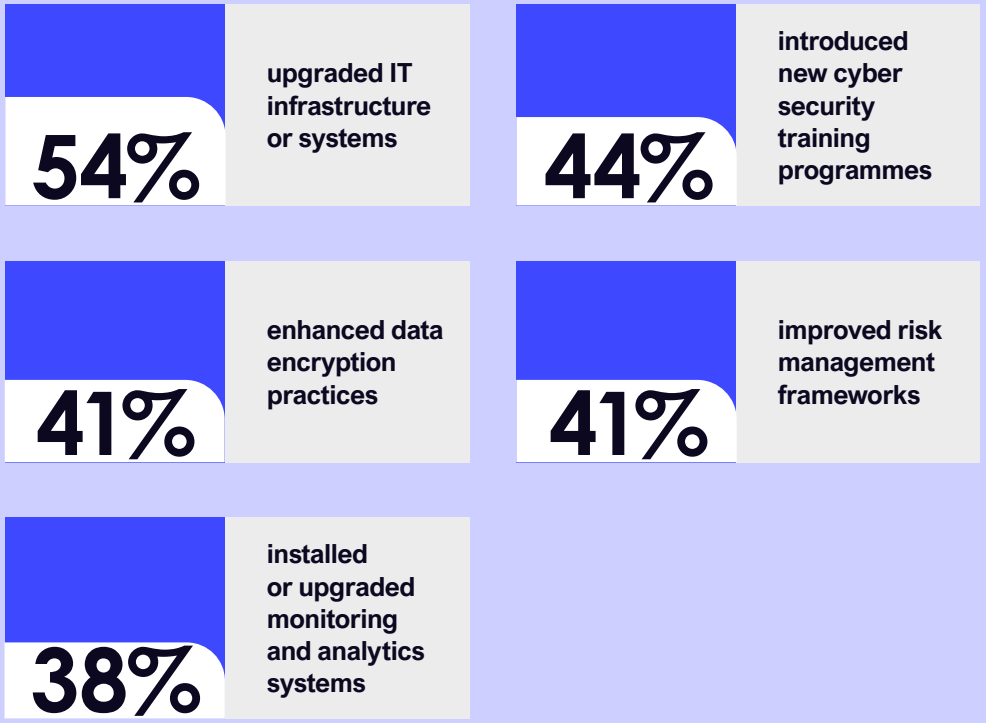
Security is a moving beast, and so continuous analysis of, and investment in supply chain security, is important to help navigate the changing threat landscape. It's also important that these investments, and the reason behind them, are communicated throughout your organisation so that everyone can continuously enhance their knowledge of the evolving threats.

In general, there is good awareness about the need to invest more heavily in supply chain security. More than 80% of respondents expect cyber security spending to rise over the next year (rising to 100% in the energy sector and 89% in IT).

Opinions on where this investment should be targeted does vary based on role and responsibility. When asked about the services they would prioritise to strengthen supply chain security, most board members, including Chairs, favoured continuous supply chain monitoring, such as security scoring (83%). This was also the top choice for owners, proprietors, and founders (70%). CEO's however, said they would prefer to invest in enforcing minimum security standards across their supply chain.

Organisations stated that they have invested in a range of different measures over the last year in an effort to safeguard themselves from supply chain threats. However 20% of semi-skilled respondents were not sure what security measures had been introduced in their organisations in the past year. This suggests that while senior leadership may be making the right decisions at the top, those actions are not always being communicated or embedded across the wider organisation. Without shared understanding, even well-funded strategies can fall short.

Which of the following have organisations introduced over the last 12 months?



To continue to enhance your security posture and keep pace with evolving threats, you must make the right level of investment, in the right places. It is also key to ensure that your strategy for securing the supply chain is understood, aligned, and embedded across every level of the organisation.

How to bridge the gap

Supply chain security isn't just about software and tools, the human side of security is just as important – ensuring that everyone understands their role, and empowering them to make the right decisions.

So, what can you do now?

Make responsibilities clear

Everyone in your organisation should understand the role they play in safeguarding it from cyber threats. Regular department-specific education can go a long way towards mitigating supply chain security risks.

Embed a security culture

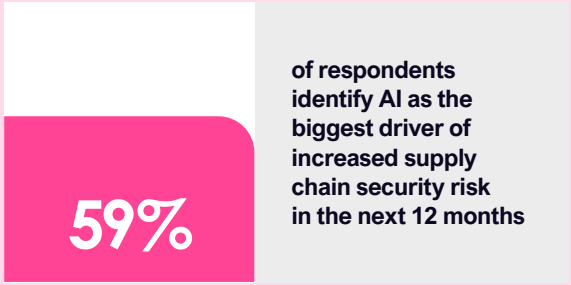
By fostering a culture of proactive cyber awareness, vigilance and continuous learning at every level, you will be able to identify threats quicker and respond faster to any incidents.

Invest and communicate

When investments are made, it is wise to explain the rationale behind them to all relevant colleagues, as this not only helps to enhance understanding of the threats, but also helps you maximise the return on your investment.

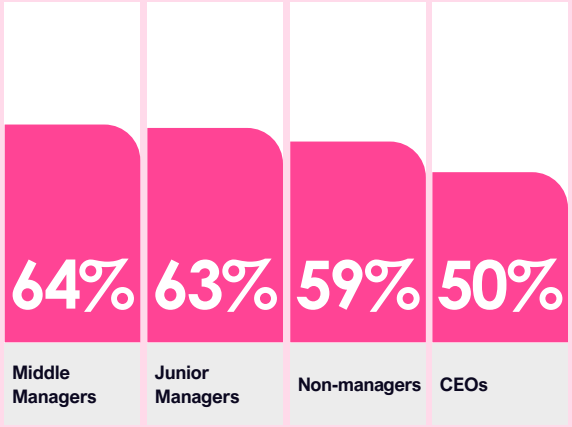
The shadow of AI

Almost every organisation is adopting AI, but how do they know what suppliers are using it for and if it's causing increased risk to their own data?



of respondents identify AI as the biggest driver of increased supply chain security risk in the next 12 months

AI will pose a major threat to supply chain security over the next 12 months, according to:



AI is one of the major technologies taking the world by storm, with 91% of AI-mature businesses appointing a dedicated AI leader, according to Gartner. AI, alongside other emerging technologies, enhances efficiency and scalability, but it also introduces new vulnerabilities that cyber criminals can exploit.

As you and your suppliers continue your AI journey, it is important to understand the myriad of ways it is being used, what data AI bots are gaining access to, and what vulnerabilities this can cause. Each new tool adds another layer to the digital ecosystem, widening the attack surface, obscuring visibility, and creating more entry points for cyber criminals who are using the technology to launch faster, more targeted attacks. For security teams, this adds yet another technology to track, assess, and secure across an already complex third-party ecosystem.

The increasing integration of AI into supply chains introduces a range of risks that are often underestimated as well. AI models are heavily reliant on vast datasets, and are therefore vulnerable to data poisoning, where manipulated inputs can distort outputs and decision-making. Poor data quality can further exacerbate these issues, leading to errors in automation, forecasting, inventory, and logistics. These challenges amplify operational risks and can have cascading effects throughout the supply chain. And an over-reliance on AI-driven automation often reduces human oversight, making it harder to detect anomalies when attackers manipulate input data.

AI models themselves also represent valuable intellectual property, and without proper safeguards, they risk theft, reverse engineering, or unauthorised replication.

Building on shifting ground

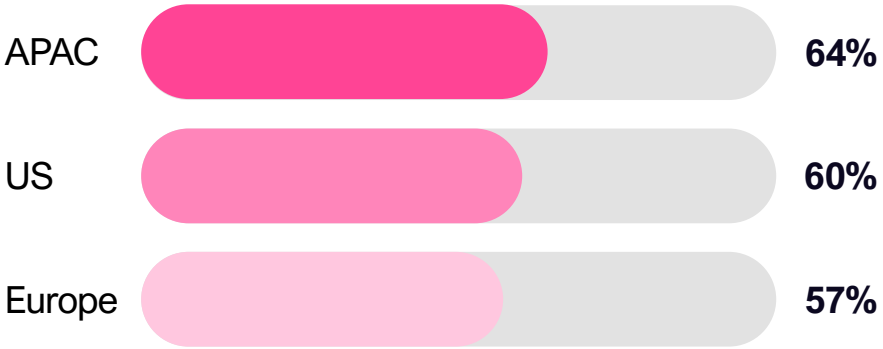
As adoption accelerates, AI is emerging as a key concern, with 59% of respondents identifying it as the biggest driver of increased supply chain security risk in the next 12 months.

Addressing AI vulnerabilities is becoming increasingly difficult, as you and your suppliers may be unaware of how AI is embedded within your systems. With the rise of shadow AI, tools are also often integrated without user knowledge. This makes it much harder for security teams to track usage and assess risks across their organisation.

This lack of visibility creates major blind spots. It complicates compliance with data privacy laws and hinders security assessments, leaving data vulnerable to misuse and allowing security gaps to go undetected. The opacity around AI deployment makes managing and mitigating the associated risks more difficult, increasing the chance of a serious breach happening before vulnerabilities can be identified or addressed.

Which regions are most concerned about AI?

When asked what they thought was the greatest driver of risk over the next 12 months, respondents across the world agreed that it was AI.



The spectre of AI: who is alert?

Respondents across all seniority levels recognise AI as a growing security risk, though perceptions vary by role. CEOs were among the least likely to identify it as the top threat, with just 50% expecting AI to drive the greatest increase in supply chain risk over the next year. In contrast, 64% of middle managers and 63% of junior managers ranked AI as the leading concern. Despite these differences, the data reveals a shared understanding across many organisations of AI's fast-evolving role in shaping supply chain security.

In conversations with the C-suite level of organisations around the globe, we are witnessing AI integration within security measures, while balancing the cyber risks it introduces.

Ade Clewlow, MBE, Associate Director and Senior Advisor at NCC Group highlights that CSOs are concerned about managing AI in supply chains: "Many CSOs recognise the need for AI-driven security measures due to budget constraints and the sheer volume of threats. They're balancing the push for AI security with other pressing cyber risks. To mitigate AI threats effectively, organisations must assess their supply chain exposure to AI and decide whether AI-powered security tools could add value to their organisation."

Beyond security teams, procurement departments are emerging as key players in identifying AI-related risks. Our research showed that procurement was more likely than other departments to see AI as a risk, with 72% expecting risks to increase in the next year. By directly onboarding suppliers that use AI in their operations, as well as those offering AI services and assessing third-party risks, procurement teams are uniquely positioned to identify potential vulnerabilities before they escalate.

72% **of people in procurement see AI as the biggest driver of risk to their supply chain**

AI regulation adds to complexity challenges

AI is clearly a concern and an evolving risk, and with mounting AI regulation, all organisations and their suppliers need to be aware of these updates.

As explained by **Katharina Sommer, Associate Director of Government Affairs and Analyst Relations, NCC Group**, legislation is still catching up with the pace of innovation: "Efforts are being made to establish governance frameworks, but there is still no global consensus on AI security regulations. This creates both challenges and opportunities for organisations trying to implement AI responsibly and monitor how AI is used."

Verona Johnstone-Hulse, Government Affairs Lead, NCC Group adds that the regulatory landscape is still fragmented so organisations need to pay close attention: "Governments worldwide are adopting different strategies to regulate AI security, which will likely impact supply chains. The European Union's AI Act enforces strict compliance measures, while the UK's approach aims to balance security with innovation. These differing strategies create a fragmented regulatory landscape that organisations must navigate carefully."

Global organisations face the daunting task of untangling governments' differing and developing approaches. These are very closely tied to geopolitical and trade relations, and could, effectively, change on a whim. In this uncertain environment, organisations must identify the key stakeholders they need to engage with to plan long-term investments, mitigate risks, and seize the opportunities that AI presents.

A weapon in the arsenal

While our respondents acknowledge AI as a risk, it can also be one of the best tools at an organisation's disposal, improving efficiencies and performance, while also helping to defend against wider cyber risks.

Chris Anley, NCC Group Chief Scientist, explains the critical role AI plays in improving security in modern-day supply chains: "The scale of cyber challenges in complex supply chains is now too great for humans alone. There's no other way forward than to identify effective automated tools and predictive technologies that remove the burden from humans and subsequently enhance supply chain security."

But to turn AI from a risk into a security asset, you need to make sure that your organisation has the right foundations in place. Without proper governance and risk management strategies, the AI risks that many respondents were concerned about could come to fruition. You must assess your AI exposure, monitor supplier use of AI, and establish clear policies to mitigate potential security gaps.

How to stay ahead of the machine

To secure the supply chain in today's rapidly evolving cyber environment, you must take a proactive and strategic approach. While emerging technologies like AI offer powerful tools, they also introduce complex risks, especially when embedded throughout supply chains.

So, what can you do now?

Evaluate supplier use of AI

Stronger oversight of AI usage across the supply chain is now essential. To help guard against the associated threats you should enforce robust security measures and seek to understand how AI-related supplier breaches could affect your operations.

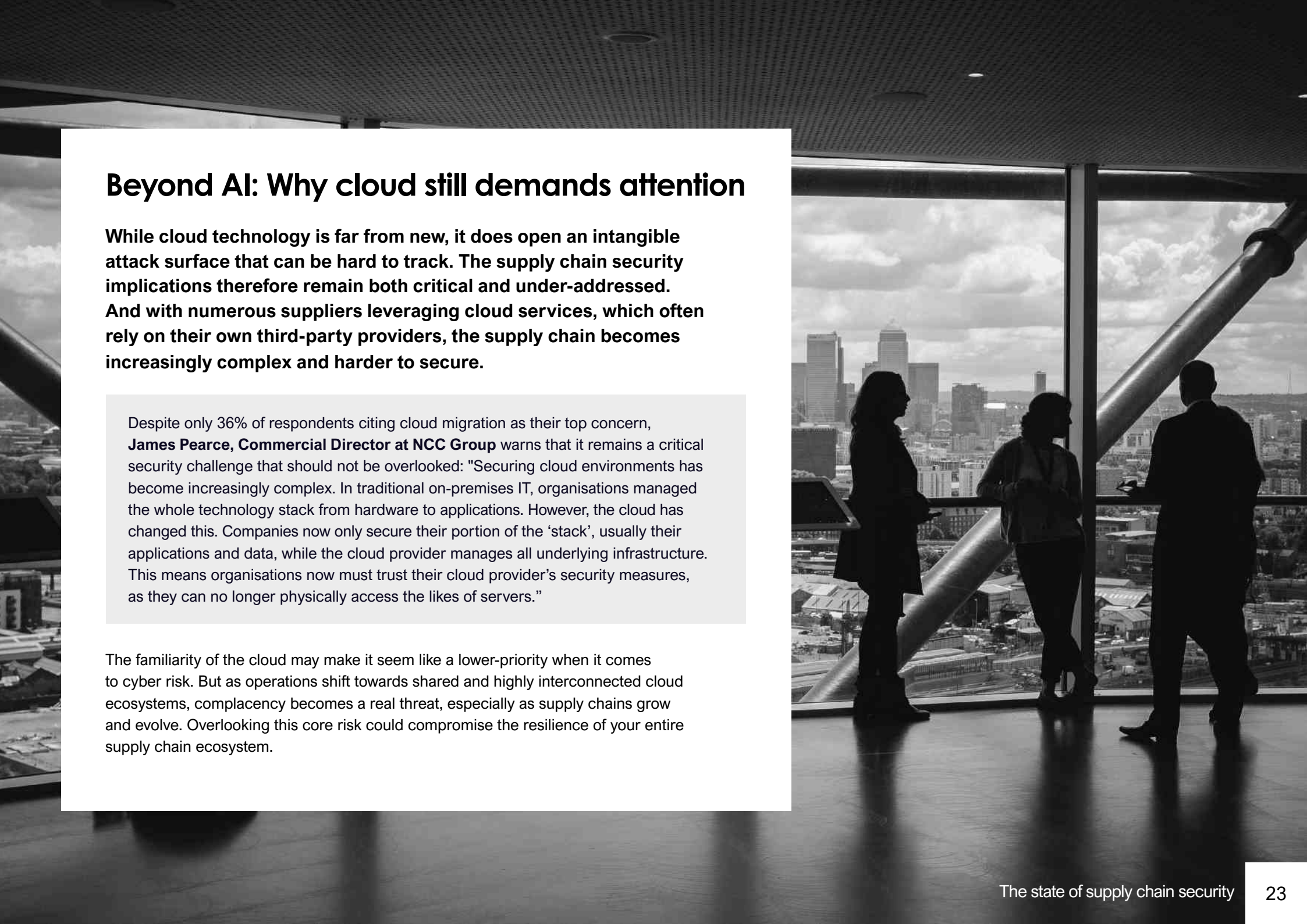
Anticipate AI-driven attacks

From deepfakes to automated social engineering and exploit tools, the threat landscape is evolving. You must prepare for these tactics by stress-testing defences and adapting your security strategies accordingly.

Make AI join the fight

Investing in the right AI-powered security can significantly enhance threat detection and response capabilities, effectively fighting AI with AI. Augmenting security teams with these next-generation tools will also assist them in predicting the likely impact of a cyber attack, across both internal systems and third-party suppliers.

Organisations that fail to proactively address the risks posed by emerging technologies may find themselves unprepared for the next wave of cyber threats.



Beyond AI: Why cloud still demands attention

While cloud technology is far from new, it does open an intangible attack surface that can be hard to track. The supply chain security implications therefore remain both critical and under-addressed. And with numerous suppliers leveraging cloud services, which often rely on their own third-party providers, the supply chain becomes increasingly complex and harder to secure.

Despite only 36% of respondents citing cloud migration as their top concern, **James Pearce, Commercial Director at NCC Group** warns that it remains a critical security challenge that should not be overlooked: "Securing cloud environments has become increasingly complex. In traditional on-premises IT, organisations managed the whole technology stack from hardware to applications. However, the cloud has changed this. Companies now only secure their portion of the 'stack', usually their applications and data, while the cloud provider manages all underlying infrastructure. This means organisations now must trust their cloud provider's security measures, as they can no longer physically access the likes of servers."

The familiarity of the cloud may make it seem like a lower-priority when it comes to cyber risk. But as operations shift towards shared and highly interconnected cloud ecosystems, complacency becomes a real threat, especially as supply chains grow and evolve. Overlooking this core risk could compromise the resilience of your entire supply chain ecosystem.

Global spotlight

Global complexities, regional nuances

As the dust settles from the 2024 election year, newly elected leaders around the world are reshaping cyber security strategies by prioritising stricter regulations, increasing oversight requirements, and introducing mandatory reporting frameworks – adding new layers of operational and compliance complexity to supply chain security.

For example, the UK government has been debating where best to invest spending to improve critical national defences. Meanwhile, with the new Trump administration now in place, and global trading becoming more volatile, supply chains are in a state of flux. And as they become more complex, cyber incidents around the world rise and attack surfaces grow, and organisations are more exposed to supply chain disruptions than ever before.

97%

of US organisations reported confidence in their ability to respond quickly to a supply chain attack

94%

of UK organisations reported confidence in their ability to respond to a supply chain attack

Confidence amid chaos: the US and UK stand out

Against this shifting global backdrop, our research examined how organisations across eight key markets – Australia, Germany, the Netherlands, Singapore, Spain, the Philippines, the US, and the UK – are responding to the evolving threat landscape. The findings revealed differences in visibility, confidence, and investment across regions, driven by varying regulatory maturity, cyber threat awareness, and economic priorities.

Despite facing elevated cyber threats, the US and UK emerged as the most confident markets in managing supply chain cyber risks. Organisations in the US (50%) and UK (41%) reported the highest levels of confidence in their ability to monitor and assess their suppliers' cyber security practices – well above the global average of 33%. In contrast, confidence was markedly lower in the Netherlands (17%), Singapore (26%), and Spain (31%), highlighting a significant regional disparity in supply chain visibility.

Preparedness to respond to supply chain cyber attacks was also highest among US (97%) and UK (94%) organisations, slightly above the global average of 94%. This suggests that organisations in both countries are confident in the investments they've made to improve supply chain security.

This confidence persists even in the face of a heightened threat landscape. According to our Annual Threat Monitor Report, North America accounted for 55% of all global ransomware attacks in 2024, making the US one of the most targeted countries worldwide. This may help explain why 91% of US organisations also believe that their overall spending on cyber security will increase in the next year.

Verona Johnstone-Hulse, Government Affairs Lead, NCC Group:
"With the changing US administration this year and Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) on the horizon for 2026, US organisations are navigating multiple changes to cyber regulation. This could be directly contributing to the heightened awareness of cyber threats to US supply chains. The UK has also undergone a change in government over the past 12 months, and the emphasis on boosting national defences aligns with the UK's increased investment in cyber security."

APAC concerns reflect diverse threat perception and priorities

Across the APAC region, our findings revealed significant variation in how organisations perceive and prioritise supply chain cyber security, shaped by differing threat environments, technological concerns, and strategic focuses.

The Philippines

Organisations in the Philippines reported the lowest confidence globally in their ability to respond swiftly to a supply chain cyber attack, with 88% expressing readiness – well below the global average of 94%. At the same time, they stood out for their heightened concern around emerging technologies with 80% of respondents stating that artificial intelligence was the single greatest threat to supply chain security, far ahead of other markets. This suggests a strong awareness of how AI could be weaponised to launch more sophisticated and harder-to-detect attacks.

Australia

Organisations in Australia emphasised supplier transparency as a key component of a resilient supply chain, with 57% of respondents identifying it as the most important factor when assessing suppliers' security posture. Australia, along with the Philippines, also led the way in investing in awareness and training for suppliers, highlighting the need for continuous capability-building across the supply chain.

Singapore

In Singapore, two major concerns dominate the supply chain security agenda: limited visibility and the cost-effectiveness of cyber security measures. More than three-quarters of respondents (76%) cited concerns about supply chain visibility – significantly higher than the global average (59%) and the APAC regional average (64%). Additionally, 56% of organisations in Singapore identified cost-effectiveness as their top priority, highlighting a need to balance improved security with financial constraints. This dual pressure may mean that while organisations are aware of their exposure, they must carefully justify every investment.

88%

of organisations in the Philippines believe they can respond quickly to a supply chain attack

57%

of organisations in Australia say supplier transparency is the most important factor when assessing suppliers security posture

56%

of organisations in Singapore identified cost-effectiveness as their top priority

Spain and the Netherlands: high exposure, low confidence

Despite facing some of the highest levels of cyber threat, organisations in the Netherlands and Spain report low confidence in securing their supply chains and limited investment, revealing a concerning disconnect between risk and readiness.

Spain

In Spain, 48% of organisations experienced a cyber incident over the last year and around 31% reported having full visibility over their supply chain's cyber security – massively trailing behind the likes of the UK and US. A key barrier appears to be budget-related, since more than half (53%) of Spanish respondents said the cost of cyber security is one of the greatest challenges when it comes to improving supply chain resilience. This aligns with a broader global trend, where the financial burden of implementing effective measures remains a top concern.

The Netherlands

In the past 12 months, 53% of Dutch organisations experienced a cyber attack or breach – the highest rate among all surveyed countries. Yet, only 17% say they have full and detailed visibility of their supply chain's cyber security, revealing a significant lack of insight that could leave them exposed. Even more concerning, just 75% expect cyber security spending to increase – the lowest projected investment level across the markets surveyed. These figures suggest that while Dutch organisations are highly exposed, they may be falling behind on both monitoring and mitigation efforts.

53%

of Spanish organisations say cost of cyber security is a major challenge when it comes to mitigating supply chain risk

17%

of Dutch organisations believe they have full and detailed visibility of their supply chain security

Regulation vs cyber threat

Worldwide, governments are recognising the increasing cyber threat. Our Annual Cyber Threat Monitor Report for 2024 found that last year was a record breaker, with the highest-ever levels of ransomware attacks.

Governments are responding by expanding the scope of regulation – for example, through the EU's NIS2 Directive, DORA, and the UK's Cyber Security and Resilience Bill – and placing greater emphasis on collective responsibility for resilience across complex supply chains.

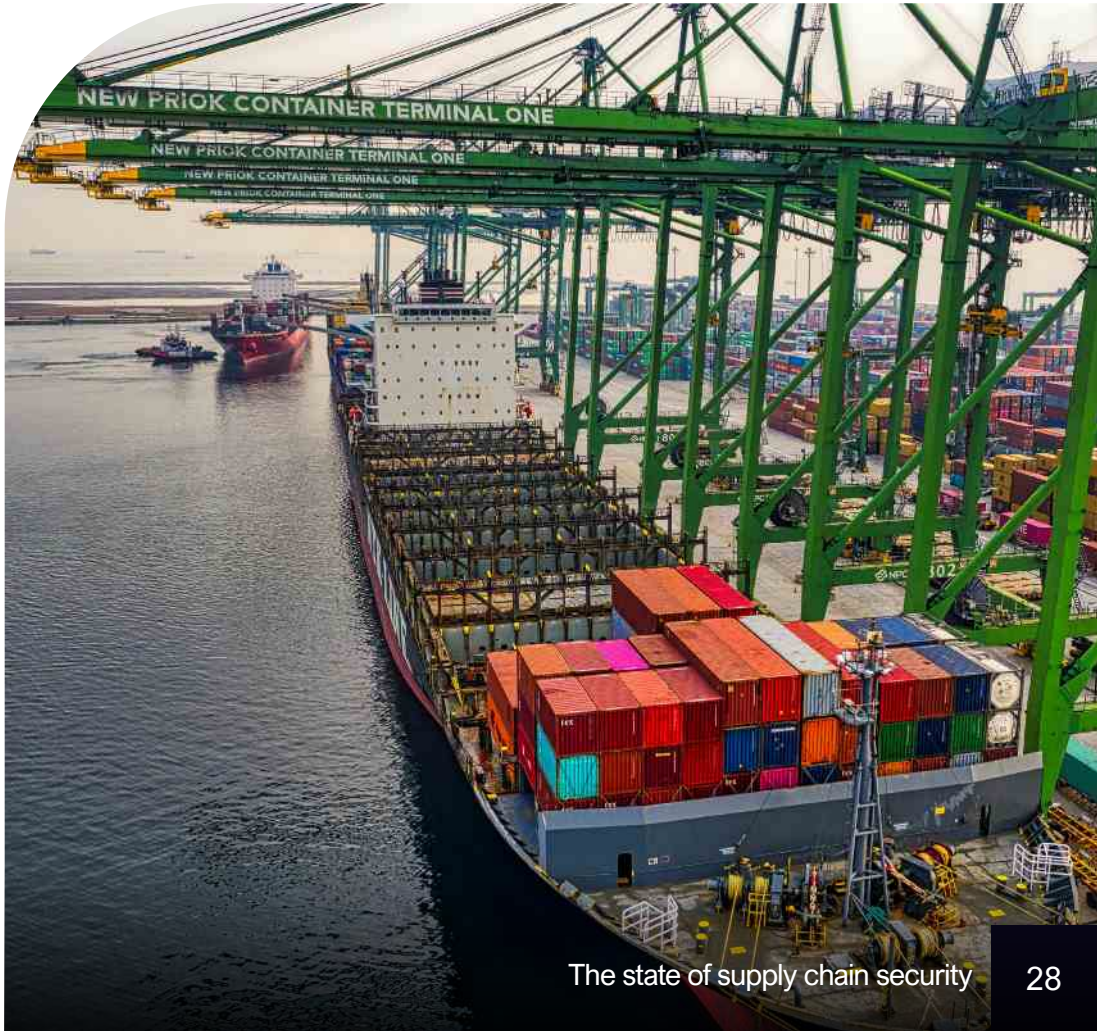
This regulatory focus is positively received by industry. Across the eight markets surveyed, over 90% of respondents expressed confidence that current cyber security standards and regulations effectively reduce the risk of supply chain attacks. This indicates strong trust in the newly introduced regulations aimed at combatting cyber threats.

However, governments and organisations are facing an ongoing battle, with two-thirds of organisations expecting supply chain cyber attacks to worsen over the next 12 months.

Matt Hull, Global Head of Threat Intelligence at NCC Group:
"Increasing ransomware levels are having a domino effect on the supply chain, causing huge pain for interconnected operations. We have seen a steady uptick in levels of cyber crime over recent years, and as threat groups become more sophisticated in their techniques, organisations must match their level of proactivity."

A need for global collaboration

As global supply chains become more intricate, spanning regions and jurisdictions, monitoring supply chains – and suppliers' suppliers – has become a huge undertaking. It is critical that regions become more joined-up in their approach to supply chain security. Further collaboration, at a political, regulatory and industry level, can help to embed good supply chain security practices throughout chains that span multiple nations.



Five steps to enhance supply chain security

Gone are the days where your focus can be solely managing your own cyber security risks. You must now also consider the security of suppliers across various sectors and borders, all of which are adopting new and fast-evolving technologies.

Without a shift in mindset and increased understanding, you are risking a supplier security crisis, where one weak link in the chain could trigger a domino effect, disrupting operations and damaging trust.

Addressing these risks requires swift action, beginning with five critical steps.

1. See the full picture
2. Break the silence
3. Fortify the chain
4. Anticipate the impact
5. Close the gaps

1 See the full picture

Map the hidden depths of your supply chain

Start by gaining comprehensive visibility across your entire supply chain. Your organisation's security is only as strong as its most exposed supplier, no matter where they sit in the network.

Ask yourself: do you know which suppliers have the most access to your systems? Are they adequately protected? And what continuity measures are in place? Do they offer meaningful SLAs for things like support and uptime? And, how well do they handle patching and support?

The scale of modern supply chains is staggering. For example, a typical automotive manufacturer may rely on 250+ tier-one suppliers, but the total number of suppliers in the chain can near 20,000. When you then consider your suppliers' suppliers' suppliers, these extensive networks present multiple points of entry for cyber criminals, dramatically increasing exposure.

Without full visibility across all tiers, critical vulnerabilities can remain hidden. And while it may not be feasible to control every link in the chain, organisations can still take proactive steps to improve their own awareness of risk. Collaborating with suppliers and their cyber security practices is not just a compliance exercise, but it's part of a long-term commitment to secure shared outcomes.

Questions to ask when selecting suppliers

Here are some questions you can use to assess a potential supplier's level of operational resilience and compliance:

Configuration and responsibility

- Who sets up and maintains your systems?
- Are secure defaults and best practices (e.g. no default creds, segmented networks) enforced?

Vulnerability disclosure and patch management

- Is there a formal vulnerability disclosure process and patching timeline?
- How are relevant vulnerabilities assessed and communicated to customers?
- Are updates regular, tested, and auto deployed, or left to customers?

Compliance and standards

- Is the solution aligned to standards (IEC 62443, ISO 27001, GDPR, NIST CSF)?
- Can you provide evidence of certification or conformance?

Operational and support considerations

- Are SLAs clearly defined, and are support staff trained and vetted?
- Is up-to-date documentation available for secure configuration and response?

Long-term viability

- What's the contingency if you, or key systems you operate, are no longer supported?
- Are there fallback options (e.g. escrow, warranty, support extensions)?

Risk-based approach

- Has an inherent risk triage been conducted to scope due diligence depth and frequency?

2 Break the silence

Embed supply chain security throughout your organisation

Given their complexity, supply chains can harbour hidden vulnerabilities at every level, from primary suppliers to smaller, often overlooked vendors. Employees may unknowingly host shadow AI software or unapproved tools, quietly expanding the supply chain and exposing the organisation to a range of threats. This makes it imperative to integrate awareness of supply chain security into the culture of your organisation.

Embedding conversations about supply chain security into everyday practices will help to normalise the topic and take steps to communicate it as a shared responsibility, rather than being solely the concern of senior leaders and IT professionals. Effective monitoring of supplier compliance becomes easier, and communication is strengthened across departments, ensuring all teams remain alert to potential risks.

In large organisations, the collective vigilance of a well-informed workforce is far more effective than relying solely on a few key leaders to spot and manage every risk. Bridging the gap between executive confidence and operational awareness is crucial to avoiding supply chain vulnerabilities.

3 Fortify the chain

Strengthen supplier contracts before the storm hits

Supplier contracts are a vital component in mitigating cyber risks. With the threat landscape evolving at pace, you need confidence that contracts are keeping pace with new risks and international compliance standards.

While vulnerabilities may not always be immediately visible, robust cyber security measures must be part of the supplier onboarding process. Incorporating controls such as Cyber Essentials should be the minimum to ensure suppliers meet basic cyber security standards.

Due diligence is critical. This includes using tools such as security scorecards and questionnaires to assess the cyber security maturity of potential suppliers. These evaluations should require evidence of compliance, either through self-attestation or third-party audits. Beyond due diligence, you should take steps to establish direct, proactive lines of communication with key contacts at each supplier. This is particularly important for large organisations, where suppliers may only be accessible via an email or chatbots. This will make a significant difference in ensuring rapid, transparent action in the event of a security breach.

4 Anticipate the impact

Build a resilient security posture before it’s tested

Cyber disruptions can have a profound impact on an organisation, and it's no longer enough to just react; you need to invest in the right resources, collaborate with experts, and adopt a forward-thinking, zero-trust approach to limit access to only those who need it.

AI is also reshaping supply chain operations, as with new technologies come new threats – shadow AI, unvetted third-party models, and unmonitored automation, all of which can quickly outpace traditional security measures. You must ask: are our defences strong enough to tackle these emerging threats? And are we compliant with the most up-to-date regulations?

A well-defined incident response plan is also essential. You should have a clear process for identifying, addressing, and recovering from breaches, especially when it comes to supply chain risks and potential phishing attacks.

Regularly reviewing your security posture and adopting a proactive, comprehensive approach to security, rather than just ticking boxes, is key to safeguarding today’s operations against tomorrow’s cyber threats.

5 Close the gaps

Unite internal and external forces for stronger defences

While external cyber security experts offer valuable insights and manpower, you must retain in-house capabilities to monitor supply chain security on an ongoing basis. Maintaining internal expertise provides an important level of security, ensuring that you are not solely reliant on vendors.

That’s not to say that all resource should be kept in-house. Collaboration with external experts, who bring specialised knowledge and timely threat intelligence, is vital to stay ahead of the curve and should complement in-house resources.

This balanced approach will enhance the ability to monitor and manage supply chain risks effectively, ensuring businesses are well-positioned to handle new and evolving threats.

Final thoughts

Mike Maddison
CEO, NCC Group

Effective supply chain management, especially when it comes to cyber security, requires expanding your field of vision. Much like efforts to eliminate modern slavery or trace product provenance, cyber risk is often hidden in the shadows. We need to bring more of the iceberg above the surface, while actively addressing the threats lurking below.

Our research reveals three critical themes that show just how much of supply chain security remains out of sight:

Complacency is a ticking time bomb

Despite growing complexity and interconnectivity, many organisations are placing too much faith in compliance. Attackers have identified this vulnerability and have the first mover advantage – organisations must play catch up.

Leadership disconnects are undermining progress

Gaps in awareness between senior leaders and operational teams are leaving organisations exposed. Cyber resilience can't be delegated or siloed, it demands a culture of openness, shared responsibility, and collaboration.

AI is reshaping the threat landscape

While awareness of AI-related risks is growing, action is lagging behind. Without clear oversight of how AI is used, internally and across the supply chain, organisations are vulnerable to data poisoning, model manipulation, and AI-driven attacks.

So, what now?

It's time to move from awareness to action. That means going beyond your own perimeter, scrutinising your supply chain exposure, building stronger partnerships, and holding suppliers to clear, enforceable standards.

Cyber threats targeting supply chains are intensifying. As complexity grows and attackers become more sophisticated, the cost of inaction will only rise. Organisations can no longer afford to leave the back door open.

Supply chain cyber security must be a board-level priority. Because if you fail to act now you may find yourself at the centre of the next major breach – with the impact not limited to your organisation, but reverberating across your supply chain.

And if you need support navigating these risks, our global team of experts is here to help.

Mike Maddison
CEO, NCC Group

Immediate actions

1. **Map the hidden depths of your supply chain**
2. **Embed supply chain security throughout your organisation**
3. **Strengthen supplier contracts before the storm hits**
4. **Build a resilient security posture before it's tested**
5. **Unite internal and external forces for stronger defences**

The key takeaway

Don't assume that your supply chain security is in hand

Our advice to leaders is clear: don't be complacent, but don't panic. The risks facing today's supply chains are unprecedented, and the time to act is now. By following the steps outlined here, you can properly safeguard your operations and ensure continuity, even when surrounded by a myriad of evolving cyber threats. The consequences of inaction are simply too great to ignore.

Methodology

In 2025, NCC Group conducted a global survey of cyber security decision-makers about their views on the current state of supply chain security.

The data was collected from 1,010 people with joint or sole responsibility for cyber security in businesses with 500 – 10,000+ employees.

The survey included 26 questions which explored sentiment towards the resilience of the global supply chain ecosystem and how prepared individual businesses felt to deal with the growing risk of a cyber attack.

Data pool

The organisations we surveyed were split between both the public and private sector, including those selling goods and services to businesses and consumers.

To understand sentiment towards supply chain security across every level of an organisation, we surveyed all seniorities, from CEOs and board members to more junior members without managerial responsibility, and every level in between.

The results were also split by departments including business, finance, human resources, IT, research and development, operations, sales and marketing, and procurement.

Markets and industries

Supply chains are global, and our survey reflected their scale. Respondents were based in eight different markets across the world, including Australia, Germany, the Netherlands, Singapore, Spain, the Philippines, US and UK.

As well as a range of markets, we also gathered responses from 11 different industries, all with vast supply chains, including energy, materials, industrials, consumer discretionary, consumer staples, healthcare, financials, information technology, communication service, utilities, and real estate.

Under attack?

Call our **24/7** Incident Response Hotline now.

UK & Europe
+44 331 630 0690

U.S. & Canada
(855) 684-1212

Australia
1800 975 310

Singapore
+61 2 8379 7870

Fox-IT – Benelux
0800 369 23 78 (NL)
+32 2304 22 16 (BE)
+31 (0) 88 369 23 78 (Int)

We are here for you

Contact us today to learn more about securing your organisation and supply chain.

UK & Europe
+44 (0) 161 209 5200

U.S. & Canada
+1 (800) 8123 3523

Australia
+61 (0) 2 9552 4451

Singapore
+65 6800 0950

Fox-IT – Benelux
+31 (0)85 799 0680 (NL)

Philippines
+63 2 8540 9450

nccgroup.com/the-state-of-supply-chain-security