CyberSmart

The CyberSmart NIS2 Survey

Key findings on EU & UK readiness

Executive Summary

Overall compliance with NIS2 across Europe and the UK is low. This appears to be down to a few key factors, most prevalently budgetary constraints and confusion or a lack of guidance on how to implement the measures.

However, this doesn't mean that most businesses don't see the value in regulation. In fact, the majority of our respondents not only see the value in cybersecurity regulation, many are also spending more than insurers recommend on compliance. This is despite clear fatigue at the number and complexity of regulations EU and UK businesses have to comply with.

For MSPs, this offers a clear opportunity. Businesses across Europe and the UK need help managing year-round compliance. Not just NIS2, but with a range of other regulations, including DORA, PCI-DSS, the UK's Defence Cyber Certification and ISO 27001. For those ready to take it, there's a clear opening to help businesses across the continent get on top of regulatory requirements, implement year-round compliance, and move towards a culture of cyber resilience.

Introduction

Cybersecurity regulation has undergone a transformation in the last decade. Early regulations, such as the UK's *Computer Misuse Act (1990)*, were heavily focused on criminality and were, for the most part, punitive rather than preventative. Even well into the twenty-tens, legislators were still taking a largely laissez-faire approach to the security standards businesses were expected to meet, and most schemes were voluntary, for all but the most highly regulated industries.

However, the last decade has seen governments across the globe begin to take a different approach. Regulations like the EU's Network and Information Security Directives 1 and 2 (NIS2), the Digital Operational Resilience Act (DORA) and the UK's Cybersecurity and Resilience Bill all signal legislators moving towards preventative tactics that place far greater obligations on critical national infrastructure (CNI) providers, businesses and their supply chains.

The reasons for the increased regulatory scrutiny are simple enough. According to the UK's National Cyber Security Centre, 2024 was a record-breaking year for attacks on critical national infrastructure. And while it's a little early in the year for figures from 2025, many industry analysts predicted last year would be even worse.

This is coupled with 2025 being the year of highly disruptive cyber incidents across Europe. The UK saw huge disruption to several major retailers, including those providing essential goods such as supermarkets and a breach at one of the UK's flagship companies in Jaguar-Land Rover, set to cost the UK government £2.6bn. Meanwhile, in Europe, the MUSE/Collins Aerospace ransomware attack brought airports across the continent to a standstill and breaches at Orange Belgium and Allianz put millions of citizens at risk.

The rationale for greater regulation is clear. However, despite regulations like NIS2 and DORA having passed into law, compliance has been a slow burn. As of late 2025, some eight EU countries had failed to transpose NIS2 into law, in defiance of a deadline of October 17 2024.

Perhaps unsurprisingly, this stasis and confusion also seems to be affecting businesses. In the UK, a large minority of businesses that fall within the scope of NIS2 (22%) claimed not to know whether the new directive applies to their business. Worse still, 10% of businesses that confirmed that NIS2 does apply to them admitted that they weren't compliant as of the October 2024 deadline.

Meanwhile, in the EU itself, ENISA (the European Union Agency for Cybersecurity) was worried enough to issue a warning to six CNI sectors that had fallen behind in NIS2 compliance in early 2025. In addition, some 96% of EU financial companies admitted their current level of data resilience falls short of DORA compliance, according to a Veeam report.

This all begs the question, why are businesses across Europe struggling to comply with regulation? Is this the natural lag in compliance expected with any new regulation? For example, it took some years for the EU's GDPR to reach widespread adoption.

Alternatively, is there something else at play? Perhaps businesses consider the regulations too onerous? Or, maybe, many business leaders simply haven't received the guidance they need on how to comply.

We set out to answer these questions by commissioning a survey of business leaders across the UK and EU in late 2025. Focusing on NIS2 – due to its widespread applicability – we sought to get to the bottom of why organisations are struggling to comply, how they're managing compliance, and what governments and the cyber industry can do to help.

What follows are the results of this study, providing insight into how businesses across Europe are tackling regulatory compliance in 2026.

Methodology

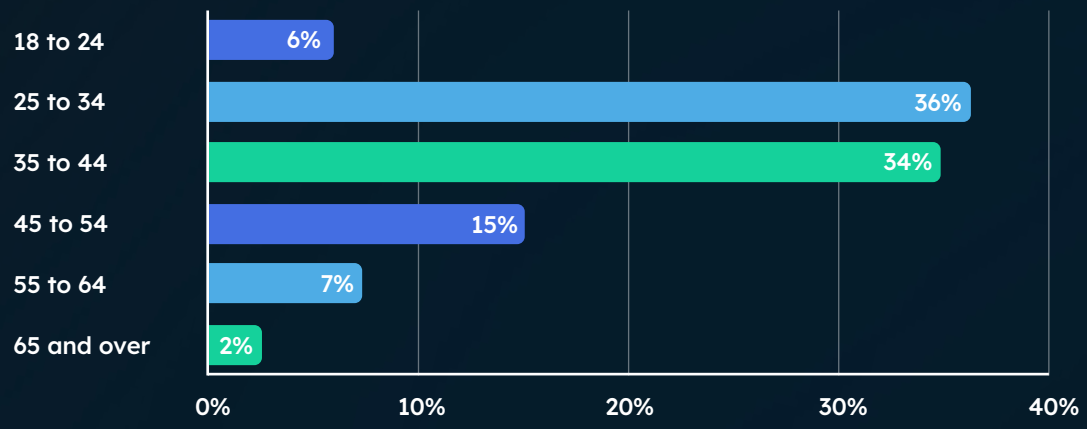
Before we get into the results, a word on methodology. We wanted this survey to be as representative as possible, so we conducted this survey with 670 business leaders from key European economies in the UK, Poland, the Netherlands, Ireland, France, Germany, Italy, Denmark, and Belgium (see figure below)

Where do you live?

Response count 670

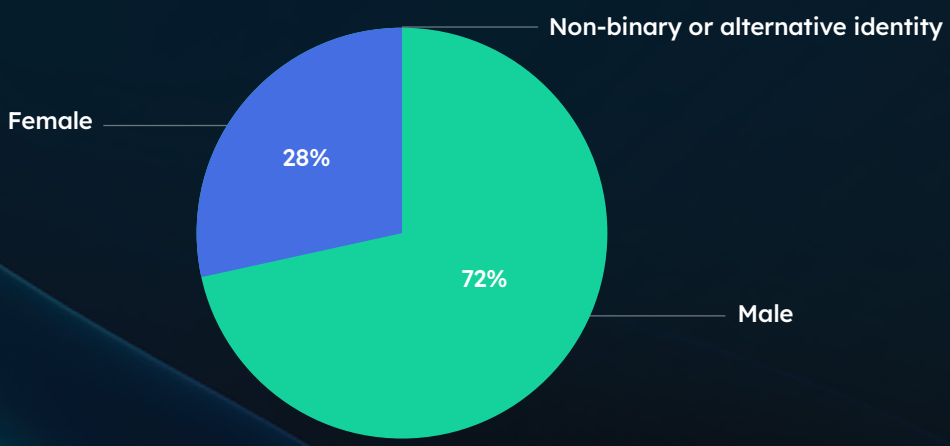
These business leaders came from across the age and gender spectrum. Although reflective of the sectors' business leaders, they skewed heavily male (72%) and between the ages of 25 and 54 (85%).

What is your age?



Response count 670

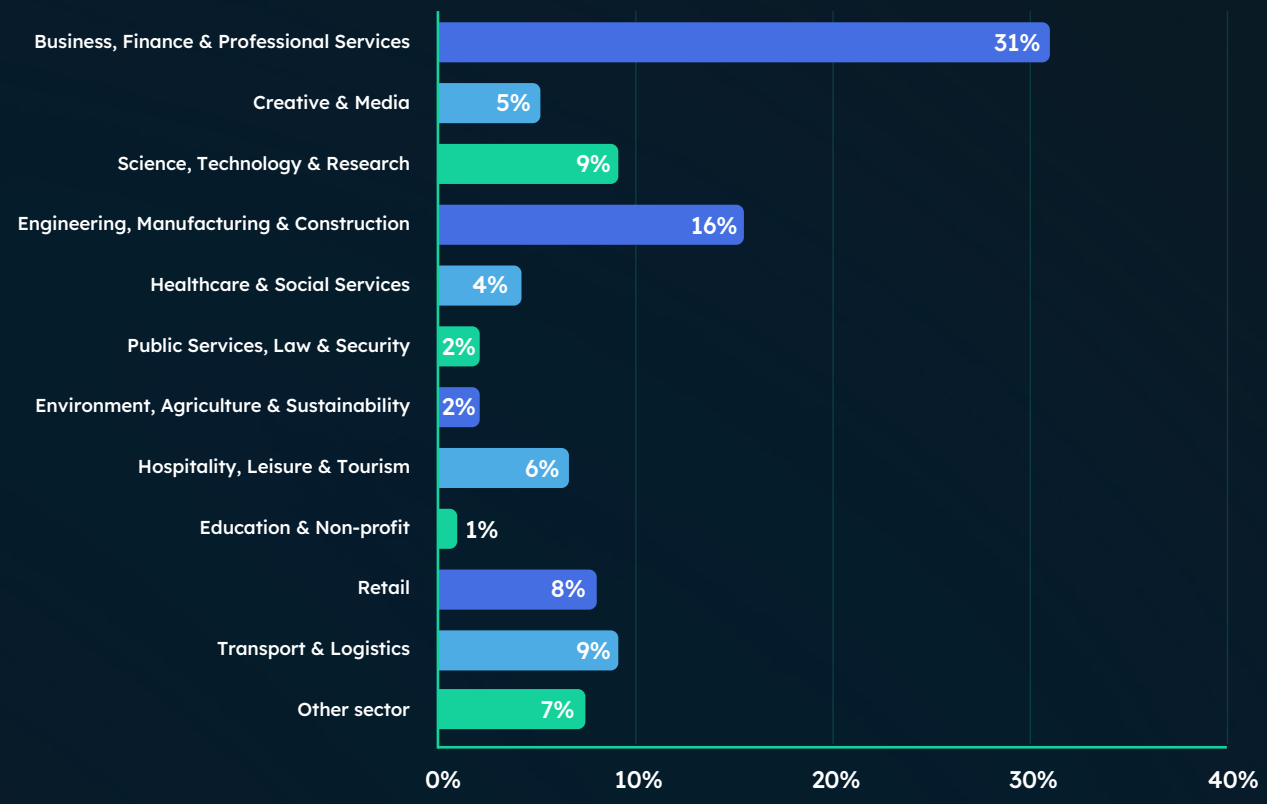
Are you...?



Response count 670

We also drew our results from a variety of industries, from finance to transport and logistics.

Which sector do you work in?



Response count 670

Finally, we only surveyed small businesses for whom NIS2 applies, that is:

- Companies defined as “important entities” with 50 to 249 employees or with a turnover greater than €10 million
- Managed service providers (MSPs) who work within the EU
- UK businesses that do business with EU entities and fall within the scope of NIS2

Businesses are following some of the measures laid out in NIS2

1. Which, if any, of the following measures have you put in place to comply with NIS2? [Select all that apply]

Response count 670

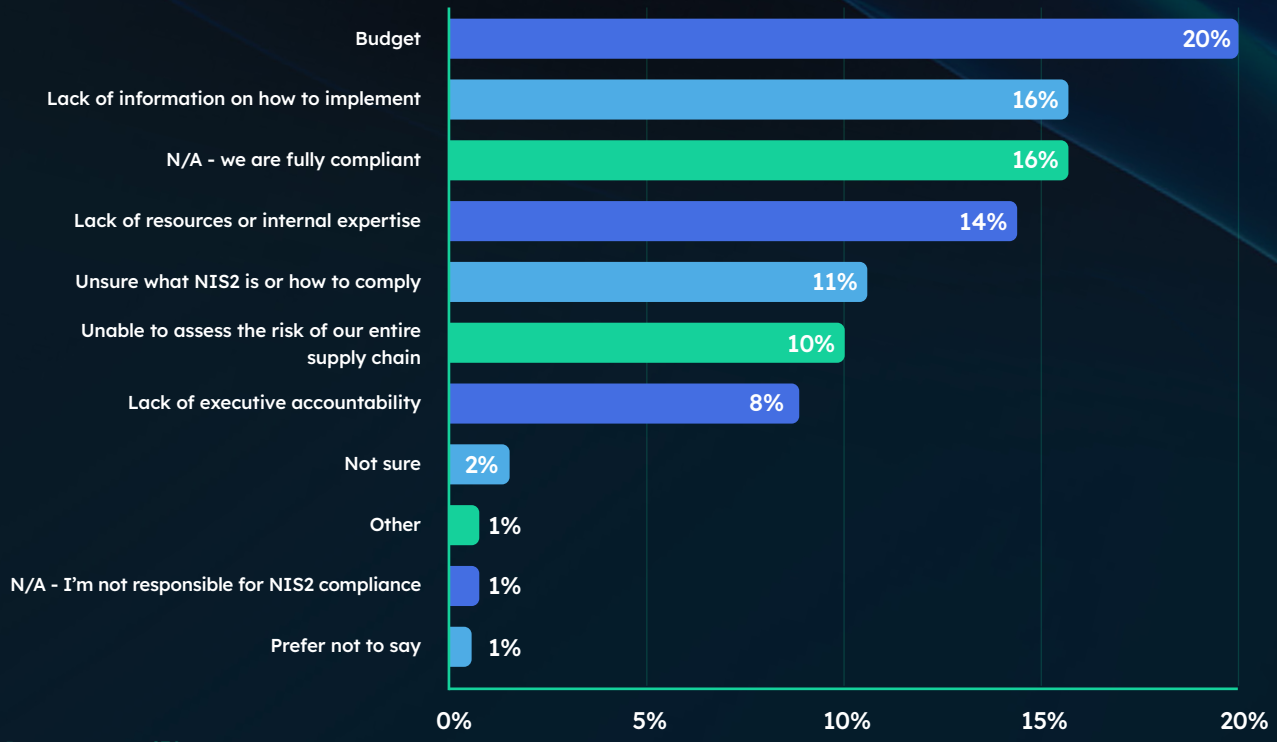
Let's begin with the positives. It's heartening to see that most organisations are implementing at least some of the cybersecurity controls mandated by NIS2. For example, that 44% of businesses are providing employees with mandatory cybersecurity training, 37% have implemented data encryption, and 35% plan to conduct regular risk assessments represents a real positive.

Likewise, just 3% of companies have implemented none of the listed measures or any at all. This demonstrates that the majority of businesses are taking cybersecurity seriously enough to put in place essential cybersecurity controls. Were we to have asked them the same survey question ten, or in some cases five, years ago, the answers likely would have been very different, which represents progress.

Nevertheless, it's worth sounding a note of caution. Organisations implementing some of the cybersecurity measures laid out by NIS2 doesn't mean they're implementing all of them. Nor, as we'll see, does this mean that businesses are necessarily compliant with NIS2. In fact, most of the measures listed are fairly common security protocols that have been recommended by governments, MSPs, and the wider cyber industry for some time, suggesting they're being applied independently of regulation.

Full NIS2 compliance is low

2. If you haven't fully complied with NIS2, what is the main reason? [Select one]



Response count 670

Following on from our previous section, our findings on full NIS2 compliance are alarming. Of our 670 business leaders, just 16% (108) were confident their organisation is fully compliant with the requirements of NIS2. Given that all our respondents are required to be compliant with NIS2, this is a staggering figure.

Worryingly, budgeting concerns (20%) were the leading reason for non-compliance. The last few years have been tough for all businesses due to the economic outlook, so it's not necessarily a surprise to see compliance lagging as leaders battle tight budgets and a lack of resources. However, what is troubling is that this would appear to suggest that for some businesses NIS2 compliance isn't seen as "essential" or something that must be budgeted for.

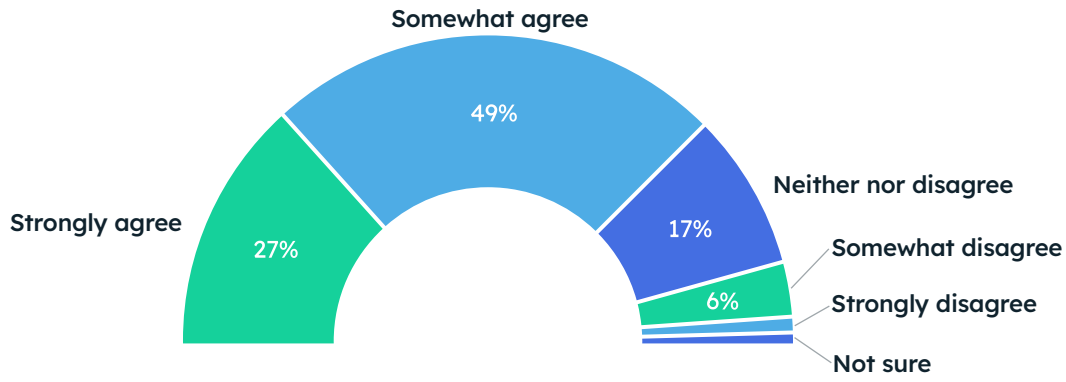
Alongside this, there seems to be real confusion on how to comply with NIS2. 16% of respondents cited a lack of guidance on how to implement the measures, 11% cited a lack of internal expertise and resources, and a further 11% were unsure what NIS2 is. Unlike the thornier issue of budgetary restraints, this is likely a simple issue of under-promotion by states and a lack of clear guidance – something MSPs and the cybersecurity industry can assist with, but more on that later.

Lastly, the other major reason is businesses' inability to assess the risk of their whole supply chain (10%). This speaks to a wider problem with inter-organisational assessment and cooperation across supply chains. Indeed, as recently as 2024, the NCSC revealed that only around **1 in 10 businesses** were adequately assessing suppliers' security measures.

Businesses do see the value in NIS2

It might sound counterintuitive, given our findings on non-compliance, but our survey reveals that businesses do see the value in NIS2. The majority of respondents recognised both the competitive advantage it offers and the importance of avoiding the repercussions for non-compliance.

3. To what extent do you agree or disagree with the following statement: "There is a competitive advantage to NIS2 compliance"?



Response count **670**

Three-quarters (75%) of respondents noted that there is at least some competitive advantage to NIS2 compliance. Meanwhile, nearly a third (27%) strongly believe that there's a competitive advantage.

4. Which, if any, of the following repercussions for non-compliance to NIS2 worries you most? [Select up to two]

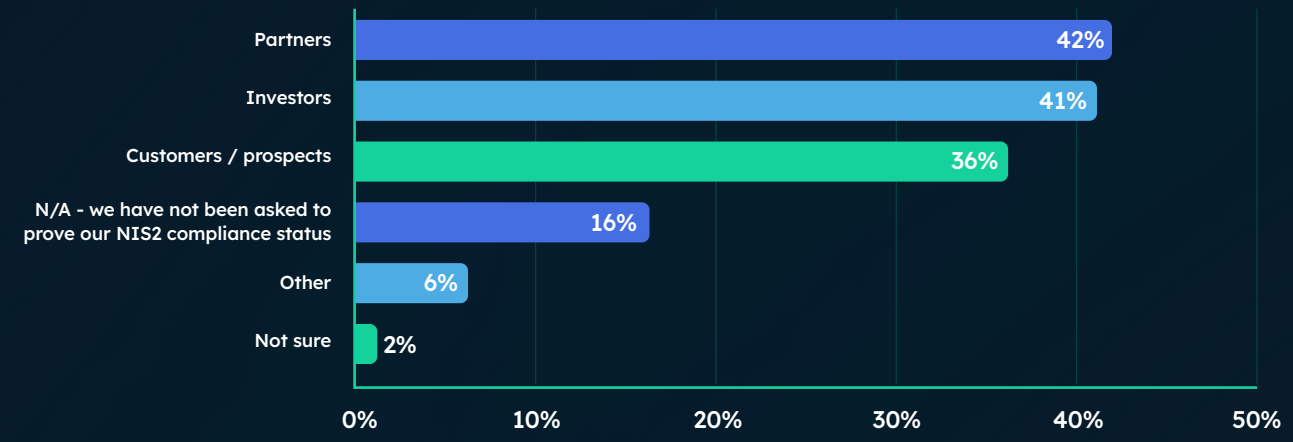
Response count 670

The same is true for the repercussions of non-compliance, with just 3% of our respondents declaring they have no concerns. Interestingly, the three most feared repercussions were operational and reputational in nature, rather than legal. Loss of productivity (18%), reputational loss (18%) and loss of customers (18%) all ranked higher than fines (16%) or legal repercussions (14%).

These findings seem to suggest that non-compliance with NIS2 isn't because most businesses don't see the value in the regulation. This reinforces our earlier findings that the biggest barriers to compliance are the perceived cost and uncertainty about how to implement the requirements.

Businesses are being asked to prove compliance

5. As part of the due diligence process, who, if anyone, have you been asked by to prove your NIS2 compliance status? [Select all that apply]



Response count 670

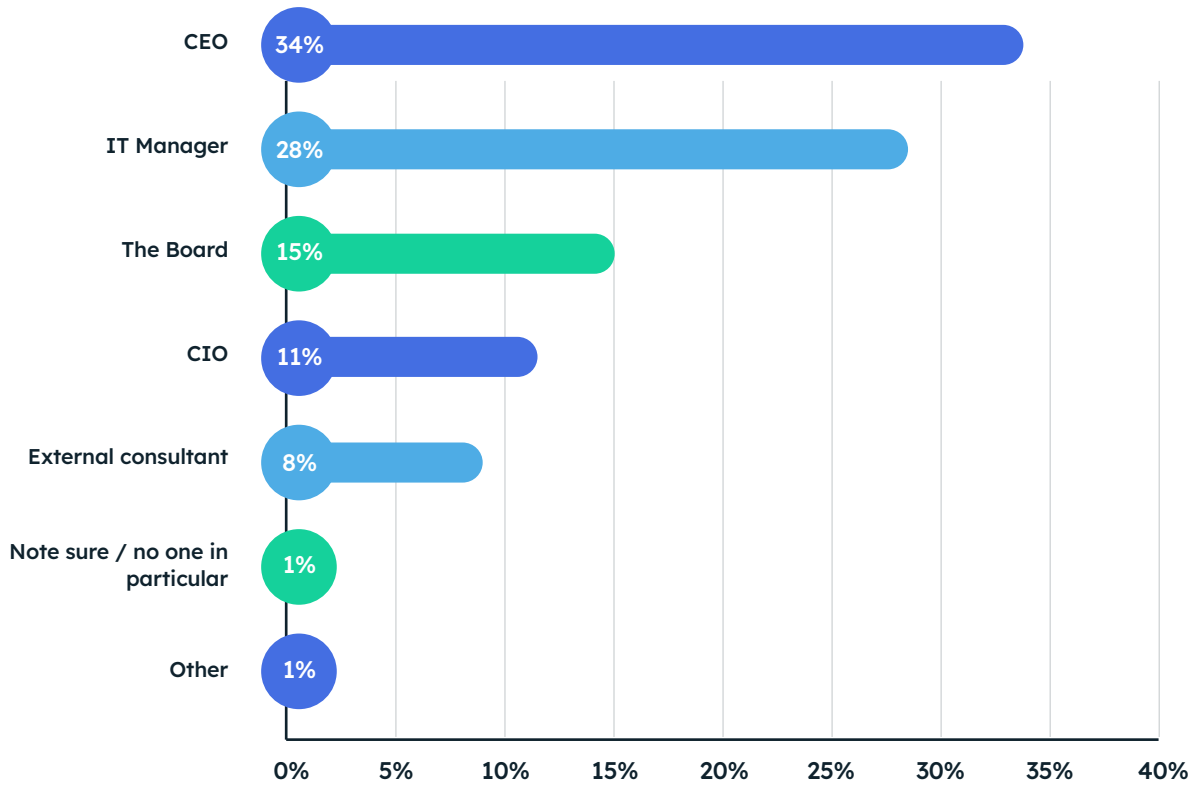
Following on from our previous section, there's also evidence that business leaders' fears about reputational impact and loss of business are playing out in their interactions with partners and customers. As part of the due diligence process, 42% of respondents have been asked to prove NIS2 compliance by partners. 41% have been asked to prove NIS2 compliance by investors. In addition, just over a third (36%) have been asked to provide evidence of compliance by customers and prospects.

We can infer from this that, despite confusion on how to implement the measures it mandates, NIS2 is having cut through as a standard that businesses want partners or suppliers to meet. Of course, NIS2 is still a relatively new standard, so we'd expect this pressure on businesses to grow even further as more organisations familiarise themselves with it and it becomes an everyday part of the regulatory landscape.

Cybersecurity compliance increasingly has board buy-in

One of the key developments in cybersecurity regulation across the last few years has been a growing emphasis on fostering board buy-in and ultimate responsibility for compliance. Indeed, it's one of the key aims of both NIS2 and the UK's **Cyber Security and Resilience Bill** (widely considered an adaptation of EU legislation). Governments and security agencies across the globe have realised the importance of top-down responsibility for cybersecurity in organisations, in opposition to the old model, which often found it siloed in IT departments and treated as something of an afterthought rather than a priority.

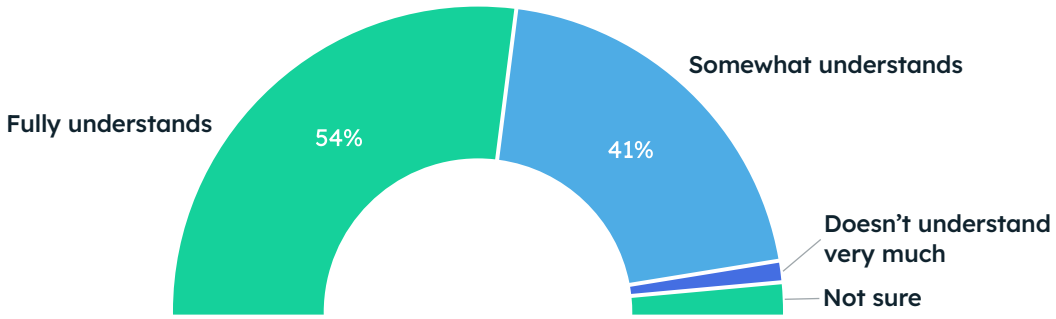
6. Who in your organisation is ultimately responsible for cybersecurity compliance? [Select one]



Response count 670

With this in mind, it's interesting to see that 60% of organisations have made either the board (15%) or members of the C-suite (CEO: 34%, CIO: 11%) responsible for cybersecurity compliance. A significant proportion of our respondents still followed the old model of IT management responsibility (28%) or outsourcing responsibility to an outside consultancy (8%). However, the high number of organisations that have implemented board responsibility represents real progress.

7. To what extent do you believe that the board fully understands the legal and reputational risks associated with non-compliance?



Response count **102**

In a similar vein, there appears to be a good understanding of the legal and reputational risks of non-compliance among board members at the businesses we surveyed. 54% said they believed the board fully understood the risks, while a further 41% said board members somewhat understood. Just 2% of respondents said there was little understanding.

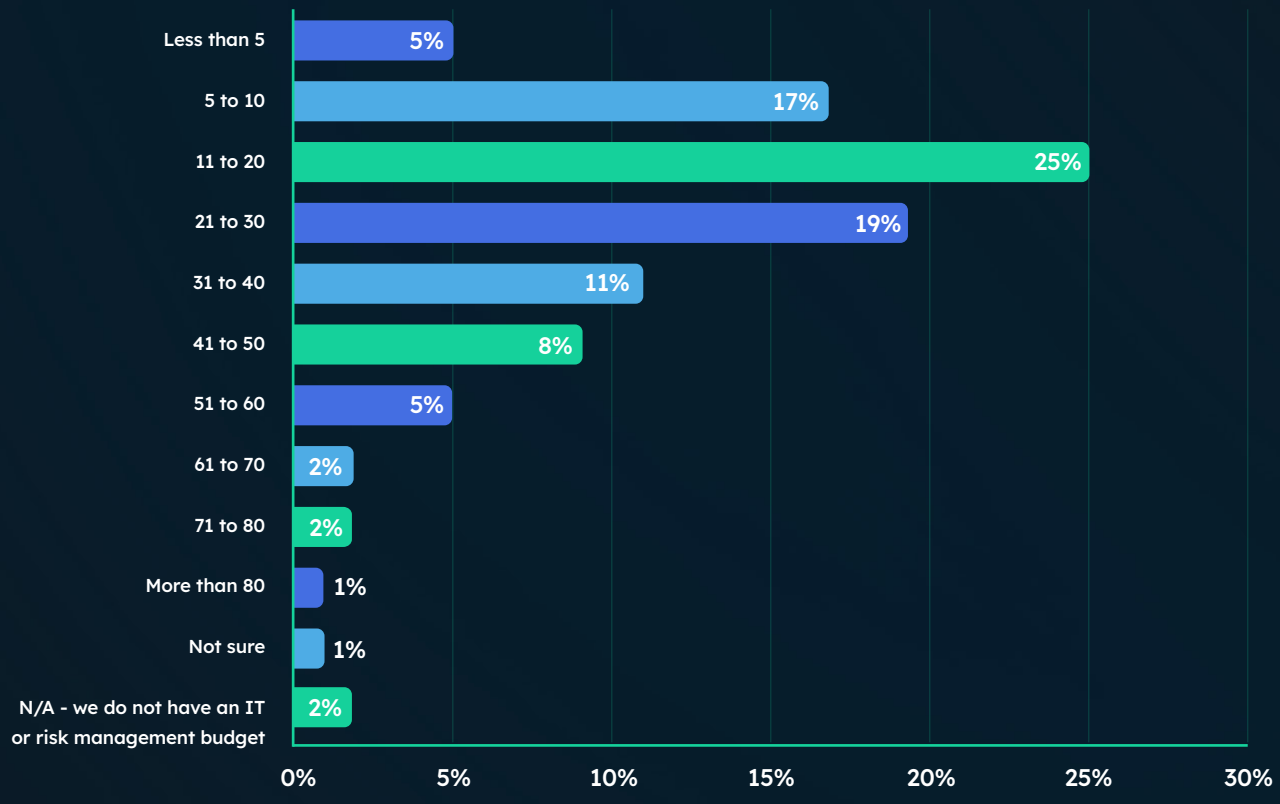
Strong executive understanding of cybersecurity has become a defining factor in organisations' cyber resilience. So, these positive results, with the caveat that boards often **overestimate understanding and their organisation's cyber readiness**, should be included.

Cybersecurity compliance spend is about right

Alongside increasing board buy-in for cybersecurity compliance, most of our respondents are spending around what they should be on security.

What an organisation spends on security can vary based on factors like size, industry, and compliance requirements, so it's difficult to put a figure on what organisations should be spending. However, insurers such as Gallagher put the figure for most organisations as between **5 and 20%** of the IT budget.

8. What percentage of your IT or risk management budget is currently allocated to cybersecurity compliance? [Select best match as a percentage]



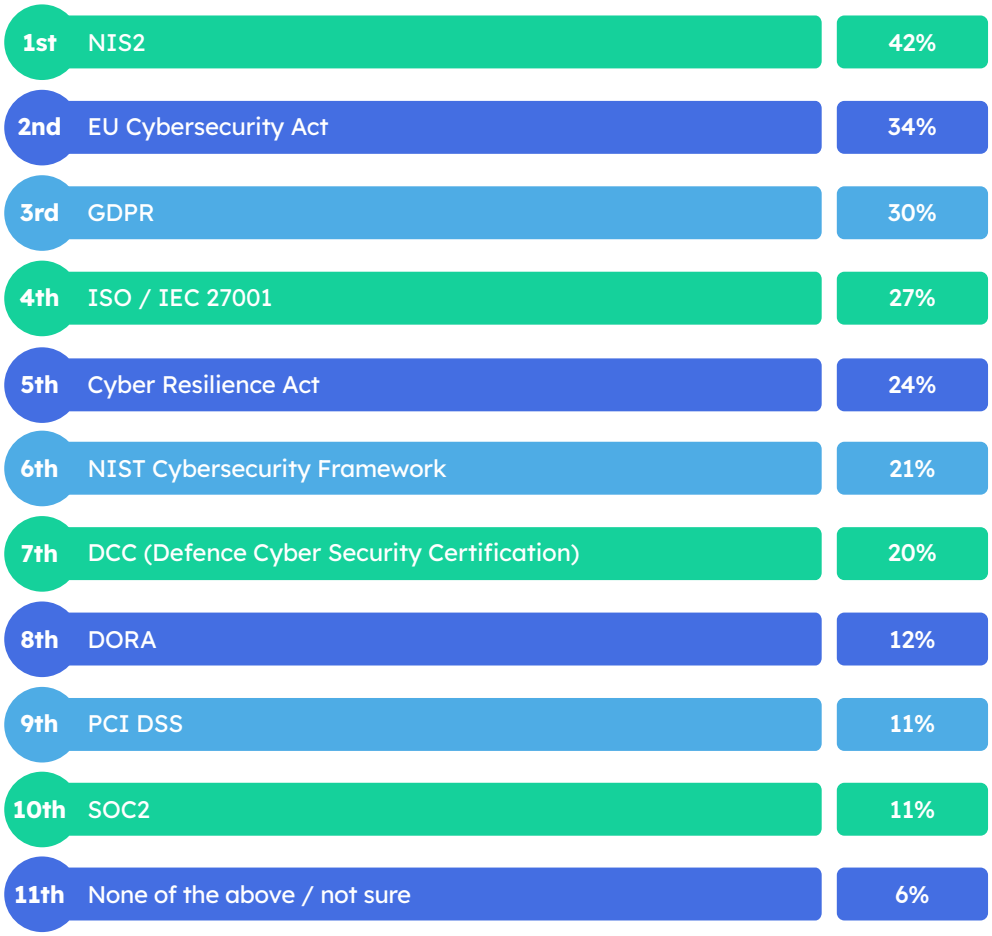
Response count **670**

Almost a third (30%) of our respondents are spending 30-40% of their organisation's IT or risk management budget on cyber (more than most insurers recommend). Meanwhile, a further quarter (25%) were spending 11-20%. Heartenningly, just 5% of our respondents are spending the recommended minimum of 5% or less on their security, signifying the shift in perceptions in cyber's importance we've seen in the last few years.

Most organisations need to comply with multiple regulations

For our final three questions, we shifted focus to cybersecurity regulations more generally to gain a picture of the compliance responsibilities businesses face.

9. Which, if any, of the following regulations should your organisation be complying with? [Select all that apply]

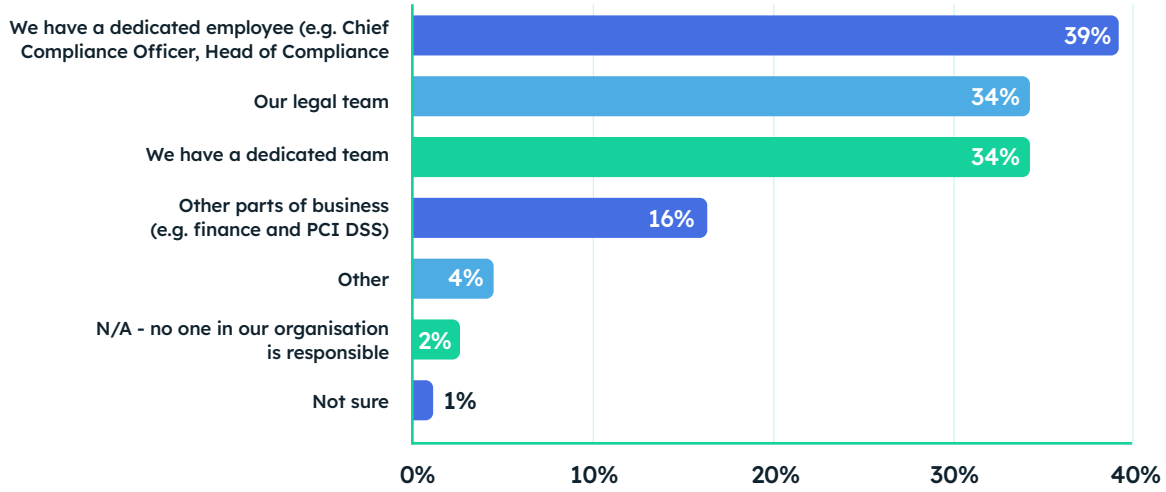


Response count 670

This revealed that most businesses, whether in the EU or the UK, are required to comply with multiple data-protection or cybersecurity regulations. For example, an EU company (or one working within the EU) could be required to comply with NIS2 (42%), the EU's Cybersecurity Act (34%), GDPR (30%), the EU's Cyber Resilience Act (24%), and ISO/IEC 27001 (27%).

For most businesses, that's going to prove an onerous undertaking. So, with that in mind, it's perhaps not a surprise to see that most organisations employ a member of staff, such as a Chief Compliance Officer (39%), a dedicated team (34%) or the legal department (34%) to tackle regulatory compliance.

10. Who, if anyone, in your organisation is responsible for compliance with regulations? [Select all that apply]



Response count 670

However, there may be a darker side to regulatory responsibilities. As we'll see in our next section, many businesses are feeling the strain of compliance.

Is regulation fatigue setting in?

11. Which, if any, of the following statements do you agree with? [Select all that apply]

Response count **670**

Our final survey question asked businesses how they feel about cybersecurity and data protection regulations. The responses we received were overwhelmingly critical of the current regulatory landscape. 42% of respondents said that there are too many regulations to comply with. Meanwhile, a further 35% said that too many regulations overlap, and 27% felt there was too much emphasis placed on them.

This doesn't appear to be a case of businesses not seeing the value in regulation. For evidence, consider that just 8% of respondents said that regulations were unimportant to their organisations. Instead, these results seem to speak to a "regulation fatigue" setting in among business leaders.

We've already touched on the reasons behind this earlier. Firstly, many businesses (particularly those based in or working within the EU) are required to comply with multiple cyber and data protection regulations. This can stretch resources or necessitate employing a specialist compliance team. What's more, our respondents are right, many of the requirements do overlap, making the case for a streamlining of regulations.

However, if we accept that legislative action is both unlikely and usually a slow process, what can be done to help businesses manage their compliance responsibilities in the here and now? We'll tackle that in our next section.

There is a clear opportunity for MSPs to support ongoing compliance

It's clear that many businesses are finding the current regulatory landscape difficult to navigate, whether due to confusion about what they're required to do, budgetary constraints, or fatigue at overlapping standards. This may even be the case for some MSPs themselves, as some fall within NIS2's regulatory scope.

However, this also represents a key opportunity for MSPs who are in a position to take it. Businesses across the UK and Europe need help managing year-round compliance, not just with NIS2, but also with DORA, PCI-DSS, the **UK's Defence Cyber Certification**, ISO 27001, and others. For MSPs, this offers the potential to become a business' trusted cybersecurity partner. And, not just for one-off certifications, but year-round.

Here are our recommendations for what MSPs and the cybersecurity industry more generally can do to help.

Our recommendations for MSPs

1. Automate and use tools where possible

One of the key reasons organisations struggle with compliance is the time and resources it takes – see many **businesses' ongoing struggles with GDPR** as evidence. However, many of the requirements of compliance and ongoing cyber resilience can be made markedly easier by the use of tools.

For example, **cyber awareness and phishing training** for employees, **vulnerability management**, and **threat monitoring** can all be made far simpler – for both end organisations and MSPs – with the use of the right tools.

2. Consider offering multi-regulation compliance services

Another difficulty our results highlight is the overlap in requirements between regulations. However, this doesn't have to be a bad thing for MSPs and service providers. Many of the requirements overlap because they're crucial to an organisation's overall resilience. For instance, training of board members and staff, adequate cyber risk management and incident planning, or the use of common security measures such as **multi-factor authentication**.

So, there's a lot to be said for offering services that prioritise overall resilience and encompass as many of these measures as possible. It'll not only make compliance with multiple regulations far simpler, but it'll also keep your clients safer.

3. Develop supply-chain security offerings

Developing a minimum security standard across supply chains is one of the key drivers behind much recent cyber regulation. The issue, as our respondents highlighted, is that it can often be extremely difficult for businesses to gain visibility of their entire supply chain.

However, technological solutions to this thorny problem do exist. For example, **supply chain risk management platforms** can go a long way towards easing the burden on businesses.

4. Encourage resilience over box-checking

Lastly, there can be a tendency among businesses to view cybersecurity compliance as something of a ‘box-checking exercise’. Instead, MSPs should encourage business leaders to view cyber resilience as an investment with far greater benefits than merely compliance.

Highlight that good cyber resilience will help their organisation retain clients, better compete for new business, and avoid costly or even catastrophic incidents – compliance with regulations is only one part of the process.

How does the data break down region-by-region?

Before we conclude with our key takeaways from the survey, it's worth examining whether there were any country-by-country or regional differences in the results. For this section, we've grouped countries with similar regulatory frameworks and security cultures into regions. For example, the United Kingdom and Ireland, or Benelux (minus Luxembourg) for the Netherlands and Belgium.

UK and Ireland

Across the UK and Ireland, our answers from business leaders generally followed a similar theme to the overall results. Like their European counterparts, most British and Irish businesses are implementing at least some of the requirements of NIS2 compliance, with training (50%), encryption (48%), regular risk assessments (43%), and backups (42%) the most common.

However, it should be noted that this is likely as much due to the presence of the Cyber Essentials (UK) and Cyber Fundamentals (CyFun, Ireland) certifications in the region as to the NIS2 framework.

Unsurprisingly, given Ireland's delay in transposing it into law and the UK's lack of regulatory clarity around NIS2, full compliance is low (24%). The reasons for this, as in other regions, are largely budgetary (17%), resource constraints (17%), and confusion about how to comply (14%).

Like other regions, board buy-in (85%), understanding (93%) and ultimate responsibility (32%) for security are strong. Likewise, just 1% of the businesses we surveyed were spending less on cybersecurity than the insurers' minimum standard of 5%. Businesses also cited the same regulatory fatigue as their European neighbours, with 71% feeling that there were either too many regulations or too much emphasis on them.

However, one area of slight divergence from other regions is related to who is asking businesses to prove their NIS2 compliance. For British and Irish businesses, investors ranked comparably high (58% to the 42% across all regions), suggesting that for those investing in the UK and Ireland, security is of paramount importance.

Benelux

Much like the UK and Ireland, Belgium and the Netherlands largely followed the overall trends. Despite this, there were a few interesting areas of divergence.

Firstly, in response to our first question on NIS2 measures, "established corporate accountability" ranked far higher at 36% than in any other region. This is reflected in who is ultimately responsible for cybersecurity compliance in Dutch and Belgian businesses. Benelux is one of the few regions where the CEO was by far the most common answer at 43%.

This would appear to suggest that both countries enjoy a culture of high investment in and accountability for cybersecurity when it comes to senior leadership. Yet, the Benelux region displayed unusually high numbers of businesses spending 5% or less on cybersecurity compliance. The 10% of businesses spending less than cyber insurers advise is the highest of any region (save Denmark) and double the overall rate across all regions. So, perhaps there's a disconnect between legal or regulatory accountability and financial investment.

It's also notable that the number of business leaders who felt there were too many regulations (43%) or that regulatory overlap is a problem (37%) was higher in both cases than most of Europe (save Germany, France and Italy). One conclusion to draw from this is that Belgian and Dutch approaches to regulatory compliance may be proving too onerous for businesses to tackle alone.

Germany, France & Italy

Together, Germany, France, and Italy form **the EU's three largest economies**. As a result, all three have relatively robust and mature traditions of both regulatory oversight and corporate responsibility, particularly in France and Germany.

Echoing the other EU region we've tackled (Benelux), Germany, France and Italy also showed strong leanings towards corporate accountability. For our first question, "established a strict incident reporting procedure" scored higher than anywhere else at 32%. In the same vein, like the Benelux countries, CEOs are ultimately responsible for security in many companies (35%). Most commendably of all, not a single respondent to our question on leadership understanding of compliance replied that board members had little understanding.

However, like the Benelux countries, a strong regulatory culture does come with a cost. Close to half (44%) of respondents thought there were too many regulations, with a further 39% feeling they overlapped. Again, this demonstrates a very real regulatory fatigue across the region.

Of some concern, too, is the number of businesses underspending on compliance. While not as high as the Benelux region (10%), 8% is still higher than our survey average of 5%. What this signifies is difficult to glean without more context. Nevertheless, it does suggest that, like their Belgian and Dutch neighbours, businesses across the region could and should be dedicating more budget to compliance and security.

Poland

Poland is one of the EU's greatest success stories. Its economy has doubled in size in the past two decades – at **twice the rate of other OECD countries** – and now has a GDP to rival much more established countries like the UK. As a result, it's also seen an uptick in its cybersecurity sector and adoption of data protection and security measures.

So it's perhaps not a surprise that our results paint Poland as another country with a strong security culture. Boards' understanding of compliance is good, with just 3% of respondents saying leadership "didn't understand very much".

Interestingly, Poland was the only country we surveyed where "The board" (30%) was the most common answer given to our question: Who is ultimately responsible for cybersecurity within your business? Given that a further 27% of respondents listed the CEO and 15% the CIO, this means that the majority of Polish businesses have either board or C-suite responsibility for compliance, evidencing an unusually strong culture of corporate accountability.

It's also clear that this has had an impact on why Polish businesses feel it's important to comply with NIS2 and other regulations. While Polish businesses are worried about the legal costs and loss of customers that can stem from non-compliance, loss of investor or stakeholder confidence also scored unusually high at 17%.

More surprisingly still, not a single respondent said their business was spending 5% or less of their IT budget on security and compliance. This was the only region or country in Europe we surveyed where that was the case, again demonstrating a strong compliance culture.

However, Polish business leaders are not immune to the same regulatory troubles as the rest of Europe. Like elsewhere, our survey respondents cited budget (20%), lack of resources (19%), and confusion on how to comply (19%) as the main reasons for NIS2 non-compliance. Polish business leaders also felt that there were too many regulations (46%), with too much overlap (34%), and too much emphasis on them (29%).

Denmark

Our survey of Danish business leaders revealed some interesting findings. In common with other EU countries, Denmark displayed high levels of board understanding, with 100% of respondents saying leadership at least 'somewhat understood' compliance. This was alongside high levels of corporate accountability for compliance; some 67% listed the CEO, board or CIO as ultimately responsible.

However, alongside this, our respondents evidenced some business scepticism towards NIS2 and compliance more broadly. Over a third of respondents (34%) didn't agree that there was a competitive advantage to compliance. And this is reflected in some businesses' spending. The 10% of businesses spending less than 5% of their IT budget on security and compliance is a European-wide high (tied with the Benelux region).

Likewise, the number of respondents who felt there were too many regulations (55%) was the highest of anywhere we surveyed. This would appear to suggest that 'regulatory fatigue' and the scepticism that often accompanies it are particularly high among Danish organisations.

Key takeaways

Finally, what can we learn from the survey? Here are our key takeaways.

1. Most businesses are implementing at least some of the measures mandated by NIS2.
2. However, just 16% of respondents are confident that their organisation is fully compliant with NIS2, despite the deadline for being so having passed.
3. The most common reasons for non-compliance are budgetary constraints (20%) and a lack of guidance on how to implement the measures (16%). Although most worryingly, 11% don't know what NIS2 is, despite needing to comply.
4. Although full compliance with NIS2 is low, most businesses see the value in the regulation. Three-quarters (75%) of respondents noted that there is at least some competitive advantage to NIS2 compliance. Meanwhile, nearly a third (27%) strongly believe that there's a competitive advantage.
5. The repercussions of non-compliance were a concern for most respondents. The top three concerns were: loss of productivity (18%), reputational loss (18%) and loss of customers (18%).
6. Businesses are increasingly being asked to prove compliance by customers and partners. As part of the due diligence process, 42% of respondents have been asked to prove NIS2 compliance by partners, 41% by investors, and 36% by customers or prospects.
7. Cybersecurity compliance increasingly has board-level buy-in. 95% of respondents believe that the board of their organisation at least somewhat understands the legal and reputational risks associated with non-compliance. And, 34% of organisations had made their CEO responsible for cybersecurity.
8. As per insurers' guidance, most businesses are dedicating at least the right amount of budget to cybersecurity compliance. Almost a third (30%) of our respondents are spending 30-40% of their organisation's IT or risk management budget on cyber (more than most insurers recommend). Meanwhile, a further quarter (25%) were spending 11-20%. Hearteningly, just 5% of our respondents are spending the recommended minimum of 5% or less on their security.
9. A quarter (25%) of respondents said that between 11% and 20% of their organisation's IT or risk management budget is currently allocated to cyber compliance. A further third (30%) are dedicating between 21 and 40% of their budget to it.
10. Most organisations – particularly those within the EU – are required to comply with multiple cybersecurity and data protection regulations, leading to businesses being forced to dedicate specialist resources to it.
11. This has led to 'regulation fatigue', with 42% of respondents saying that there are too many regulations to comply with, 35% feeling that too many regulations overlap, and 27% concerned that there is too much emphasis on regulations.
12. Businesses are finding the regulatory landscape difficult to navigate on their own. This presents a huge opportunity for MSPs to position themselves as a one-stop shop for regulatory compliance and ongoing cyber resilience.

A final word from our CEO

Our research shows that most organisations aren't ignoring NIS2 - they're stuck trying to implement it. Only 16% feel fully compliant, despite growing board-level ownership, real budget allocation, and a clear belief that compliance matters.

The problem is not motivation. It's the gap between what the regulation asks for and the practical support businesses have to deliver it - especially while juggling overlapping standards and limited internal expertise.

NIS2 is also changing how trust works in the market. Partners, investors and customers are already asking organisations to prove compliance, not just promise it. The organisations that succeed will be the ones that turn compliance into routine - and move from uncertainty to confidence.

Jamie Akhtar, CEO at CyberSmart