Deloitte.

Deloitte CISO Programme

The Last 90 Days of a CISO

Taking control of your legacy

2025

MAKING AN IMPACT THAT MATTERS since 1845

Contents

1. Foreword
2. Executive summary
3. The challenge of balance
4. Politics and trust
5. Resilience through adversity
6. The human element
7. The weight of accountability
8. Conclusion: Taking control, leaving a legacy
9. *From one CISO to another...*
10. Authors
11. Methodology

Foreword

Cyber incidents naturally have significant impacts on systems, data, operations and reputations. Beyond this, the ramifications can also be felt at a more personal level; affecting CISOs' wellbeing, and ultimately in some cases their careers. But, while cyber-attacks can be incredibly stressful, they can also be career-defining in a positive sense. They provide the opportunity to respond in a manner which reinforces customer and stakeholder confidence, to gain real-world experience of handling an incident and to unite teams around a common cause.

In response, the Chief Information Security Officer's (CISO) role has evolved into one of the most critical leadership positions in the business.

It is a role full of opportunity: to shape strategy, influence culture, and drive meaningful change. But delivering on that, while managing the day-to-day pressures of the role, is a real challenge. The most effective CISOs can take control of their destiny, define their own success, and ensure that their legacy is shaped by intent.

This report is not just a reflection on the role; it explores what it truly means to lead in cyber today. Drawing on candid interviews with CISOs from across industries, it explores their experiences of the role.

The insights reflect the excitement and fulfilment of being a CISO but also examine the weight of the role and the pressures it can bring. From surviving the crisis call on a Friday night to shaping strategy in the boardroom, this report highlights the realities and rewards of leading in cyber today, providing practical insight and perspective for those navigating the challenges of security leadership.

Whether stepping into the position for the first time or considering the legacy you want to leave, this report offers a chance to reflect—and take control of what comes next.

Peter Gooch
Partner, Cyber
CISO Programme Sponsor

Executive summary

This report offers a rare and unfiltered look into the reality of life as a CISO. Based on in-depth interviews with 25 CISOs across industries, geographies, and experience levels, The Last 90 Days of a CISO captures the complexities of the role; from high-stakes pressure to moments of quiet resilience and personal growth.

It tells the story of a role under constant scrutiny, where many CISOs feel the pressure of risk, not only to the business, but increasingly to their own professional standing and wellbeing. With rising expectations, limited resources, and the ever-present fear of an attack, many describe a sense of isolation and vulnerability. In fact, some of those interviewed said they wouldn't take on the CISO role again. For many, job security feels fragile, and the margin for error razor-thin.

And yet, what came through clearly in these conversations was not just pressure, but purpose. Many CISOs spoke with energy and enthusiasm about the influence they've built, the teams they've developed, and the change they've driven. While the challenges are real, so too is the sense of impact.

A recurring theme throughout the interviews was the importance of focusing on what you can control; your priorities, your relationships, and the environment you create around you. That mindset, more than any single tactic, is what helps leaders thrive in this complex, high-stakes role.

The insights are organised across five key themes:

1 | The challenge of balance

The constant juggling act between long-term strategy and day-to-day firefighting. The most effective CISOs learn to delegate, prioritise, and avoid chasing perfection.

2 | Politics and trust

Building influence and navigating stakeholder relationships is as vital as technical know-how. Trust, not tools, defines success.

3 | Resilience through adversity

Adversity, from ransomware to regulatory pressure, shapes strong leaders. Those who thrive use challenges to sharpen their focus and reinforce their purpose.

4 | The human element

No CISO succeeds alone. Strong teams, peer networks, and empathetic leadership are essential, not just to performance, but to wellbeing.

5 | The weight of accountability

The weight of the role is heavy, but CISOs can define their legacy by fostering defensible, business-aligned security cultures.

Note - Given the sensitive nature of CISO roles and the information shared, all participants have contributed anonymously to this report.

1 | The challenge of balance

At any given moment, you can be pulled between strategic decision making and operational firefighting, business engagement and technical detail, leading teams and answering to leadership. And often, you're expected to excel at all of it at once.

Throughout the course of this research, CISOs consistently highlighted just how elusive balance can be in practice. Many described feeling pulled in multiple directions; responding to incidents, managing teams, engaging the board, all while trying to carve out time for strategic leadership. Several told us that the only way to protect that time was to deliberately ringfence it in their calendars and treat it as immovable. Others spoke of the mental toll of being constantly "on," and how burnout crept in when recovery time wasn't actively prioritised.

A few mentioned that it took a crisis, personal or professional, for them to realise that balance wasn't a luxury, but a necessity. "It took me getting physically unwell to realise I had to delegate more," said one. Another reflected that their most impactful leadership came after they learned to say no to things that didn't require their involvement. The message was clear: balance doesn't happen by accident. It has to be earned, protected, and defended.

This juggling act rarely leaves time for reflection. Many CISOs enter the role with clear aspirations to drive transformation, embed a long-term strategy, or reshape organisational culture but reality often takes over. Incident response plans become daily routines and Board presentations are squeezed between crisis calls. There's little room to step back and think beyond the next breach.

"The most effective CISOs are skilled delegators."

"Strategic planning is crucial, but the reality is that a significant portion of my time is spent on reactive measures."

"It took me getting physically unwell to realise I had to delegate more."

1 | The challenge of balance

"Our role is to make the organisation securable, but not to do it all alone. Success comes from focusing on frameworks that endure beyond the immediate crisis."

"I never realised how 24/7 it would be. It's hard to switch off, always waiting for that Sunday night phone call."

"Not every security issue is created equal. I have learned to focus on the highest-impact risks. Prioritisation is an art!"

What emerges isn't a lack of ambition, it is a lack of capacity and focus, driven by fear of missing something that could have critical consequences.

CISOs must constantly prioritise; balancing the urgent with the important and making deliberate choices about where to invest limited time and energy. But while CISOs accept that perfect security is impossible, boards and executive teams who understand the need for a risk-based approach often lose sight of that in the middle of an incident.

That disconnect makes it harder for CISOs to justify the trade-offs that are not only necessary, but strategic. It creates friction, adds pressure, and limits their ability to focus on long-term outcomes.

When CISOs are pulled too deep into day-to-day firefighting, the organisation misses out on their ability to embed security into broader business thinking.

This is a signal that the role is outgrowing traditional models. Today's CISO is far less a technologist and far more a business leader; one who must influence culture, educate the Board, shape investment decisions, and align security with commercial goals. This requires space to lead, not just capacity to cope.

Still, it's important to challenge the myth of "perfect balance". A more sustainable mindset is one of intentional trade-offs. Rather than striving for flawless equilibrium, successful CISOs are learning to prioritise with purpose: to create time for strategic thinking, to set clear boundaries, and to build teams they trust to manage operations without their constant presence.

Key takeaways | The challenge of balance

Balance is not a luxury. It is something many CISOs told us was essential to their effectiveness.

Those who found space to step back, delegate with confidence, and focus beyond the immediate described not only performing better themselves, but enabling stronger, more resilient teams around them.

Make space for strategic thinking

Block out regular time away from operational noise to reflect, reset, and refocus. Protecting this space helps you lead with intention, not just reaction.

Educate upwards on balance

Help senior stakeholders understand what a risk-based approach looks like. Balance isn't about doing less; it's about aligning effort with impact and accepting that not everything can be secured at once.

Draw boundaries to protect perspective

Know when to switch off and where your energy is best spent. Maintaining your balance helps you make better decisions and sets a visible example for your team.

Invest in support – above and below

Build a team you can delegate to and cultivate relationships with peers and leaders who help you zoom out when the pressure spikes.

2 | Politics and trust

One of the most consistent themes across our conversations was the challenge of role definition. Few CISOs step into a clearly scoped mandate. Some inherit legacy expectations shaped by their predecessor, while others walk into organisations where the CISO role has never existed before. The level of investment, the maturity of the security function, and the organisation's risk appetite all shape what the CISO is expected to be, but these expectations are rarely consistent or well-articulated.

Several CISOs described spending their first year "defining the job as much as doing it." For many, that meant carefully navigating internal politics, understanding key relationships, and gradually shifting perceptions of what security leadership could look like; building influence, aligning stakeholders, and creating space to lead.

The remit of the CISO is inherently broad. But with breadth comes ambiguity. Some CISOs said they were seen as technologists, others as compliance owners, and a few weren't entirely sure what the Board expected of them at all. As one leader put it: "If you don't define the role, others will define it for you, and you probably won't like what they come up with."

That's where trust becomes critical. In the absence of a fixed blueprint, trust is what enables a CISO to take control, not by asking for more power, but by exercising influence. This begins with clear communication. Several CISOs spoke about tailoring their messaging, presenting detailed methodology to some Board members, offering reassurance and clarity to others.

CISOs who feel empowered by their Boards, given both the mandate and the means to act, are better equipped to maintain this balance. Where that support is missing, frustration sets in fast. A lack of Board alignment isn't just a governance issue; it is a talent risk. Several CISOs noted they had considered moving on because they couldn't fulfil the role's potential in an unsupportive environment.

"Trust, not technology, is the foundation of a strong security posture. Without the trust of stakeholders, even the most advanced tools are ineffective"

Trust-building isn't limited to the boardroom. Many CISOs reflected on the importance of lateral relationships with CIOs, CROs, COOs, and business leads. Where relationships were strong, priorities were easier to align, resources easier to unlock, and support easier to sustain. Where trust was lacking, CISOs found themselves justifying every decision and struggling to secure backing for even minor changes.

2 | Politics and trust

"You can't do this role well if you're constantly defending your right to exist."

"A CISO's effectiveness is directly proportional to their ability to build trust and credibility with stakeholders."

"Cybersecurity isn't a technology problem; it's a people problem. Building strong relationships and fostering a culture of security awareness is key."

The CISO–CIO relationship was noted as pivotal. While some described a natural tension—risk versus innovation—most saw it as a complementary partnership. One CISO explained: "We have different objectives, but the same outcome; we both want to protect the business. That starts with understanding what matters to each other."

Downward trust was just as important. Many CISOs described how empowering their teams helped them step back from constant firefighting. One leader noted: "My team knows the mission. I don't need to be in the room for them to make good decisions." That clarity allowed them to reclaim time for strategic thinking and to avoid burnout.

This matters most during incidents. Several CISOs echoed the now-familiar phrase: "It's not if, but when." When an incident does happen, trust from above is critical and becomes a force multiplier. CISOs who had taken the time to educate the Board, align with business leaders, and empower their teams said those investments paid off. They weren't managing chaos alone; they were guiding a coordinated response.

Resource allocation was another recurring theme, particularly the frustration of being expected to deliver strategic transformation while buried in operational noise. Some CISOs addressed this by lobbying for headcount. Others focused on helping the business put the right skills in the right place, even if that meant advocating for another team. In both cases, the goal wasn't control for control's sake—it was the freedom to focus on what mattered most.

Key takeaways | Politics and trust

Ultimately, the ability to build trust and navigate internal politics is what allows CISOs to move from reactive delivery to intentional leadership. And in a role where so much can feel outside your control, those relationships are the foundation on which influence, and longevity is built.

Start with clarity

Work with the Board to define your role and align expectations. Don't assume others know what you're there to do, shape the narrative early.

Tailor your engagement

Adapt your communication style to stakeholders' preferences. Knowing what each audience values helps build credibility and trust.

Bring others on the journey

Co-create security goals with peers across the business. When people feel included, they become champions rather than blockers.

Use trust to enable strategy

A trusted CISO is empowered to say no, set priorities, and delegate. Invest in trust as a strategic asset, not just a leadership trait.

3 | Resilience through adversity

For CISOs, pressure is constant. And when incidents hit, that pressure sharpens into something more intense; scrutiny, urgency, emotional load. In those moments, the job becomes all-encompassing and not just about managing a technical response. It's about steering the organisation through uncertainty, supporting exhausted teams, and helping senior leaders make high-stakes decisions; often without a complete picture of the incident.

Many of the CISOs we spoke to were open about how tough this can be. They described long nights, high-stakes calls, and moments of isolation that linger well beyond the crisis. But they also talked about perspective. There was a shared understanding that while incidents feel overwhelming in the moment, the world keeps turning. "You feel like everything is on fire," one CISO said, "but part of leadership is staying calm enough to realise it won't burn forever."

For some, these moments became personal turning points. Incidents pushed leaders to clarify their decision-making, test their communication style, and confront the limits of their own capacity. Several reflected on how they emerged stronger and better equipped. "It didn't break me," one said. "It taught me how to lead under pressure."

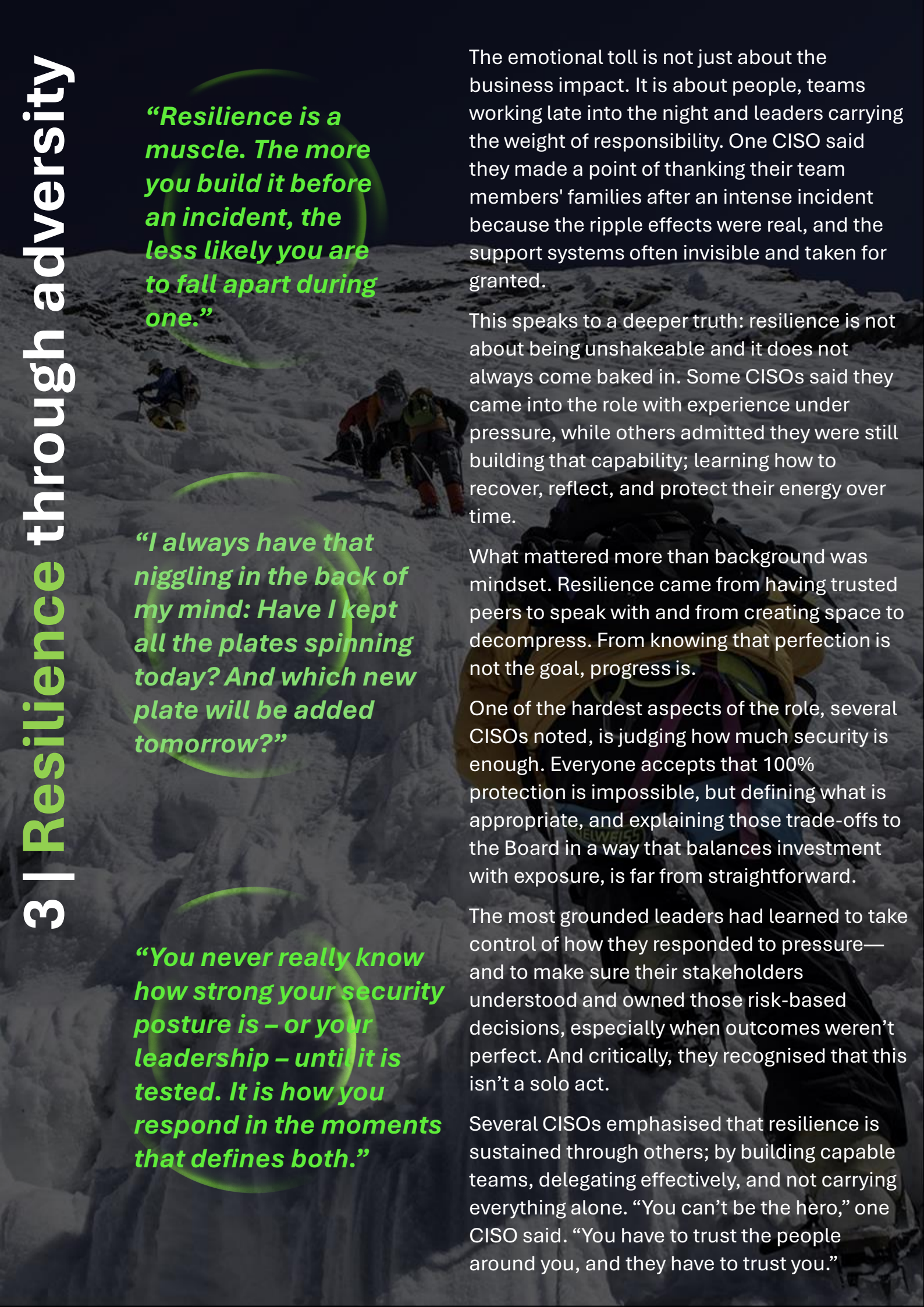
But that growth rarely happens in isolation. Many CISOs spoke about the importance of feeling supported. Where organisations had a realistic understanding of risk and a strong relationship with the CISO, the experience while still demanding, was navigable. Where that wasn't the case, it could feel deeply isolating. "The threat was manageable," one CISO noted. "It was the second-guessing, the constant explaining, that is what wore me down."

"I should have supported my team better. I would feel that moment—that sickness—that I could have done more. That's what makes you better next time."

"Every crisis is a lesson. The hardest moments teach you to prioritise, stay calm, and focus on what truly matters."

"After a breach, people look to the CISO not just for answers but for confidence. You have to be the calm in the storm, even when you don't feel it yourself."

"Resilience is a muscle. The more you build it before an incident, the less likely you are to fall apart during one."



"I always have that niggling in the back of my mind: Have I kept all the plates spinning today? And which new plate will be added tomorrow?"

"You never really know how strong your security posture is – or your leadership – until it is tested. It is how you respond in the moments that defines both."

The emotional toll is not just about the business impact. It is about people, teams working late into the night and leaders carrying the weight of responsibility. One CISO said they made a point of thanking their team members' families after an intense incident because the ripple effects were real, and the support systems often invisible and taken for granted.

This speaks to a deeper truth: resilience is not about being unshakeable and it does not always come baked in. Some CISOs said they came into the role with experience under pressure, while others admitted they were still building that capability; learning how to recover, reflect, and protect their energy over time.

What mattered more than background was mindset. Resilience came from having trusted peers to speak with and from creating space to decompress. From knowing that perfection is not the goal, progress is.

One of the hardest aspects of the role, several CISOs noted, is judging how much security is enough. Everyone accepts that 100% protection is impossible, but defining what is appropriate, and explaining those trade-offs to the Board in a way that balances investment with exposure, is far from straightforward.

The most grounded leaders had learned to take control of how they responded to pressure—and to make sure their stakeholders understood and owned those risk-based decisions, especially when outcomes weren't perfect. And critically, they recognised that this isn't a solo act.

Several CISOs emphasised that resilience is sustained through others; by building capable teams, delegating effectively, and not carrying everything alone. "You can't be the hero," one CISO said. "You have to trust the people around you, and they have to trust you."

Key takeaways | Resilience through adversity

In a role where visibility is high and expectations can feel unrelenting; resilience is not just a nice-to-have. It's what helps CISOs keep perspective, maintain their confidence, and stay in control even when everything around them feels uncertain.

Build resilience into every day

Top CISOs develop routines, rituals and support systems to stay steady amid constant strain. Simulations and crisis playbooks are vital, but so is practising how you communicate under pressure, manage upwards, and maintain clarity when the mental load is high.

Normalise the emotional impact

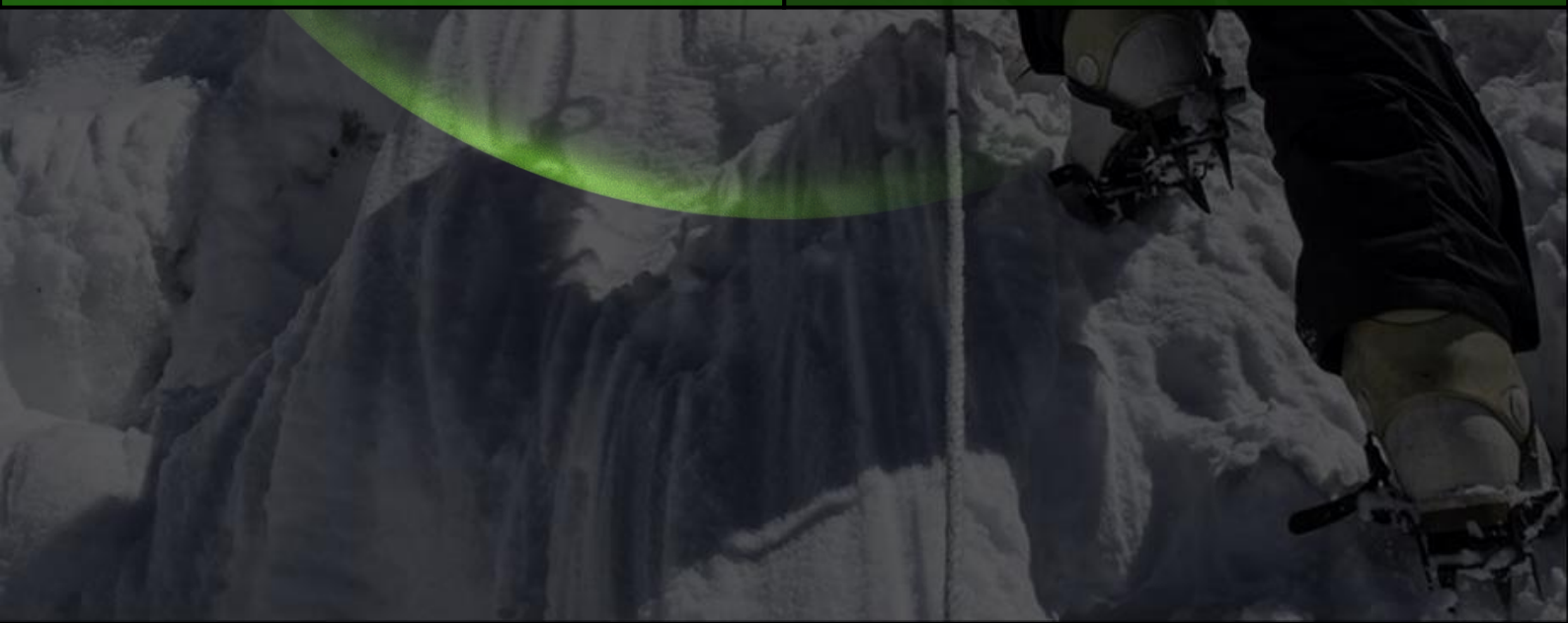
Recognise that pressure is part of the role, but so is vulnerability. Speak openly with peers, share the load with your team, and challenge the idea that resilience means going it alone. The healthiest leaders are those who know when to ask for support.

Build structures that share the weight

Delegate authority, empower deputies, and define clear roles so the burden doesn't rest solely on you when things go wrong.

Prioritise reflection and recovery

After an incident, debrief fully—not just operationally, but personally. What did you learn? And how are you?



4 | The human element

Ask a group of CISOs what matters most in their role, and you won't hear "technical depth" or "certifications" as the top answer. What we heard consistently was that the human side of leadership is where the role is truly won or lost.

One CISO put it best: "Technical expertise gets you into the room, but it's your human skills that keep you there." It's those human skills of communication, empathy, self-awareness and influence that shape how CISOs lead, how they're trusted, and how they're remembered.

In a role where pressure can spike without warning and relationships define your ability to act, emotional intelligence is essential. Leading a high-performing team, building trust with peers, knowing when to push, when to pause, and how to deliver hard messages without losing people along the way all demands a high level of emotional maturity.

The CISO role also requires support. While most leadership frameworks focus on the people you lead, many CISOs reflected on the importance of the people who support them. That includes deputies and deputies-in-waiting, but also peers, mentors, family, and friends. "You can't do this job well if your only identity is 'CISO'," one leader said. "You need people who'll remind you who you are outside of it."

Several spoke about the importance of personal support systems to help them keep perspective. One CISO described how their partner encouraged them to dedicate a few hours a week to completely switch off, helping them to step back from the constant pressure and reconnect with real life. Another talked about how regular non-work rituals like dinner with family, walking the dog, playing music etc. became anchor points that protected their energy and focus. These are the foundations of long-term effectiveness.

Inside the organisation, building the right team is as much about trust as it is structure. CISOs who deliberately invested in a strong deputy spoke about the human value of that relationship: a trusted confidant who could offer challenge, provide support, and grow into a leader themselves. It's a reflection of mature leadership; not just creating resilience in the system, but in the people within it.

It also made them less of a single point of failure. "I sleep better knowing someone else can step in," said one CISO. "And the business should sleep better too."

But support also came from outside the organisation. One of the most valued assets for many CISOs was a strong peer network. Unlike CEOs or CFOs, who are often pitted against each other in competitive markets, CISOs are aligned against a shared adversary. This fosters a level of openness and collaboration that's rare in senior leadership.

"It's important to have someone you can call who understands. A friend, a peer—you need someone who gets it."

These networks, whether formal or informal, serve a practical and emotional function. CISOs described using them to test ideas, validate decisions, troubleshoot vendor challenges, and debrief difficult Board interactions. But perhaps more importantly, they used them to feel seen. "It's the only place where I don't have to explain the job," one said. "Everyone just gets it."

Key takeaways | The human element

This sense of shared experience also reinforced the idea that the job doesn't have to be done alone. The most grounded leaders made peace with the fact that they wouldn't always have the answers and that leaning on others wasn't a weakness, but a strength.

Invest in your human skills

Prioritise leadership development for yourself and your team. Communication, empathy, and the ability to influence across the business are core to success, not optional extras.

Use the CISO network intentionally

Connect regularly with your peers. Whether for advice, challenge, or shared experience, your network is a unique asset and a powerful antidote to isolation.

Lead through trust, not control

Coach rather than command. Build a culture where your team feels ownership, autonomy, and clarity, especially when the pressure is on.

Create leadership depth

Identify and empower a deputy who can step up when needed. This is about continuity, fostering trust and creating space to lead more strategically.

5 | The weight of accountability

There's a moment every CISO recognises when a security incident breaks, and every eye in the room turns to them. It doesn't matter what time it is, who else was involved, or how well the organisation prepared. In that moment, the CISO is the focal point for questions, for reassurance, and for responsibility.

And yet, what emerged from our conversations was not fear, but purpose. Despite the pressure, many CISOs spoke with clarity about what drives them: the chance to make a real difference. Whether it's safeguarding people, enabling innovation, or building secure cultures from the inside out, the role offers a rare kind of meaning. "We're not here to block progress," said one CISO. "We're here to make sure it lasts."

But that sense of mission can come at a cost. When something goes wrong, it's often the CISO who feels it most deeply. Several leaders reflected on the emotional toll, not of blame, but of personal accountability. One described lying awake at night after an incident out of worry for the people affected. "It wasn't about consequences or blame," they said. "It was about wondering—did I do enough?"

This is where accountability becomes more than just a professional obligation. For many CISOs, it's heightened because the role has become as much a vocation as a profession. It's that sense of purpose that drives high standards, thoughtful decisions, and ethical leadership.

But it can also become a vulnerability, particularly in organisations where expectations are unclear, or where risk ownership is poorly defined.

Unlike the dynamics explored in the previous chapter, this isn't about influence or navigating relationships. It's about managing the internal weight of the role. One leader described it as "always being on call, even when you're off." Another said, "It's the anticipation that gets you. The constant readiness for something you can't control."

"You cannot do this job well without a personal sense of responsibility. That's the weight that never really leaves you."

"It's the anticipation that gets you. The constant readiness for something you can't control."

"Accountability is not just about answering to the Board. It is about being able to look yourself in the mirror after an incident."

5 | The weight of accountability

"We're not here to block progress. We're here to make sure it lasts."

"Being a CISO is a vocation, not a job. You don't' clock-off because the risk doesn't clock off!"

"You cannot carry it all alone. The moment you try to own 100% of the risk without support, you're already set up to fail."

That's why setting clear boundaries matters. The CISOs who sustained their performance over time were those who clearly defined their responsibilities, documented key decisions, aligned with the organisation's risk appetite, and communicated expectations early. It didn't eliminate risk, but it reduced confusion when things went wrong.

When that clarity was missing, the emotional burden intensified. A few interviewees shared stories of being held accountable for things they had flagged in advance; risks raised, mitigations proposed but ultimately deprioritised by the business.

In those moments, the frustration was about being expected to carry a risk the organisation had chosen to accept.

This is where the line between accountability and culpability matters.

CISOs understand that the role carries weight, but that accountability shouldn't rest on them alone.

When Boards engage in risk discussions, understand trade-offs, and support informed decisions, accountability becomes a shared effort, not an individual burden.

Security incidents are tests of culture. And during those tests, the CISO becomes more than a responder, they become a symbol of how the organisation handles adversity.

Leaders who had strong foundations, documented decisions, and shared ownership said they were able to lead confidently, even when outcomes were not ideal.

Key takeaways | The weight of accountability

Ultimately, accountability in this role isn't something to fear. When managed well, it's a source of strength. A reflection of leadership integrity and a foundation for long-term influence. But that depends on more than grit. It depends on clarity, communication, and the conviction to know what you're responsible for, and what you are not.

Define and document your decisions

Keep a clear record of key risk decisions and align them to business objectives. This builds credibility and protects against second-guessing.

Communicate expectations early

Clarify with the Board and executive team what accountability looks like and what it doesn't. Mutual understanding prevents future frustration.

Share responsibility, not just reporting lines

Position security as a shared risk. Work with business leaders to define ownership of risks where they arise.

Balance personal commitment with perspective

You can care deeply and still protect your energy. Talk to peers, seek feedback, and avoid shouldering everything alone.

Conclusion | Taking control of your legacy

In a role defined by pressure, unpredictability, and constant scrutiny, the most effective CISOs find strength through the things that they can control.

Throughout this report, five key themes have emerged that define what successful leadership looks like in cyber today:

Own the narrative

Clarity doesn't come from waiting; it comes from leading with purpose. Whether stepping into the role or stepping away, define your direction, articulate your impact, and stay ahead of events.

Lead through people

Trust, empathy, and influence are essential skills. Effective CISOs lead through relationships, not just subject matter expertise. They invest in others and let others invest in them.

Focus on long-term impact, not short-term perfection

No CISO can eliminate every risk. Those who align decisions with business value, communicate trade-offs, and role-model integrity leave behind organisations stronger than they found them.

Understand the politics...and engage with them

Security doesn't exist in a vacuum. The most respected CISOs understand power dynamics, navigate ambiguity, and align stakeholders behind difficult decisions.

Make balance a priority

Resilience is built on recovery. Sustainable leadership means protecting your time, empowering your team, and creating space to think, not just react.

Cyber leadership will never be easy. But it can be intentional and incredibly rewarding. Taking control is about navigating pressures with purpose. It's what enables CISOs to step back from the firefight, focus on the bigger picture, and lead in a way that leaves them and their organisations stronger, more secure, and more resilient than before.

Take control of your time. Take control of your story.

Take control of your legacy.

From one CISO to another | direct quotes

"Be clear on what you are there to do as the CISO. Are you there to provide advice and guidance or are you there to own the risk and to get the funding and deal with it yourself?"

"Always do what is right. Don't try to overthink it or say what other people want to hear."

"Get experience across a breadth of disciplines, then specialise. Build your network and put yourself in positions to be presented with opportunity and then go for it."

"Know when to walk away from a role. Have the courage to hold principles strongly."

"You cannot do it alone. You go faster alone but further together."

"Put good people around you, even if they're better than you. Don't worry that they will show you up."

"Create a safe place for your people. Allow people to raise their hand for support and help."

"Build trust and relationships by being onsite and so you can bump into the exec."

"Match your strategy to the organisation. Know what you need to be successful and identify who you need to be successful."

"Build a strong team...and then get out of their way!"

"My role is to make sure other people make informed risk decisions – you need to be business aware and think about what is right for the business. Being a CISO is about being a leader. Security is 50% sales and marketing."

"Listen to everybody's opinion. Talking through decisions with them helps hugely in gaining their support, even if they do disagree."

"Don't spend every day worrying about tomorrow."

"Wherever you work, make sure they can afford to manage security."

"People mimic behaviours, lead by example."

"Don't try to do everything at once. Make progress every day, rather than massive jumps every now and then."

"It's about putting resources where they're needed—even if it's not your team."

Authors

Peter Gooch
Partner, CISO Programme Sponsor
pgooch@deloitte.co.uk

Abbie Keenan
Senior Consultant, Technology & Transformation
akeenan@deloitte.co.uk

Jennifer Holland, PhD
Manager, Technology & Transformation
jholland@deloitte.co.uk

Special thanks to the Deloitte team:
Craig Clydesdale, Luke Webber, Chris Sloan, Wil Rockall, David Pybus, Nick Seaver, Andrew Johnson, Jitender Arora, Bia Bedri, Patrick Start, Nish Vishwanath, Vojtech Brtnik, Lorna Brocklesby, Kyle Taylor, Euan Ballantyne

Research methodology

This research was conducted by Deloitte UK between spring 2024 and early 2025.

The study draws on in-depth interviews with 25 Chief Information Security Officers from across a range of sectors and industries.

Participants represented organisations from a broad spectrum of size and scale; from non-profit government agencies to multi-national corporations with revenues in excess of £50bn.

On average, respondents had held the CISO role for more than five years.

Interviews were conducted both in person and via video conferencing platforms.

All participants contributed anonymously and voluntarily and were not compensated for their time.

Deloitte CISO Programme

The Deloitte CISO Programme is designed to support and empower today's cyber leaders. Built around the evolving needs of CISOs, it provides a space to develop leadership skills, challenge assumptions, and elevate impact through a carefully curated mix of peer discussion, thematic roundtables, experiential learning, and exclusive content.

At its core, the programme is about perspective—offering CISOs the tools, insights and relationships needed to lead with confidence, navigate complexity, and shape the future of cybersecurity within their organisations.

Whether you're tackling board-level engagement, scaling a security culture, or planning the next phase of your career, the CISO Programme creates opportunities to grow, connect, and lead by example.

If you are not already a member of the CISO Programme and would like to discuss the possibility of joining, please email us at CISOProgrammeUK@deloitte.co.uk