Inside the Mind of a CISO:

WHAT SECURITY LEADERS ARE REALLY THINKING

Casey Cammilleri

Host of Ahead of the Breach &
Founder of Sprocket Security

INTRODUCTION:

Over the past 50+ episodes of Ahead of the Breach, we've had conversations with red teamers, researchers, engineers, and vendors. But this report focuses on a specific group: the CISOs.

We've spoken with more than ten security leaders from industries like tech, healthcare, manufacturing, finance, and defense. They shared how they're thinking about risk, trust, compliance, AI, internal politics, and the day-to-day tradeoffs that define the job. These interviews were candid, detailed, and full of hard-earned lessons.

Not everyone has time to listen to every episode — so we created this ebook as a summary of what we heard. It's built around the biggest themes that kept coming up. Each section includes direct quotes from the CISOs themselves, offering a look into how they're making decisions, managing pressure, and leading teams in a constantly shifting landscape.

This isn't a vendor pitch or a hype piece. It's a snapshot of what security leadership really looks like right now. Let's get into it.

THANK YOU TO OUR CISOs

Jack Leidecker
CISO at Gong

Mario DiNatale
CISO at Odyssey Group

Nir Rothenberg
CISO/CIO at Rapyd

Bindi Davé
Deputy CISO at DigiCert

Dan Creed
CISO at Allegiant Travel Company

Joshua Brown
CISO at Spektrum Labs

Konrad Fellmann
VP of IT Infrastructure and CISO at Cubic

Partha Chakraborty
Former Deputy CISO at Natixis

Al Imram Husain
CISO & VP of Global Infrastructure at MillerKnoll

Vivek S. Menon
CISO & Head of Enterprise Data at Digital Turbine

TABLE OF CONTENTS

CHAPTER #1

THE CISO ROLE, UP CLOSE

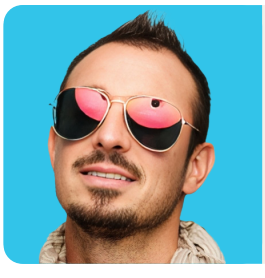
If you ask five people what a CISO does, you'll get ten different answers. Even among security leaders themselves, the role is constantly shifting. Some describe it as part technologist, part politician. Others say it's mostly risk management dressed up as cybersecurity. Everyone agrees it's messy, often misunderstood, and more about people and business strategy than tools and tech.

Across the conversations in this series, CISOs shared how they define the job, what they actually spend their time doing, and how they got into the role in the first place. No one followed the same path. Some started in consulting, others in compliance, others in red teaming or operations. But every single one had to learn how to connect security to the business in ways that resonate.

"I don't see my role as a security leader. I see my role as a business leader that happens to have a security background."

Jack Leidecker, CISO at Gong

That perspective came up again and again. The job isn't to enforce controls for the sake of it. It's to understand what the company needs to achieve and then figure out how to help them get there without leaving the doors wide open.



"A good CISO will look at risk and translate that into business value. That's when the organization listens."

Mario DiNatale, CISO at Odyssey Group

"I think the CISO has to help the business succeed. If we just scream 'no' all day, no one's going to bring us to the table."

Nir Rothenberg, CISO/CIO at Rapyd

A big part of the role is communication. Almost every guest talked about needing to bridge different languages. One for technical teams, one for executives, and sometimes another for the board. The pressure is real, but the expectations are often vague.

"There is no textbook to be a CISO. You're kind of thrown into the fire."

Bindi Davé, Deputy CISO at DigiCert

"As a CISO, you're in the middle. You're not at the top. You're not the bottom. You're in the middle trying to make both sides understand what the hell is going on."

Dan Creed, CISO at Allegiant Travel Company

Even defining what "secure" means can be a moving target. It often depends on who's asking.

"There's not always a clear finish line. What looks like good security to the dev team may be unacceptable to the board."

Joshua Brown, CISO at Spektrum Labs

"The CISO is there to say, 'Here's what we know, here's what we don't know, and here's the risk in both."

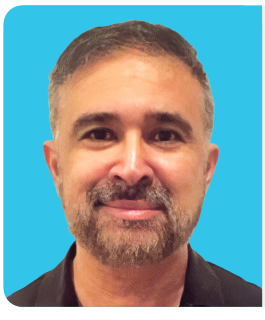
Konrad Fellmann, VP of IT Infrastructure and CISO at Cubic

For some, the toughest part isn't threat modeling or incident response. It's cleaning up what's already in place.

"What I found in many organizations in day one when I joined, having a PowerPoint diagram sometimes is considered to be architecture. Sometime calling someone who knows how the system was designed is something to be architecture. And in some time the information scattered across emails or 20,000 Word documents is also architecture."

Partha Chakraborty, Former Deputy CISO at Natixis

Al Imran Husain echoed the same frustration, particularly in environments with deep legacy infrastructure.



"You go into these environments where equipment's 20, 25 years old. No documentation. You're dealing with serial ports. You're dealing with air-gapped systems. There's no patching. There's no scanning."

Al Imran Husain, CISO & VP of Global Infrastructure at MillerKnoll

That disconnect—between what's ideal and what's actually there—is a core part of the job. The CISO doesn't just own security. They own the gap between what people think exists and what's really in place.

"Everyone's talking about zero trust and AI, but a lot of the job is still walking into the server room and figuring out what's even plugged in."

Vivek Menon, CISO & Head of Data at Digital Turbine

In the end, no two CISOs are doing the job the same way. But all of them are adapting constantly. They're aligning with the business, educating teams, and managing the gray areas no one else wants to own. As the role evolves, one thing is clear: this job isn't just about security. It's about making risk visible, actionable, and aligned with everything the company is trying to do.

CHAPTER #2

RISK, METRICS, AND THE BUSINESS LANGUAGE OF CYBERSECURITY

One of the most consistent topics across every CISO interview was the challenge of explaining risk in a way that the business actually understands. Technical teams can talk in terms of CVEs and control gaps, but that language doesn't always land with executives, boards, or even other departments.

CISOs spend a large part of their time acting as translators. They take complex, constantly shifting information about threats and controls, and find ways to connect it to business impact, operations, and outcomes. The goal isn't to simplify risk. It's to make it visible.

"The way that we've approached it is we kind of boil it down to what are the core services that the business delivers. And then try and understand what the top risks are to those services from a security perspective. And then align controls to that."

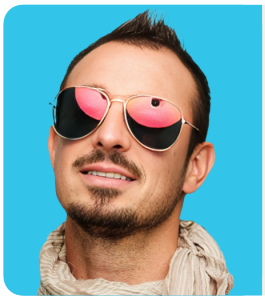
Konrad Fellmann, VP of IT Infrastructure and CISO at Cubic

Rather than talking about individual vulnerabilities or tools, Fellmann starts with what matters to the business and works backward. That pattern showed up in other interviews too: align with the organization's goals first, then frame security in that context.

"So I would start with the KPIs. Can you identify a set of KPIs, a set of principles, and some type of a charter or direction that says this is what we want to achieve from a business enablement standpoint."

Partha Chakraborty, Former Deputy CISO at Natixis

Metrics aren't just about tracking performance. Chakraborty's point is that they also signal direction. If the security program can't show measurable progress toward a defined business goal, it risks being seen as overhead.



"The only way you can tell your story is if you show value. The only way you can show value is if you are measuring something. And if you are not measuring anything, then it's your story versus mine."

Mario DiNatale, CISO at Odyssey Group

This quote cut to the heart of a problem many CISOs face. Security is often invisible until something breaks. Without metrics, it becomes a trust game. That makes the role harder and can erode credibility.

"I think the future of security is moving more towards business enablement. I think it's going to be less about how many systems did we patch this week and more about what outcomes did we enable."

Jack Leidecker, CISO at Gong

Leidecker's framing reflects a shift that many CISOs are pushing toward. Metrics need to show movement, not just maintenance. Boards and executives want to know how security helps the business move forward, not just how it keeps things from falling apart.

That doesn't mean abandoning technical depth. But it does mean layering it under a clearer business message. Risk reporting, dashboards, even incident postmortems all have to answer the same core question: how did this impact what the business is trying to do?

"You have to talk about risk in the same sentence as business. If you're not, you're not in the right room."

Nir Rothenberg, CISO/CIO at Rapyd

Security will always be technical at its core. But CISOs today are being asked to operate in executive environments where clarity, narrative, and alignment matter just as much. Metrics, risk frameworks, and communication strategy are now essential parts of the job.

If you can't translate security into business terms, someone else will translate it for you. And they probably won't get it right.

"You have to know how to speak to different audiences. I can't go to the board with a CVE. I have to go with impact — what does this mean for us financially, reputationally, operationally."

Bindi Davé, Deputy CISO at DigiCert

CHAPTER #3

AI AND THE EXPANDING ATTACK SURFACE

The hype around AI is impossible to ignore, but for CISOs, it is not just a technology trend. It is a fundamental change to the threat landscape. Across interviews, leaders described both excitement and unease. On one hand, AI introduces new tools and faster insights. On the other, it lowers the barrier for attackers and makes it harder to trust what you see.

Several CISOs pointed to AI-generated content and impersonation as an immediate threat. Deepfakes and synthetic media are no longer theoretical problems. They are starting to show up in phishing, fraud, and executive impersonation.

"People can replicate your voice and create synthetic voice messages of you. And if you're a high-value target, that can easily be weaponized against your organization."

Konrad Fellmann, VP of IT Infrastructure and CISO at Cubic

Other CISOs focused on the speed and scale of attacks. Large language models make it easier to craft targeted phishing or social engineering campaigns. That makes it harder to train people on what to watch for.

"You don't need to be a native English speaker. You don't need to understand cultural nuance. The LLM will handle that for you. That's a huge leap in capability for attackers."

Nir Rothenberg, CISO/CIO at Rapyd

Rothenberg also raised a concern that came up in other interviews: the tools being used to automate business processes can also be used to automate attacks. There is no clear line between the two.

"I think what we're going to see is AI being used to supercharge the work of malicious actors, in the same way it's being used to supercharge business productivity."

Nir Rothenberg, CISO/CIO at Rapyd

The challenge is not just anticipating what AI can do, but figuring out how to build controls without blocking innovation.

"We're trying to guide people toward responsible use. We don't want to be the team that says no to everything. But we do want to make sure people are asking the right questions before they plug a model into sensitive systems."

Joshua Brown, CISO at Spektrum Labs

Some CISOs are starting to experiment with AI in defense. That includes simulations, threat modeling, and faster detection. But they were also realistic about the limits.

"You can use LLMs to simulate phishing attacks and adversarial behavior. That's powerful. But you still need someone who understands the environment. The model can't do that for you."

Jack Leidecker, CISO at Gong

Most agreed that the tooling will improve. But no one saw AI as a silver bullet. The risks are real, the rules are still being written, and the attackers are not waiting for compliance frameworks to catch up.

"We can't assume this will be solved with a policy or a playbook. It's already moving faster than most organizations can track."

Mario DiNatale, CISO at Odyssey Group

CISOs are not waiting either. They are adapting their security programs to monitor new entry points, watch how users are interacting with AI tools, and prepare their teams to respond to risks that didn't exist a year ago.

This is not a future problem. It is already here.

CHAPTER #4

DEEPFAKES, ZERO TRUST, AND DIGITAL TRUST

In a world where anyone can spoof a voice, fabricate an email, or clone a user session, the question of digital trust has become central to how CISOs think about risk. Across these interviews, leaders returned to the same issue: we can no longer rely on static assumptions about users, devices, or networks. Trust has to be earned continuously.

The threat of deepfakes isn't theoretical anymore. It's showing up in phishing attempts, executive impersonation, and social engineering attacks that don't leave a technical trace.

"People can replicate your voice and create synthetic voice messages of you. And if you're a high-value target, that can easily be weaponized against your organization."

Konrad Fellmann, VP of IT Infrastructure and CISO at Cubic

Attacks like these blur the line between technical compromise and psychological manipulation. It's not just about code and controls anymore. It's about influence and deception, and the tools are getting more accessible every day.

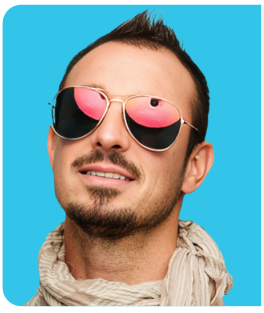
This shift has forced CISOs to rethink how access and trust are managed across the enterprise. Identity, posture, and context now matter more than location or role.

"Zero trust for me is not just a product. It's not just a marketing term. It is really about making sure that you have a good identity strategy. And then layering access on top of that with context and telemetry."

Jack Leidecker, CISO at Gong

Leidecker's definition moves beyond vendor messaging. For many CISOs, zero trust is less about a checklist and more about reducing assumptions. It's a mindset shift: verify everything, assume nothing, monitor constantly.

Several guests pointed out that old trust models are still baked into systems everywhere — especially in large, distributed enterprises.



“We’re still undoing years of implicit trust in legacy environments. Devices talk to each other freely. Credentials don’t expire. Admin rights are everywhere. It’s like a soft shell and gooey middle.”

Mario DiNatale, CISO at Odyssey Group

That metaphor came up more than once. The "soft inside" model may have worked in a perimeter-based world, but it breaks down under pressure from third parties, remote work, and cloud infrastructure.

“You can't assume trust just because someone is on the network. You can't even assume trust just because someone has a valid login. Everything needs to be verified.”

Nir Rothenberg, CISO/CIO at Rapyd

This constant verification creates friction, but it also creates clarity. Several CISOs emphasized the need to make trust decisions visible and reviewable — not just enforced in the background.

The job of a modern security team isn’t to block everything. It’s to build systems where trust is earned, not assumed. That means revisiting identity, rethinking architecture, and staying aware of how quickly attackers are adapting.

“We’re in an era where attackers don’t need to break in. They can log in. And if you’re not watching every step, you won’t know the difference.”

Joshua Brown, CISO at Spektrum Labs

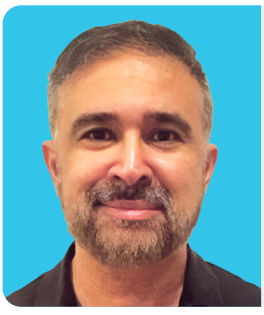
This is what modern trust looks like: not just encrypted tunnels and firewalls, but real-time context, visibility, and accountability. In this landscape, the old rules no longer apply.

CHAPTER #5

THE LEGACY TECH PROBLEM

If you've worked in a manufacturing environment or around critical infrastructure, you've seen it. Ancient control systems running unpatched software. Machines connected to networks they were never meant to touch. And vendors that disappeared years ago, leaving behind tech that's still holding up half the plant.

The challenge with legacy tech isn't just technical. It's cultural, operational, and economic. Replacing these systems is expensive. Disconnecting them is impossible. And securing them often feels like trying to build a firewall around a toaster.



"You go into these environments where equipment's 20, 25 years old. No documentation. You're dealing with serial ports. You're dealing with air-gapped systems. There's no patching. There's no scanning."

Al Imran Husain, CISO & VP of Global Infrastructure at MillerKnoll

This was one of the clearest themes in our conversations with CISOs who've worked in operational technology (OT) or hybrid environments. Many inherited systems where security wasn't even part of the original architecture. The protocols were open, the devices trusted everything, and no one expected to need MFA in a factory.

"We had everything from water treatment systems to conveyor belts being managed by Windows NT and XP boxes. We were told not to touch them. Don't reboot them. Don't even run AV."

Joshua Brown, CISO at Spektrum Labs

In these environments, visibility is often limited and change control is brutally slow. Even small updates have to be coordinated across engineering, operations, and safety teams. That makes proactive security feel like threading a needle.

"OT systems weren't built for change. They weren't built to be patched weekly. They were built to run for decades without touching them."

Partha Chakraborty, Former Deputy CISO at Natixis

Chakraborty pointed out that even when organizations want to modernize, the incentives aren't always aligned. In industrial environments, downtime means lost production — and security upgrades rarely get prioritized over uptime.

"If you tell a plant manager that you need to take something offline for security, the first question is, how many hours of production are we losing?"

Mario DiNatale, CISO at Odyssey Group

The convergence of IT and OT has made these gaps more dangerous. Once-isolated systems are being connected to analytics platforms, remote monitoring tools, and vendor-managed services. That creates new value — but also new exposure.

"The minute you plug in a dashboard, you've expanded the attack surface. And the more devices you connect, the more you have to assume compromise is possible."

Konrad Fellmann, VP of IT Infrastructure and CISO at Cubic

Security teams are trying to catch up, but the reality is that OT environments are years behind IT. And they don't follow the same rules. You can't scan production networks like you do in a cloud environment. You can't reboot things without risking safety incidents.

"This isn't just about applying IT best practices to OT. That mindset will break things. You need people who understand the physical and digital layers."

Dan Creed, CISO at Allegiant Travel Company

CISOs working in these environments aren't just defending data. They're defending uptime, safety, and often national infrastructure. That raises the stakes and complicates every decision.

Legacy tech may not make headlines like AI or ransomware. But for many CISOs, it's the real front line.

CHAPTER #6

REGULATION, COMPLIANCE, AND THE POLICY BOTTLENECK

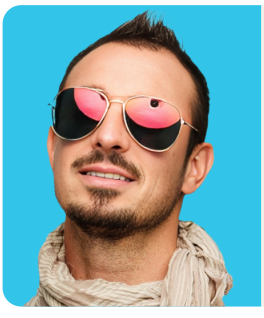
No matter how fast threats evolve, security policies tend to lag behind. Most of the CISOs we spoke with had strong feelings about compliance frameworks, certification regimes, and regulatory demands. The consensus was clear: regulation is necessary, but it often adds complexity without always improving outcomes.

Multiple guests described the widening gap between what's required for compliance and what's actually needed for security.

"The compliance frameworks are a minimum bar. They're not designed to keep out modern attackers. They're designed to make sure you have your paperwork in order."

Konrad Fellmann, VP of IT Infrastructure and CISO at Cubic

Even frameworks that were once considered gold standards are now being re-evaluated. One issue CISOs face is the shrinking certification lifecycle. Annual audits are no longer enough. Customers, partners, and regulators are asking for near-continuous assurance.



"You get SOC 2 certified and six months later someone wants to know if anything's changed. And then three months after that, you've got a new vendor audit. It never ends."

Mario DiNatale, CISO at Odyssey Group

This constant churn creates real friction. Compliance teams are pulled into cycle after cycle of evidence collection and policy review, often at the expense of forward-looking strategy. And security leaders are stuck managing checkboxes while threats keep moving.

"I don't think any CISO wakes up excited to fill out an Excel sheet for another audit. But that's what the job becomes if you don't push back."

Nir Rothenberg, CISO/CIO at Rapyd

"Sometimes it feels like we're spending more time preparing for audits than actually reducing risk. That's not sustainable."

Bindi Davé, Deputy CISO at DigiCert

The problem isn't just the number of audits. It's that policies often fossilize. They get written for a certain architecture or vendor, and then they stay locked even as the environment changes. That disconnect shows up during real-world response scenarios.

"We had an incident where we needed to isolate a system quickly. But the policy required three approvals. By the time we got the green light, it was too late."

Joshua Brown, CISO at Spektrum Labs

Many CISOs spoke about the importance of designing policies that are operationally aligned — not just auditor-friendly. The goal isn't to avoid scrutiny. It's to build systems that can adapt while still proving their integrity.

"I want controls I can show to an auditor and trust in a breach. If I have to choose, I pick the latter."

Jack Leidecker, CISO at Gong

Security that's only compliant on paper is fragile. CISOs are calling for better alignment between policy and practice, faster revision cycles, and audit models that reflect real risk — not just historical precedent.

This isn't about ignoring compliance. It's about designing it to move at the speed of the threat.

CHAPTER #7

WHAT KEEPS CISOs UP AT NIGHT

CISOs live in a state of high alert. Even when everything looks fine, most are mentally preparing for the moment it won't be. That's not just paranoia — it's a job requirement. Across our interviews, leaders opened up about the weight they carry, the scenarios they fear, and the boardroom dynamics that shape their decisions.

"The stress level, the fact that you don't sleep well at night, the fact that you're always on call — that's just how it is. You know that a single decision or oversight could cost the company millions."

Konrad Fellmann, VP of IT Infrastructure and CISO at Cubic

Many CISOs spoke bluntly about personal liability. High-profile breaches don't just impact customers or revenue — they land squarely on the CISO's desk. Some described sleepless nights not because of active incidents, but because of the quiet.

"It's not the alerts that worry me. It's the silence. That's when I start wondering what we're missing."

Mario DiNatale, CISO at Odyssey Group

Others pointed to the pressure that comes with explaining complex threats to boards and executives who expect certainty in an uncertain domain.

"You've got fifteen minutes in front of the board, and they want a yes or no answer to something that's inherently probabilistic. That's the job. Translate chaos into clarity."

Nir Rothenberg, CISO/CIO at Rapyd

For some CISOs, what keeps them up isn't just what's happening inside their networks — it's what's happening in the world. Critical infrastructure, supply chain dependencies, and geopolitical instability are now core to the risk equation.

"We've seen attackers shift from data theft to disruption. Nation-state activity is now something you have to account for, even in private enterprise."

Joshua Brown, CISO at Spektrum Labs

Despite the pressure, most CISOs weren't cynical. They were realistic — honest about the tradeoffs, clear-eyed about the risks, and committed to building programs that could survive bad days.

But none of them pretended the fear goes away. It just gets managed.

CHAPTER #8

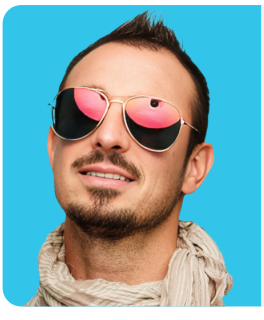
ADVICE FOR THE NEXT GENERATION

Security doesn't have a straight path in. Some come from engineering. Some from policy. Some stumble into it through incident response or help desk work. But if there's one consistent message from the CISOs we interviewed, it's this: curiosity, grit, and communication matter more than any one tool or cert.

"If you are naturally curious and if you really want to solve the problem, not just check the box, then you're going to be successful."

Partha Chakraborty, Former Deputy CISO at Natixis

Technical skill can be taught. But drive and resilience — the ability to keep learning and adapting — are harder to fake. Especially in an industry that evolves by the month.



"You can't be someone who just wants to stay still. You have to want to learn the next thing because the thing you're doing right now will be irrelevant soon."

Mario DiNatale, CISO at Odyssey Group

Several CISOs also emphasized communication as a defining skill — not just presenting slides, but knowing how to read a room, persuade a team, and explain tradeoffs clearly.

"The best security people I've worked with aren't just smart. They know how to talk to legal, to marketing, to ops. That's what makes them effective."

Joshua Brown, CISO at Spektrum Labs

Jack Leidecker pointed out that the next generation will also need to be comfortable navigating ambiguity. There won't always be playbooks. And that's the point.

"You have to be okay being uncomfortable. That's where the interesting problems are. If you want predictability, you're in the wrong job."

Jack Leidecker, CISO at Gong

One recurring piece of advice: don't chase titles. Chase environments that help you grow. Seek mentors. Read widely. Say yes to the hard problems.

"Find the place where you're stretched. Where you're not the smartest person in the room. That's how you get better."

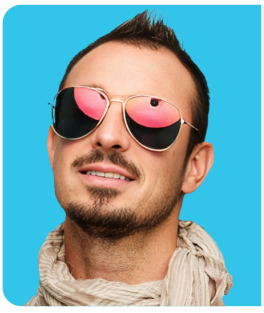
Nir Rothenberg, CISO/CIO at Rapyd

Whether you're trying to get your first SOC role or looking to move into leadership, the message from those who've been there is clear. The industry doesn't need more tool jockeys. It needs thinkers, translators, and people who give a damn.

CHAPTER #9

BUYING SMART — HOW CISOs PROCURE TECHNOLOGY

If you've ever tried to sell a security tool to a CISO, you know it's not a quick sale. Every guest we spoke to made it clear: they're not just looking for cool tech. They're looking for a fit — and a partner they can trust when things go wrong.



"I don't want another blinking dashboard. I want something that solves a real problem my team actually has."

Mario DiNatale, CISO at Odyssey Group

This sentiment came up again and again. CISOs are overwhelmed with vendors. Cold emails. Booth pitches. Promises. The ones who cut through aren't the loudest — they're the ones who ask good questions, listen, and adapt to the environment.

"Come in with humility. Show me you understand what kind of business we are. Don't treat me like a persona from your pitch deck."

Nir Rothenberg, CISO/CIO at Rapyd

Most procurement cycles start with a problem. That problem gets mapped to potential solutions. From there, it's about proving it works — usually with a lightweight proof of concept or pilot.

"If you can't show impact in 30 days, I'm not buying. Period. I need to see something move — alerts get better, detections get tighter, time to respond shrinks."

Joshua Brown, CISO at Spektrum Labs

Budget is part of it. But time and credibility matter more. CISOs are building mental models of vendors based on every interaction — especially how they behave when the deal slows down or hits friction.

"I always notice who still shows up after we say no. That tells me more than the demo."

Partha Chakraborty, Former Deputy CISO at Natixis

Jack Leidecker stressed that a good procurement process has to involve more than the CISO. His team, operations, and finance all need to see value — and risk — clearly.

"If I can't explain why this matters to my CFO and my SOC at the same time, I'm not ready to buy it."

Jack Leidecker, CISO at Gong

Across the board, CISOs want solutions that reduce complexity, not add to it. Tools that integrate well, don't require a six-month implementation cycle, and actually reduce analyst fatigue — those win.

The tech might be impressive. But if it doesn't fit the org, doesn't show value fast, or can't be explained simply, it's not getting bought.

CLOSING REFLECTIONS — WHAT WE'VE LEARNED FROM THE BREACH

Across every conversation, one truth kept surfacing: there is no single blueprint for cybersecurity. Every organization is different. Every CISO carries different scars. But certain lessons echoed across the board.

"If you think you're going to build a perfect program, you're going to be disappointed. You have to focus on resilience. Assume you'll get hit and plan for recovery."

Joshua Brown, CISO at Spektrum Labs

Resilience. Recovery. These ideas came up more than threat feeds or firewalls. CISOs are building not for prevention alone, but for continuity — for surviving breach events without burning down the business.

"Security is about making sure the company can survive its worst day. Everything else is tactics."

Mario DiNatale, CISO at Odyssey Group

At the same time, no one pretended this work is easy. Many leaders described tension between long-term strategic bets and day-to-day firefighting. They talked about burnout, decision fatigue, and second-guessing.

"Sometimes you're not sure if you're doing it right until something breaks. That's the nature of this role. You operate in the unknown, and you still have to make calls."

Nir Rothenberg, CISO/CIO at Rapyd

While technical strategies diverged, certain cultural values were consistent: transparency, humility, and a willingness to revisit assumptions. Nobody's stack was the same, but every strong program shared clear lines of accountability and high trust.

“The tech will change. What won’t change is the need to be honest about what’s working and what’s not. That’s where good security comes from.”

Jack Leidecker, CISO at Gong

Several CISOs left us with direct advice — not just for peers, but for anyone in the space. Some warned against complacency. Some reminded us that we’re all part of something bigger.

“You’re not securing a network. You’re securing trust — with your customers, your employees, your partners. Don’t lose sight of that.”

Partha Chakraborty, Former Deputy CISO at Natixis

No one gets this perfect. But what separates strong programs from the rest isn’t how they patch or scan or monitor. It’s how they think, how they lead, and how they respond when it all goes sideways.

The breach isn’t a question of if. It’s a matter of when. And what we’ve learned is that the best CISOs already know that — and build with that reality in mind.

Want To Keep Up With Our Latest Conversations?

LISTEN TO:

SUBSCRIBE