# Why cyber resilience is now a leadership competency: a Cybercrime Magazine podcast

Insight

**January 19, 2026**

**Category:** cybersecurity

**Tags:** ai, compliance, consulting, incident, podcast, resilience

Cybersecurity has a way of revealing uncomfortable truths about leadership. How decisions get made under pressure. Whether accountability is clear when something breaks. Whether preparation was real, or simply well-documented.

In a recent conversation on Cybercrime Magazine's Cyber Crime Radio podcast, host Paul John Spaulding sat down with Justin Greis, founder and CEO of acceligence, to discuss how cybersecurity, AI, regulation, and operational resilience are converging in the executive suite. What quickly emerged was that this is no longer a conversation about tools or frameworks. It is a conversation about leadership behavior – before, during, and after disruption.

Threats are accelerating. AI is compressing timelines. Regulatory scrutiny is increasing. Yet organizations that navigate incidents well are rarely the ones with the most sophisticated technology stacks. They are the ones whose leaders understand how their business operates, communicate risk clearly, and prepare their teams to act decisively when conditions deteriorate.

## Listen to the podcast

Cybercrime Magazine · Cybersecurity & Organizational Resilience. Challenges & Trends. Justin Greis, CEO, acceligence.

*Check out Cybercrime Magazine and their Podcast Channel on SoundCloud*

## The real failure point is rarely technical

**Paul:** You've worked with executives across industries. What patterns kept showing up that led you to found

acceligence?

**Justin:** There were really two things I kept seeing over and over, and they were related, but distinct.

The first was what CIOs and CISOs were dealing with inside their organizations. In most cases, they weren't confused about the risk. They understood the threat landscape. They knew where controls were weak, where technical debt was accumulating, and what needed to change. The issue wasn't insight – it was traction.

What consistently broke down was alignment with the rest of the executive team and the board. Cybersecurity conversations were happening in a language that made sense inside the function, but not at the enterprise level. Vulnerabilities, control maturity, tooling gaps – all real, all important, but abstract unless they were clearly connected to business outcomes. How does this affect revenue? How does it affect our ability to ship product, serve customers, or keep operating if something goes wrong?

When that translation didn't happen, cybersecurity stayed marginalized. Not because leaders didn't care, but because they couldn't see how to prioritize it alongside competing business demands. The moment the conversation shifted to business impact and risk tradeoffs, things changed. Decisions became faster. Alignment improved. And security stopped feeling like an endless cost center and started to look like a business enabler.

The second pattern I kept seeing was on the consulting side. The traditional advisory model was increasingly misaligned with what clients actually needed. We spent enormous amounts of time diagnosing problems that were already well understood, producing assessments and roadmaps that clients largely agreed with, and then handing them over at the exact moment when the real work should begin – getting leaders aligned and driving action.

That model made sense when getting to the "ground truth" was slow and expensive. It makes far less sense now. With the rise of AI and better data, we can understand an organization's environment, patterns, and risk posture far faster than before. The constraint is no longer analysis. The constraint is leadership alignment and execution.

What clients need today isn't more documentation of what they already suspect. They need help shaping the narrative, accelerating decisions, and moving the organization forward. That combination – leaders struggling to translate risk internally, and a consulting model optimized for diagnosis rather than action – is what ultimately pushed me to do something different.

The failure point wasn't technology. It wasn't even expertise. It was the gap between knowing and acting. And closing that gap is a leadership problem on both sides of the table.

## AI doesn't replace judgment, it exposes whether you have

## any

**Paul:** AI is moving fast, and there's a lot of concern around it. What are you seeing?

**Justin:** Most organizations are experimenting, but very few are realizing sustained value yet by traditional measures. The difference isn't whether AI is being used. It's how it's being used and who is using it.

AI is incredibly powerful when it's paired with experience. When experts challenge outputs, pressure-test assumptions, and use it to accelerate thinking rather than replace it. It becomes risky when it's treated as an authority instead of an assistant.

From a leadership standpoint, the work is defining boundaries. What decisions can AI support? Which ones must remain human-led? Where does accountability ultimately sit? Those guardrails shouldn't be static, because the technology won't be.

Avoiding AI altogether isn't a strategy. Neither is blind adoption. Responsible experimentation, grounded in expertise and clear expectations, is how organizations move forward without creating unnecessary exposure.

## You don't rise to an incident, you fall to your level of preparation

**Paul:** When cyber incidents occur, why do some organizations recover quickly while others struggle?

**Justin:** The difference is preparation. Incidents are not the moment to figure out roles, escalation paths, or decision rights. If that's happening in real time, you're already behind.

Scenario planning and tabletop exercises aren't about predicting the future perfectly. They're about familiarity. They force leadership teams to work through uncomfortable tradeoffs before the pressure is real.

I've seen organizations simulate scenarios they thought were highly unlikely, only to face them months later, almost exactly as imagined. The benefit wasn't that the incident was easy. It was that leaders weren't surprised. They had already debated the hard decisions.

Preparation doesn't eliminate disruption. It prevents paralysis.

## Boards don’t need certainty, they need clarity

**Paul:** Boards often ask, “Are we secure?” How should leaders handle that?

**Justin:** Any board asking about cybersecurity is engaging in the right conversation. The challenge is that “Are we secure?” implies a yes-or-no answer that doesn’t exist.

There is no amount of spending that makes an organization immune. What boards should expect instead is a clear, business-grounded view of risk. What matters most to the company? How is it protected? Where are the gaps? How are tradeoffs being made?

One of the hardest but most important things a leader can do in the boardroom is acknowledge uncertainty. Cyber risk is dynamic. You won’t always have all the answers. Transparency builds far more trust than overconfidence.

When cybersecurity is discussed in business terms, boards start asking better questions. That’s when governance actually improves.

## Compliance raises the floor, it doesn’t define success

**Paul:** With regulatory expectations increasing globally, how should executives think about compliance?

**Justin:** Compliance is necessary, but it’s not sufficient. Regulations establish minimum expectations. They are a baseline, not a strategy.

Organizations that treat compliance as the goal tend to optimize for checklists rather than outcomes. Strong security programs, on the other hand, produce compliance as a byproduct of thoughtful risk management.

Regulation can be a useful forcing function, especially for foundational controls. But if compliance becomes the ceiling of ambition, resilience will always be out of reach.

## Resilience starts with understanding how the business really works

**Paul:** Looking ahead, what will distinguish resilient organizations?

**Justin:** The most important capability is understanding the business end-to-end. How value is created. Where dependencies exist. Where failure would hurt the most.

Once leaders understand that value stream, resilience becomes a set of deliberate choices. Where redundancy makes sense. Where rapid recovery is enough. Where manual processes need to exist, even if they're rarely used.

Technology makes many of these options more achievable than they used to be. But technology doesn't create resilience on its own. Leadership decisions do.

## Closing reflection: cyber resilience can no longer be delegated (or relegated)

Cybersecurity is no longer something leaders can delegate away as a technical concern or relegate to a dark corner of a cold computer closet. It tests judgment, communication, and preparation under pressure.

AI is accelerating everything – including the consequences of poor decisions. Leaders who treat cyber resilience as a core competency position their organizations to absorb disruption with far less damage. Those who don't will be forced to learn when the cost of learning is highest.

Cyber resilience isn't about perfection. It's about readiness. And readiness is, unmistakably, a leadership responsibility.