From Hammer to Mission Enabler:

Reframing the Cybersecurity Practitioner Mindset

Whitepaper | April 2026

Avint LLC
205 Van Buren St., Suite 400, Herndon, VA 20170
571-287-7715 • www.avintllc.com

Author:
Marcie Nagel
Avint Founder and CEO
Email: marcie.nagel@avintllc.com
Phone: 571-287-7718

TABLE OF CONTENTS

1 A Call I Won't Forget

Not long ago, a cybersecurity practitioner I've mentored for nearly a decade called me at her breaking point.

She had spent the past year doing exactly what she believed was her job, pushing system owners and product teams to implement security controls exactly as written. Every conversation turned into a debate. Every requirement became a standoff. Progress was slow, tension was constant, and she felt like she was losing ground.

"I'm doing everything right," she told me. "So why does it feel like I'm failing?"

The truth was difficult, but necessary.

She wasn't failing because she lacked knowledge or work ethic. She was failing because she had been operating under the wrong paradigm.

And in that moment, I realized something harder: I hadn't taught her this lesson early enough.

2 The Hidden Trap in Cybersecurity

Many practitioners enter this field with a strong sense of responsibility. They are trained to understand controls, enforce standards, and protect systems from risk.

But somewhere along the way, that responsibility becomes something else.

It becomes control.

Practitioners begin to see themselves as enforcers, measuring success by how strictly they uphold requirements rather than how effectively they enable outcomes. They adopt the posture of a traffic cop, stopping progress in the name of compliance, often without the authority, ownership, or resources to actually implement what they are demanding.

This is the trap.

Because most cybersecurity practitioners, ISSO, ISSM, security advisors, do not own the system. They do not control the budget. They are not accountable for mission delivery.

Yet they are expected, and often expect themselves, to enforce as if they do. The result is a fundamental misalignment: responsibility without authority, accountability without ownership, and enforcement without control.

Over time, that misalignment creates friction everywhere it touches.

3 When Cybersecurity Becomes the Problem

When this mindset takes hold, cybersecurity stops being a support function and starts becoming a barrier.

Conversations with system owners become adversarial. Requirements are delivered as ultimatums instead of options. Progress slows, not because the mission lacks urgency, but because the path forward feels blocked.

Practitioners feel it too. The constant resistance, the lack of forward movement, the sense that no matter how hard they push, nothing changes. It leads to frustration, burnout, and ultimately disengagement.

At scale, the impact is even greater.

Critical capabilities are delayed. Outdated systems remain in place longer than they should. Costs increase as teams cycle through rework and stalled decisions. Trust between cybersecurity and mission teams erodes, and in the worst cases, cybersecurity becomes exactly what it was meant to prevent:

A self-imposed denial of service.

4 The Shift: From Enforcer to Mission Partner

Cybersecurity was never meant to be the function that says “no.”

It was meant to ensure the mission succeeds securely, intelligently, and with full awareness of risk.

That requires a different posture.

The most effective practitioners do not act as gatekeepers. They act as partners. They understand that their role is not to control outcomes, but to inform them.

At its core, the job is simple:

Tell the truth about risk clearly, credibly, and in context, so that those who own the mission can make informed decisions.

What they do with that truth is not yours to control.

And that is where many practitioners struggle.

Letting go of control does not mean lowering standards. It means aligning to reality. If you do not own the system, the budget, or the mission outcome, then your role is not to decide, it is to advise.

That clarity is what transforms cybersecurity from a source of friction into a force multiplier.

5 Start With Yes

One of the most practical ways to operationalize this mindset is through a simple principle:

Start with yes.

Not because every request is safe. Not because every idea should move forward unchanged. But because beginning with “no” shuts down the very collaboration required to make something secure.

When a mission or product owner brings forward a requirement, the question is not whether it perfectly aligns with policy. The question is:

How can this be done in a way that manages risk appropriately?

Sometimes the answer is a fully compliant solution. Other times it involves compensating controls, phased implementation, or an informed decision to accept a certain level of risk in order to achieve a critical outcome.

The practitioner’s role is to lay out those options, clearly and credibly.

To translate controls into risk.

To explain consequences, not just requirements.

To provide paths forward, not dead ends.

Because there is almost always a way to move forward.

6 A Lesson Learned the Hard Way

This wasn’t always clear to me.

Early in my career, I approached cybersecurity the same way many practitioners do, with a focus on enforcement. If the control said it needed to be done, then the expectation was simple: it had to be implemented.

It wasn’t until I was serving as a cybersecurity program manager supporting investigative systems within the FBI that my perspective changed.

In that environment, the systems we were securing were not theoretical. They supported real investigations—national security threats, crimes against children, and some of the most sensitive data in the government.

Delays had consequences.

There were moments where the “safe” answer, the perfectly compliant answer, would have slowed the deployment of critical capabilities. And in those moments, it became clear that being a roadblock was not neutral.

It was harmful.

The work required a different approach. We had to build security into systems that had never existed before. We had to make risk-informed decisions in real time. We had to balance protection with urgency.

And most importantly, we had to enable the mission, not stand in its way.

That experience reshaped how I see this profession.

Cybersecurity is not the mission.

It exists to support the mission.

7 What Changes When You Get This Right

When practitioners adopt this mindset, the impact is immediate and measurable.

Conversations change. Instead of resistance, there is collaboration. Instead of debate, there is alignment around outcomes. Practitioners experience less burnout because they are no longer fighting battles they were never positioned to win. They become trusted advisors rather than external enforcers.

Organizations benefit as well. Capabilities are delivered faster because security is integrated into the process rather than imposed at the end. Legacy systems are decommissioned more efficiently because risk is managed strategically. Costs decrease as friction and rework are reduced.

Most importantly, trust is built, and in cybersecurity, trust is everything.

8 What This Means for Us

If we do not teach this early, we set practitioners up for frustration. We create professionals who feel responsible for outcomes they cannot control, measured by standards they cannot enforce, and caught in a cycle that leads to burnout.

We owe them a better model.

For practitioners, this means shifting from enforcement to advisory. Starting with yes. Focusing on enabling outcomes, not simply implementing controls.

For those of us leading and mentoring, it means reinforcing this mindset early and often along with aligning expectations with the reality of the role.

9 Conclusion

Cybersecurity is at a crossroads.

We can continue to operate as enforcers, slowing progress, increasing friction, and exhausting the very people we rely on. Or we can embrace our true role.

Not as gatekeepers.

Not as traffic cops.

But as mission enablers.

The difference is not in the controls we implement.

It is in how we show up.

Start with yes. Tell the truth. Enable the mission.

10 About the Author

Marcie Nagel is the Founder and CEO of Avint LLC, a cybersecurity services firm supporting federal agencies in high-risk, highly regulated environments. With nearly 30 years of experience in cybersecurity, she has led large-scale programs across the Department of Homeland Security and supported investigative system security within the FBI.

Her work focuses on helping organizations move beyond compliance-driven security toward risk-informed, mission-aligned outcomes—ensuring cybersecurity accelerates, rather than hinders, mission success. She is passionate about mentoring the next generation of cybersecurity practitioners and reshaping the role of cyber as a true mission enabler.