THE MYTH OF OVERNIGHT SUCCESS: WHY TRUE SECURITY LEADERSHIP TAKES DECADES TO BUILD

By Amy Mushahwar, Chair of Data Privacy, Security, Safety & Risk Management, Co-founder of Data360, Lowenstein Sandler LLP


Amy Mushahwar

When a security leader becomes highly visible, people often assume something dramatic happened. They believe a specific moment created the rise. Visibility may spike suddenly. Execution may accelerate. Credibility, however, develops over many years of disciplined work that most people never see.

Success in cybersecurity, privacy and artificial intelligence governance is never immediate. I didn't go from a farm in Michigan to advising Fortune 500 companies overnight. It took years of study, trial, troubleshooting and pressure testing. It took the hard work that no one gets to see.

TWENTY YEARS OF LEARNING TO SPEAK ENGINEER

Early in my career, I was a technologist seeking legal assistance. When my company needed legal counsel, I realized that I needed to educate the lawyer about what my technical breakage risk meant for a small consulting shop with larger clients that had the capacity to sue if I made a mistake. Even then, I was keenly aware of the liability stakes. It meant my family's survival. My lawyer, however, didn't understand the technical disruption I was facing. It was the early 2000s; we had not yet fully articulated the concept of "breach," but the lawyer should have known that technical disruption can create detrimental legal risk.

It was then that I realized that lawyers who cannot "speak Engineer" will struggle to protect an enterprise. This insight shaped my development, and I went to law school. I spent years sitting with product teams, shadowing developers, learning how systems behave under stress and understanding how architecture decisions create regulatory and safety consequences. Before legal and technical fusion was a concept, I was already building this capability as a young lawyer explaining technical risk in an area where other lawyers thought the tech was too dense to tackle. First, I started in the telecommunication sector, wireless and satellite, and then payments, retail, government contractors and beyond. My experience across a variety of sectors has given me invaluable insights.

I did not gain legal-technical fusion fluency through certifications; I learned it from repetition and experience, and my time as a former CISO. I learned through hundreds of incident response calls, architecture reviews, engineering standups and practical exposure to system behavior. These experiences allowed me to translate engineering realities into risk decisions that leaders could understand.

CRISIS RESPONSE AS THE HARDEST CLASSROOM

Crisis is a challenging but powerful teacher in the security field. For two decades, I have helped companies weather ransomware events, data extortion, insider threats, destructive attacks, artificial intelligence misuse and operational failures. These moments reveal the strengths and weaknesses of an organization in a way daily operations never could.

Patterns become clear. Organizations fail when alignment breaks down. Technical teams often understand the risk long before leaders do. Lawyers who cannot keep pace with engineering create bottlenecks. Silence slows response. Precision without speed creates hesitation. Speed without clarity creates chaos. Over time, these observations form institutional knowledge that only comes from repeated exposure.

THE CONVERGENCE ERA

We now live in what I call the convergence era. Artificial intelligence governance, cybersecurity, safety, data ethics, regulatory enforcement, crisis communication and enterprise trust are no longer separate conversations. They share one ecosystem, shaped by technology and human behavior. Leaders who have worked across these fields for many years have been preparing for this moment long before it arrived. Rising visibility usually reflects alignment between long-standing preparation and current market needs.

DISCIPLINE AS A PROFESSIONAL OPERATING SYSTEM

Outside the office, I train in taekwondo and compete in triathlons. These disciplines influence how I lead. Strategy matters more than strength. Calm breathing supports good judgment. Loss teaches more than victory. A leader who exhausts energy too early cannot guide others through the highest-pressure moments. Security programs thrive when they are grounded in discipline rather than in adrenaline.

DATA360 AS A FRAMEWORK BUILT OVER MANY YEARS

I now lead Lowenstein Sandler's Data Privacy, Security, Safety & Risk Management practice, which includes our technical legal platform known as Data360, which unites technical and regulatory lawyers who collaborate seamlessly with engineering teams to deliver actionable, business-aligned advice. From the outside it may appear new but in reality, it is the structure I have been building throughout my entire career as both as a lawyer and a CISO.

The principles behind Data360 reflect lessons I have learned from two decades of observing how organizations behave under threat. Lessons such as respect engineering time. Combine legal reasoning with technical fluency. Prepare long before the crisis. Build playbooks with the teams who will use them. Align executives early. Treat safety as an asset that supports innovation, not only as a compliance requirement.

With this approach, I have saved organizations from bankruptcy during a breach, caught attackers, and saved software-as-a-service providers when a thousand or more B2B companies had the capacity to sue them. But the lessons I've learned as a legal security professional also translate directly to technical positions.

BUILDING CAPACITY BEFORE YOU NEED VISIBILITY

Security leaders cannot wait for a crisis to begin developing the capabilities that crisis will demand; by then, it will be too late. Here are three practices that build institutional capacity long before visibility becomes necessary:

- Embed your team with engineering during normal operations. Most security organizations engage with product teams only during architecture reviews or incident response. This creates a transactional relationship that breaks down under pressure. Instead, assign security engineers to attend product standups, participate in design discussions and understand how engineering teams make trade-offs between speed and safety. This investment pays dividends when you need engineering cooperation during a critical incident. Technical teams respond faster and more specifically to security leaders who already understand their constraints and speak their language.
- Document institutional knowledge before people leave. Organizations lose critical capability every time an experienced security professional departs. Capture decision frameworks, not just procedures. When your team handles a complex incident, document why certain decisions were made, what alternatives were considered and what assumptions proved right or wrong. Create case studies that show how context shaped response strategy. This transforms individual experience into organizational memory that survives personnel transitions.
- Develop executive understanding during peacetime, not during crisis. Leadership teams that discuss security only during breach response will struggle to make good decisions under pressure. Use tabletop exercises, realistic scenarios and structured discussions to help executives understand how security decisions connect to business risk, before an actual incident forces those conversations to be reactive and impulsive rather than calculated and controlled. Leaders who have practiced these discussions in low-stakes environments make better choices when real consequences are in play. These practices require time and patience. They do not generate immediate visibility. They build the foundation that allows organizations to respond effectively when visibility arrives, whether or not they invited it.

AS REGULATORY REQUIREMENTS CONTINUE TO EVOLVE, HEALTHCARE LEADERS MUST REASSESS THEIR LIABILITY COVERAGE.

THE TAKEAWAY FOR ENTERPRISE LEADERS

If I could offer one message to security and technology leaders, it would be this: Visibility should not be confused with readiness, and reduced visibility does not signal weakness. The future belongs to leaders who have invested in building capacity long before anyone noticed.

Success in security is the result of many small, disciplined choices. What appears to be a sudden rise is usually the moment when preparation and opportunity finally meet.

True security leadership does not happen overnight. It is constructed patiently and consistently over many years. ES