PROFILES IN *Confidence*

CASSIE CROSSLEY

VP SUPPLY CHAIN SECURITY
Schneider Electric

Global Headquarters: Rueil-Malmaison, France

Employees: 150,000+

Annual Revenue: $41.2 Billion

BRIDGING CODE AND CONVERSATION

When Cassie Crossley began her career decades ago as a software developer, it quickly became clear that while she loved technology, sitting in silence to write lines of code wasn't her calling. "I'm an extrovert," she says with a laugh. "Back then, project managers didn't exist. It was just, 'Here's the dev manager, now go code.' I couldn't sit still long enough."

That restless energy and need to connect with people would become a defining thread in her career, weaving together deep technical expertise with an intuitive grasp of change management, governance, and strategic thinking. Today, as Vice President of Supply Chain Security at Schneider Electric, a multinational specializing in energy management and industrial automation, Cassie is leading global efforts to secure both hardware and software supply chains.

She's spent nearly 15 years at the company, moving through six different roles that reflect her hunger for challenge and transformation. "When I get bored, I switch gears," she says. "I've always been drawn to complex problems, especially at the intersection of technology and people."

A FOUNDATION IN TECH AND PEOPLE

Her journey into cybersecurity was not a straight line. After leaving software development, she found her voice at Lotus, working in technical support and documentation, Cassie says, "I loved being on the product side, talking to users, improving how things worked."

However, Cassie's first exposure to security came in the 1990s working at McAfee. "We didn't call it cybersecurity then. It was just virus scanning software," she recalls. From there, she moved into project and program management, eventually leading multi-million-dollar initiatives.

At Schneider Electric, she started as a Program Management Office Director and later transitioned into cyber governance, writing the company's IT cybersecurity policies and launching a 'crown jewels' initiative focused on protecting priority applications and data. "This was before CISOs were common in big companies," she explains. "A lot of the early CISOs came from network engineering. I came from governance, change management, and a desire to understand systems holistically."

ARCHITECTING SECURITY FROM THE INSIDE OUT

Six years ago, she shifted her focus from internal IT to product security. In a company with 14,000 R&D employees and dozens of product lines, her team implemented Secure by Design principles, developed secure development lifecycle processes, and curated a training catalog hundreds of hours deep.

Then came the pivotal merger of two security teams, IT and product, which led Cassie to take on her current role: heading global supply chain security. "We're selling into critical infrastructure and governments around the world," she says. "It's not just about the software you're building. It's about where the hardware comes from and how everything is integrated."

Her work now spans continents and disciplines, engaging with regulators from countries like Australia and Singapore, helping define global standards for software and hardware transparency. She worked closely with NIST on its Cybersecurity Framework 2.0, helped shape the CISA Secure Software Development Attestation Form, became a leader in the software bill of materials (SBOM) movement, and has helped governments define IoT labeling baselines.

SILENT RISKS IN THE SUPPLY CHAIN

When asked what security risk is quietly growing in importance, Cassie doesn't hesitate: "Supply chain security. We've heard about it, but the deeper issue is traceability. Most of the chips in our devices aren't high-end AI chips. They're simple processors made years ago, often with embedded firmware from third or fourth-party vendors. And they're everywhere in cars, buildings, and power systems."

This, she says, creates a ticking clock around product longevity. "We've gotten used to disposability, but that doesn't work when digital components are embedded in physical products. You can't just replace a car every five years. What happens when a chip manufacturer goes out of business? Who maintains that firmware?"

Cassie believes this is a problem few consumers and too few executives fully understand.

BOARDROOMS AND BLIND SPOTS

That disconnect extends to the C-suite. "Boards know how to assess a company's financials and external cyber hygiene," Cassie explains. "But when it comes to product development, especially in large companies with hundreds of dev teams, there's no visibility. One team might follow secure architecture principles. Another might not."

Cassie has seen countless third-party security assessments filled out, with companies offering vague reassurances at the global level. "We'd say, 'We do this process globally, but if you want product-level details, let us know.' Nobody ever came back to ask."

She argues that boards need to take a much more active role in understanding digital dependency and resilience. "What happens if Microsoft Teams or Outlook goes down for a week? If your supplier's supplier was using CrowdStrike during the failure? Boards aren't asking those questions. They don't know what's under the hood."

BUILDING RESILIENCE BEFORE IT'S TOO LATE

Cassie is adamant: cybersecurity needs to be embedded across the business, from policy to product, and from governance to grassroots development. She views supply chain not as a checklist, but as a living ecosystem of hardware, software, and global regulation.

Her philosophy? "Ask what you can't live without for a week. Prioritize from there."

With her background in both communication and technology, Cassie is uniquely positioned to navigate this evolving terrain. She may have left software development behind, but she never stopped building, only now, she's architecting the security of the future.