IBM's Royce Curtin on building a strategic security program

Discover how IBM has built an industry-leading security program focused on people, partnerships, and driving business resilience.

Not too long ago, security was viewed as a reactive function — something to be addressed after a breach, theft, or disruption had occurred. But in a world where threats are global, multifaceted, and increasingly unpredictable, a proactive, strategic approach is essential.

IBM Chief Security Officer and VP of Corporate Security Royce Curtin is at the forefront of what it means to lead a strategic security program. With a background that spans three decades in the corporate private sector, FBI, and U.S. military, Royce is skilled in leading enterprise corporate security teams. He's a change agent and role model for other security leaders – particularly those at global organizations.

Together with Securitas, Royce spearheaded the launch of the world's first global Vested security agreement, an innovative approach to enterprise security that focuses on shared goals and outcomes rather than traditional transactional buyer/seller agreements.

We sat down with Royce to learn more about how he's been able to gain stakeholder buy-in, build an industry-leading security program, and elevate the role of security in a global enterprise.

Security as a competitive advantage: Insights from IBM

Reflecting on your own journey in security, what personal philosophies or experiences have guided you in shaping IBM's security program?
My principal focus is always people first. This means understanding their unique expertise, looking for growth opportunities to develop the next generation of leadership, making sure people are heard and valued, and creating an environment where people are comfortable coming forward with problems or concerns.

I feel transparency and being an active listener pay immeasurable dividends in building teams, supporting their missions, and maturing their professional growth. I want to create an environment where people can be bold, take risks, fail, recover, and thrive. When I look at my team and see people with the right skills, in the right roles, who are supported and empowered, I know we have a winning formula that's gratifying and inspiring.

My thinking is always: What's in it for we?

How do you communicate the value of security as an investment in the company's future rather than just an operational expense?
Security is a proactive investment. It is a force multiplier. It accelerates and enables the business to move faster. It's part of the trust factor of our business value proposition to clients. Clients want more than just great products, innovation, and exemplary consultancy – they want to know the company they're partnering with invests robustly in security. That its offerings, infrastructure, and data integrity are secure by design and continuously measured against a dynamic threat landscape to adjust controls at speed to keep data and the enterprise secure.

What advice can you offer to other security leaders who are striving to elevate the role of security within their organizations?
We as leaders have to be able to articulate value for money – it's about communicating the "why." We use real data and cite real-world examples to show that there's a direct correlation between security costs, and risk identification, response, mitigation, service recovery, and resiliency. Thoughtful and efficient security contributes to strong brand reputation.

Can you discuss the role that security plays not just in protecting people and assets, but in driving business resilience?
Business resilience is an important part of any security program. We focus on understanding and deploying security controls that protect our people, facilities, technology innovation, IP, and more, but, also make sure we have robust plans to respond to business disruption.

You have to build, maintain and exercise the right partnerships with business units and shared services across the enterprise to ensure continuity plans identify the issue quickly, deploy appropriate mitigations, and ultimately restore client and business services as quickly as possible.

A robust security plan is critical to our business and a very important assurance we make to our clients.

IBM is charting a new path forward for the industry with the Vested partnership model, which shifts away from traditional security models that have been largely transactional in nature. Why do you believe this is an important next step for IBM?
Moving away from transactional relationships into this Vested methodology gives us bi-lateral flexibility. It allows us to specify requirements to secure the enterprise and our people, and it gives Securitas flexibility to deliver those requirements using a combination of assets – including physical guarding, security technology, or various other incident response tactics.

We established requirements and built key performance indicators to make sure we get the full value of the contract. Securitas has the ability to maneuver across a broad set of tools in their portfolio to deliver security to mutually agreed standards and KPIs, tracked by a governance team representing both sides. This ensures continuous performance measurement, accountability and delivery against contract terms.

In closing, what's the most important component of a strategic security program?
People at all levels, period. Our operators, mid-level managers, executives, contractors, suppliers, internal stakeholders, and external partners. We invest significant energy in these relationships to ensure they're healthy, open, transparent, and informed. And, we emphasize servant leadership – building an inclusive environment where our people and teams are empowered, supported, and challenged to stretch into new, uncomfortable space to take risks and achieve incredible outcomes. We align their talent to business needs, celebrate their successes, learn from failure, and encourage them to be bold explorers.

"Security is a proactive investment. It is a force multiplier."

Royce Curtin
Chief Security Officer and
VP of Corporate Security, IBM