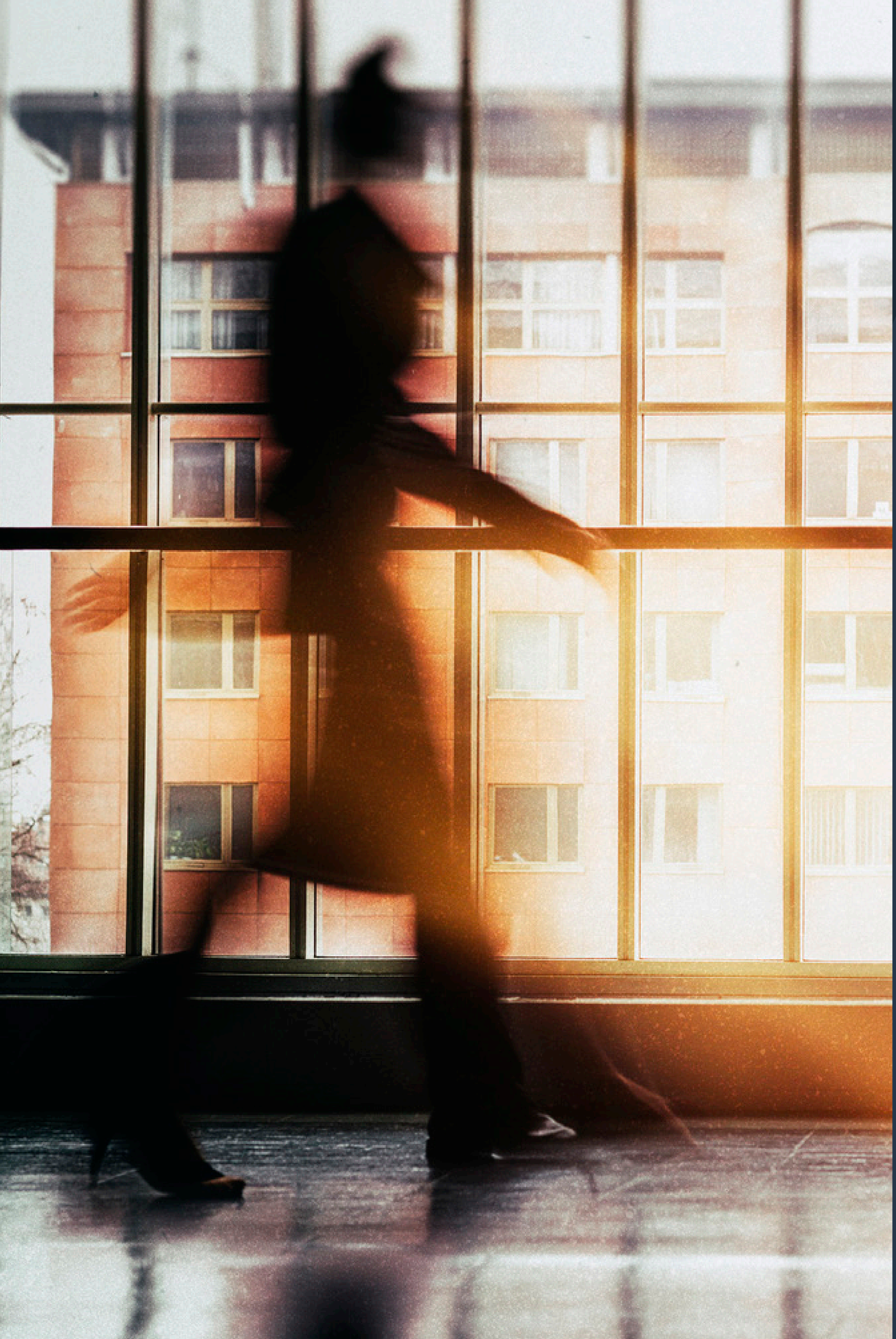

Cultivating Security Leadership

How enterprise CISOs are going beyond security systems—and investing in their people—to safeguard their organizations

Security leadership is a collective pursuit.

What matters most to Chief Information Security Officers—operational excellence? Business continuity? Staying out of the headlines? Maybe it's all of the above.

The role of CISOs is to help guide the board and their peer C-suite leaders as they proactively protect their brands and customers.

With the exponential growth of data in today's businesses, there has been a new emphasis on IT's role in securing that data. Security, which used to be more infrastructure-centric, demands a new focus on software, and technology leaders have to be deeply involved in software development and investments.

At the same time, security teams also require different skills and mindsets to succeed in new domains. So, while they might be technologists first and foremost, the most successful CISOs recognize that strong security goes well beyond bits and bytes.

Stephen Schmidt, CISO, Amazon Web Services, shares three key behaviors of security leaders:

1. **THEY LOOK AHEAD**—they do not wait to address risks to the organization. Instead, they lean in on emerging research and threats to stay ahead, while keeping compliance and regulatory requirements front of mind.

2. **THEY INVEST IN PEOPLE**—collaboration is critical in security, and they recognize security teams need to work well with CIOs, IT teams, and other groups.

3. **THEY ACT FAST**—risk decisions need to be made quickly, and security leaders do not delay. When things escalate, they use their relationships and experience to pick up the phone and address the problem.

WHY IS IT IMPORTANT TO CULTIVATE SECURITY LEADERSHIP?

Most CISOs wear many hats: guardian, strategist, and technologist, but it's the role of mentor that often gets left behind.

This is especially problematic when a Black Hat survey indicated that 73% of organizations need more skilled security talent. Investing in people is a good way to both prevent turnover and continue building the organization's strong security apparatus into the future.

And more importantly, in an increasingly competitive environment, CISOs can't expect to act as the sole guardian at the gate. Sharing knowledge, encouraging a diverse skill set, and building a talented team increases agility and adaptability. At the end of the day, these habits make the business far more secure.

Let's meet two security leaders who recognize that advancing talent is just as important as investing in technology.

Giving Security the Airtime it Deserves

Paul Lynch

GROUP CISO &
GROUP TECHNOLOGY DIRECTOR
ITV

Paul Lynch discusses the unlikely route to his role, why it's given him a unique perspective, and how he advocates for security at a broadcasting powerhouse.

Business first, security second

Unlike many CISOs, Paul's journey didn't begin in security. His roots are firmly planted in the business, where for a time he led operations for Video on Demand at ITV, the largest commercial broadcaster in the United Kingdom.

The way he sees it, that route turned out to be a scenic one, particularly when it comes to leadership. Early on, he was exposed to business disciplines and challenges like corporate governance, digital transformation, and strategy development, all of which have served him well in leading security.

"The CISO role doesn't require deep tech knowledge on a day-to-day basis," Paul says. "It's much more about alignment with the wider business." So, while he oversees teams of solid technologists, he believes they need to be business leaders first and security experts second. That means embedding his people in business teams and including them in steering boards, audit committees, and senior-level meetings. This allows them to observe the nuances of conversations and gain visibility among leadership.

> "
>
> As technical literacy rises throughout organizations, I want my team to consist of effective change agents."

Know your audience

In the world of the modern enterprise, security can—at times—fight uphill battles with executives and employees who, instead of viewing security policies as protective and benign, see them as limiting to the business. For Paul, a big part of overcoming this as a security leader is to simply acknowledge and appreciate your environment.

For the highly creative folks at ITV, Paul thinks carefully about the kinds of programs he chooses and how he messages them; how he embeds them and how he makes them stick. “At a creative company like ours, a CISO can’t just walk up and do cybersecurity by the numbers.”

To win security advocates across the organization, Paul and his team built an experience in lieu of a traditional program. Employees are immersed in a cybersecurity exercise that has them “locked” in a room until they solve a series of real-world security challenges using various clues and tools. This gives them tangible insights into how cybercrime actually happens. It also appeals to their creative spirit and inquisitive nature.

“

Our people want a more experiential path.”

Get comfortable with being uncomfortable

The world of corporate security has unique challenges, fraught with unexpected events or difficult circumstances that arise. Apart from the constant threat of cyberattacks that could damage the business, ITV is in a transitional period when it comes to technology.

Like most organizations, ITV still operates some of its business on legacy systems that are a decade old. The adoption of cloud, SaaS, apps, and mobility continues to open a lot of possibilities, but at the same time poses many new challenges in security.

It's only natural for security people to want to solve every problem, and solve them quickly. "Not so fast," is Paul's first piece of advice to his team.

"When I see young security professionals coming up, they have a burning desire to fix everything, make everything right, and take all the risk away," he says. "What I have to remind them is that it's not possible or practical." Even beyond that, he tells them that what they're trying to do might not be what the company needs.

"Businesses have to take risks to evolve and stay relevant. That can make it uncomfortable for us in security." So, his next piece of advice? Adjust your expectations, assume positive intent, and get cozy in the grey area.

What has Paul learned about leadership by working with AWS?

"

In security, time is our most valuable resource. AWS gives me back time."

ITV began their relationship with AWS back in 2011. Since then, they've expanded their partnership into many parts of the business—not just web and online, but also in broadcasting and delivery of ERP systems. In fact, together they built a talent payment system from the ground up.

Paul recalls when AWS experts showed up on site to walk the ITV legal team through security controls and features to ensure they knew how to protect their data and platform. To him, this hands-on, customer-centric approach to security has helped to shape his own methodology within ITV. "Working with AWS has been incredibly helpful."

"Also, I need to invest time in moving the business forward," he says. "With AWS, I don't have to worry about basic security hygiene anymore." This frees Paul to focus on identifying and growing leaders on his team, aligning with business groups, and securely launching new products and services.

Finally, for Paul, building security in from the beginning is essential. AWS—combined with strong leadership—has helped make this possible.

Sainsbury’s

Putting Security Before the Cart

Mun Valiji
CISO
SAINSBURY’S

Mun Valiji shares his mission to make security a central strategy at Sainsbury’s through the power of business-driven communications.

Make security central to your digital business strategy

A 20-year security veteran, Mun is more than familiar with the ever-changing nature of the security landscape. It's not just that threats evolve, or that new risks arise, it's also that organizations themselves transform, especially now as they digitize products or services.

For him, security and transformation are inseparable—security must be deeply embedded into the fabric of every digital business.

That perspective has served him well in his current role as CISO of Sainsbury's, one of the UK's largest retail organizations that provides customers a wide range of products and services including grocery, general merchandise, homeware, loyalty and financial services. Sainsbury's Tech team are leading the transformation of Sainsbury's through innovative solutions to become the UK's No.1 Multi-Brand, Multi-Channel business.

"I work essentially as a trusted advisor to the business. That makes for a very progressive, customer-and outcome-driven relationship where security, privacy and trust are at the center of discussions."

> "
>
> If we look to develop our brand and our capabilities, or to build respect in the market, security has to be at the center of that proposition."

Technical credibility is a given; business acumen is a must

Placing security at the center of the business' agenda takes a special kind of leadership mindset. For Mun, security leaders cannot be technology experts alone—their expertise must be coupled with an in-depth understanding of the business and a pragmatic view of risk.

In his view, technological expertise provides the necessary credibility to be given a seat at the table. But by itself, it's not enough. "What's more important is having the commercial and business acumen to be able to abstract what's essential to the business in the face of an ever-complex threat landscape."

> "
>
> Being able to rationalize and assimilate business information out of technical data is more important than having all the data on hand."

That is, security leaders need to be able to speak the language of business. Without it, executive-level discussions will miss an opportunity to show the impact and value of security investments to the business.

When he brings together his leadership team, Mun likes to over-index on this skillset, spending time talking about non-IT issues, teaching his people how to map back to the customer what they're delivering, and framing outcomes through a business lens.

Communications have the power to demystify a "dark art"

Getting security to sit at the center of business strategy can only happen through sustained and open communications. Serving as that trusted security advisor to the business means that Mun regularly engages with executives and the board to explain security strategies and investments.

In fact, it's not just top-level leadership that is the focus of Mun's communications. His open-door policy means in the same day he might talk security with the CIO and a Sainsbury's Tech field engineer—all important to bringing clarity to the world of security, a space that for most people is still mysterious, something akin to a "dark art."

But communication doesn't just start and end with Mun. When building his leadership team, he looks to bring in people with strong interpersonal skills. While technical skills can always be enhanced or taught, soft skills are an absolute requirement. This is particularly important since Mun's UK team is highly distributed—good communication practices are critical for team cohesion and understanding.

In the end, it's using communications to change mindsets when it comes to security. "It's about having a vision led by culture change—making sure the company understands the value and importance of security and taking people along on the journey."

Challenging their security thinking with AWS

"

AWS helps me be the best leader I can be as we work together to shepherd Sainsbury's on its journey to embracing the cloud securely."

Sainsbury's relationship with AWS goes back to 2016. Using cloud is still a relatively new practice within Sainsbury's yet adoption has happened on an accelerated timeline compared to other internal projects.

The company enjoys a very close working relationship with AWS, connecting regularly, sometimes daily or multiple times a week across teams. The support has benefited both organizations. Mun notes that Sainsbury's has learned a lot from Amazon's cross-industry experience in security, which has allowed them to check or adjust their own thinking when it comes to security, as well as gauge their progress relative to their peers.

"Our AWS relationship has helped me across multiple levels," said Mun, "making sure Sainsbury's Tech are doing the right thing strategically, from how we're positioning our security investments, to whether we're making the appropriate choices, or even to tap into the AWS team's expertise on ways to remain best-in-class."

Also, feedback and requests from the Sainsbury's Tech team has enabled AWS to productize those ideas, enhancing existing services and releasing new product features as a result.

IN CLOSING

Use the AWS Cloud to transform the way you do business. Automate security and compliance tasks to reduce risk so you can innovate faster and free up the resources to focus on important areas, like cultivating future security business leaders.

Learn more

AWS Security and Compliance website

Engage your team

Security Fundamentals Course

AWS Tech Talks | Webinar YouTube Channel

AWS Certifications

AWS Certified Security Specialty Certification

Security Operations on AWS