Industry insights

Q&A with IBM Global Security Technology Lead

The state of the physical security industry is changing. In this Q&A, Steve Riley discusses some key findings from a recent industry survey. He also shares what's next for IBM and where they're focusing security investments in 2023.

We sat down with Steve Riley, Global Security Technology Lead at IBM Corporate Security, to get his insights on how IBM is overcoming some of the common challenges we discovered in the State of Physical Security Report and what they are focusing on for 2023.

Steve has worked in the industry across various organizations and roles for over 27 years. And today, as new opportunities and challenges come up, he's leaning on this experience to adapt and lead his team forward.

Q: What are some important changes you've seen within the industry?

A: There's clearly still an element of reluctance from many to move to the cloud. Some have maybe dipped their toes in it and trialed a small proportion of their deployment in the cloud. But going full cloud is still being seen as a challenge and a risk. We're facing these same challenges and risks at IBM, but we still want to move in the direction of the cloud.

Cybersecurity is also a top requirement. We all need to maximize the value of the cybersecurity features within our physical security products and IoT devices and adhere to cybersecurity best practices to protect the communication between those systems and devices.

Then, there are the challenges of product shortages over the last couple of years. Right now, it's all about catching up with the projects that were scheduled to be delivered or potentially delayed. This requires more foresight and planning and building a roadmap to recovery.

Q: What differences have you noticed within your job since integrating specialized roles?

A: We've recently integrated more specialized IT expertise into our physical security department. And this has been quite essential for us to move towards a more global hybrid-cloud environment.

The key skills that we brought in are cloud SMEs. Our own internal IT teams have also been incorporated into our technology teams or physical security technology teams. They've played a pivotal role in how we architecturally deliver our solutions globally. That includes building resilient networks and ensuring we capitalize on all the cutting-edge features within edge technology, operating systems, applications, and hardware.

These skills are increasingly in demand within IBM. We first started with a few SMEs within the video surveillance and access control functions. But we're now bringing in cloud and data specialists. As we upgrade globally, we also want to enhance how we manage our portfolio of products, so we're keen on finding more resources to oversee asset management and future upgrades.

Q: IBM is a cloud-first company. What is the primary driver for this strategy?

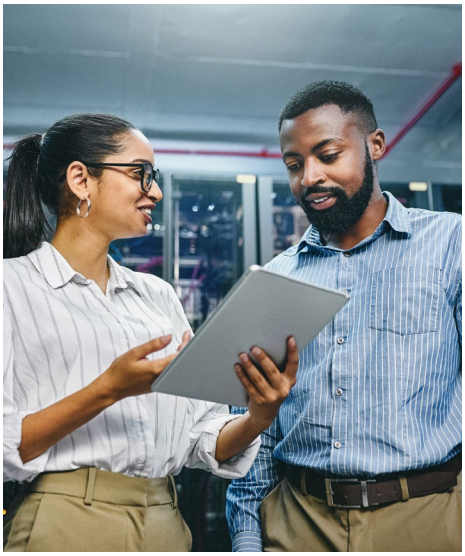
A: Moving to the cloud means we no longer need to send technicians on-site to maintain on-premises systems and hardware. We can significantly reduce maintenance and enhance efficiencies. We can also access many great analytical tools, some fueled by deep learning and artificial intelligence. These can not only simplify our security operations but also provide valuable business insights. With this, we have an opportunity to shift our current operating model from a cost center to a revenue-generating function. And that strengthens our cloud ethos within the organization.

But I think there will always be an element of hybrid because right now, we're not aligned with a fully cloud-based solution. That's why our ultimate goal is to become cloud ready.

Right now, we're managing the transition from an on-premises solution to a hybrid-cloud solution across our locations. We have a mixture of small, medium, and large sites, and each one comes with various network requirements and unique challenges. So how we move to the hybrid-cloud model is a challenge based on the number of locations we have, as well as the number of systems we have at each location.

We also have some analog systems still out there that require a physical device on-premises for IP conversion. We'd like to replace analog equipment with new IoT devices in these locations, negating the need for any on-premises solutions at all. But we're working with annual budgets so that influences how quickly we can move to cloud solutions as well.

There will always be some challenges around moving a deployment into a cloud-based environment. But working with Genetec™, we know that technology is changing, and as it evolves, it'll be easier to transition to the cloud.



"There will always be some challenges around moving a deployment into a cloud-based environment. But working with Genetec we know that technology is changing, and as it evolves, it'll be easier to transition to the cloud."

Q: What do you say to regions that are more conservative in their cloud adoption?

A: I think it's important to consider the risks and how the industry is evolving. For example, Europe, the Middle East, and Africa are probably the most mature in terms of surveillance deployment across the world, but also in terms of integrating various disparate surveillance systems. So based on that type of footprint, I can understand the hesitancy they're having to move into a cloud environment.

But I think each year, more organizations will accelerate in the direction of cloud and work towards addressing those perceived risks associated with that move. To do that, they should work on logical architectural designs to migrate to the cloud and see how that would fit as an executable surveillance operation within their organization. Because the full cloud solution versus the hybrid-cloud solution is very different—and there are some strengths around virtualization where you have more control over that space too.

Hopefully, working with their architectural teams and understanding how the architecture design builds resilience within the environment would ease their concerns. Because cloud environments are inherently resilient. And having that knowledge of how those environments are built coupled with architectural design lends itself to a strong proposition.

Q: How has your team at IBM mitigated supply chain issues?

A: We've been able to manage these supply chain risks by engaging with our internal procurement teams regularly. We also have a direct connection with our original equipment manufacturer (OEM) and engage with them monthly to ensure that we know about any potential product delays. We're doing our best to plan our projects well in advance so that our OEMs and distributors have better visibility of our needs.

We're also looking at our product portfolio and working closely with our integrators to narrow it down to key products that meet all our requirements. In some cases, we've even looked at securing these products as early as possible, even before any installation activities.

However, we also recognize that we have bigger distribution challenges in specific locations such as Latin America. So, we're conscious of how important it is to work with our distributors, OEMs, and integrators in various regions and provide full transparency of what our project portfolio will look like in the coming years, so they know what we're trying to achieve.

Q: OPEX budgets look like they're increasing. Where are you focusing investments for 2023?

A: Our strategic direction in 2023 will be the creation of a Genetec cloud environment. And our focus will be particularly in the Asia-Pacific (APAC) region, starting from Q1 right through Q4. Then, we'll move into the Americas from Q3 and Q4 onwards.

We're not necessarily transitioning each site from on-premises to cloud environments during that period. But our goal is to set the foundation, build out the environment, and then make them available for our operational teams.

By delivering these key requirements next year, we'll have everything in place to begin piloting, testing, and delivering these architecturally designed systems. Then, from late 2023 into 2024-2025, we'll be able to move our on-premises systems into this cloud environment.

Another key area we would like to explore is the automation of system access control (AoA). We'd like to give our users access to tools that help automate the provisioning of access control privileges to minimize human intervention and simplify the end-to-end activity of accessing our systems.

Q: How is your team at IBM keeping up with the rising threat of cyberattacks?

A: Cybersecurity is a big risk for everyone, not just IBM. Since IBM is such a large organization with a global footprint, we are especially susceptible to attacks and risks.

So, we are constantly reviewing our landscape and doing due diligence on understanding any potential risks associated with the products that we deploy on our network. We manage much of that by defining products that we deploy to an approved type and standard, and by working closely with IBM network implementation teams and applying stringent controls to the IBM network.

Many of our sites are also independent of one another, but we have strong policies and processes that depict the movement of data across our networks.

We're also investing heavily in the hardening of our technology and understanding the best practices to apply based on recommendations by Genetec and industry-leading partners to mitigate any potential risk of a cyberattack. Also, we're handling continuous verification across our devices and constantly performing vulnerability scans and tests on all our products, enabling us to identify and remediate issues if required.

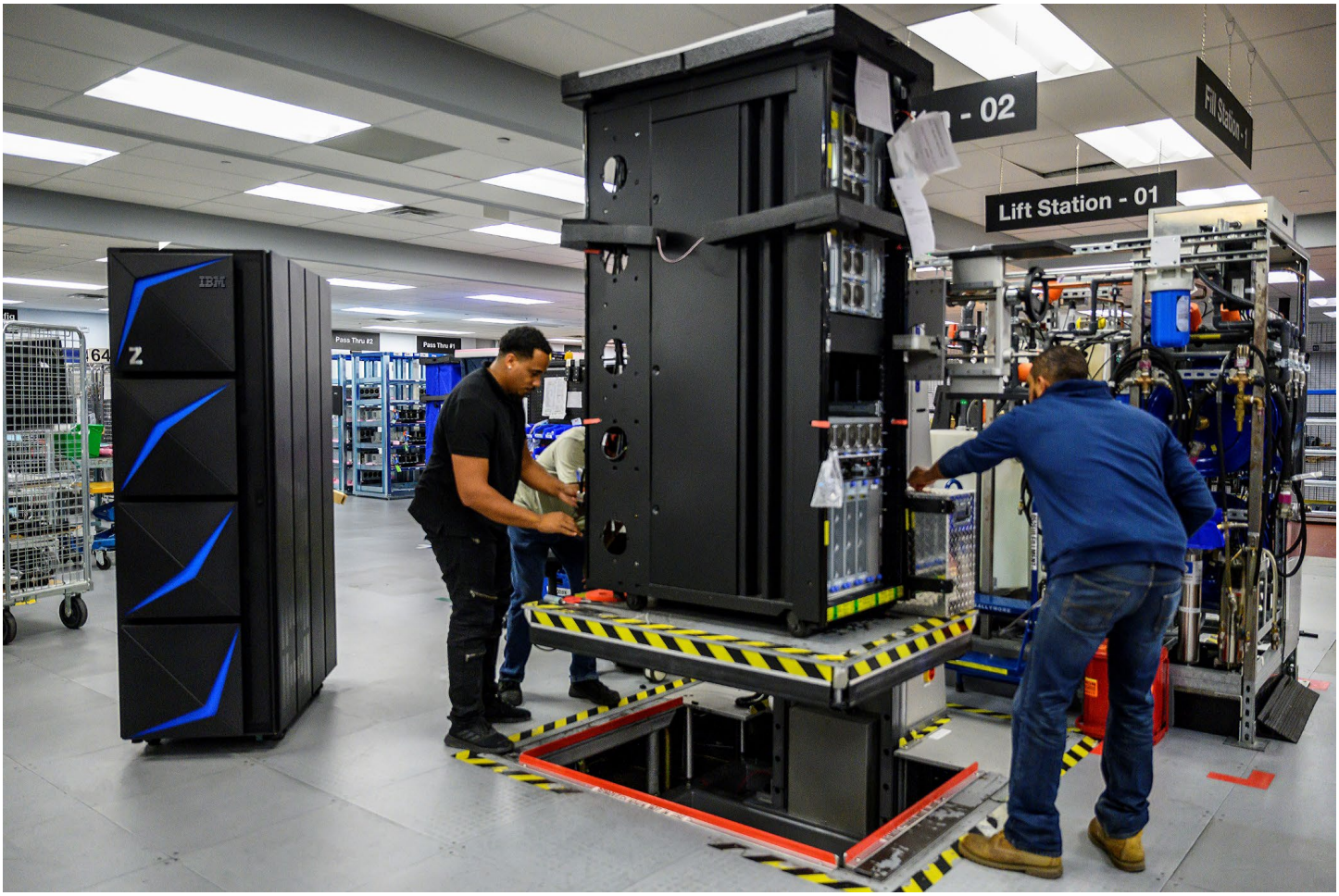
Lastly, we also ensure our security installers are fully versed in our data protection standards, so all expectations are clear.

Q: Are there any other interesting trends you see coming in the physical security industry?

A: Unification helps us effectively manage all our systems through one view. So, we're starting a pilot project in the United States, and potentially Switzerland, to unify our existing video systems with the Synergis™ access control system.

I think more generally across our industry, we're going to see enterprises having to manage, maintain and control their systems by providing strong governance of more of their estate from a central perspective. So, if we can replace a thick client with a thin client and still get the same, if not more, functionality, that's a strong way forward because it reduces the amount of management and support required.

At what pace will the industry move in that direction? That's to be seen. For our team at IBM, we will move to web-based clients where possible, but that's heavily dependent on the level of functionality available to us within the web client.



Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec