McKinsey
Digital

Enterprise-wide security is both a technology and business issue

CISOs have important skills that can position them for the CIO role.

March 2020

A chief information security officer (CISO) focuses on creating a secure operating environment, while a chief information officer (CIO) strives to deliver value to the business. But if you don't get the former right, it becomes impossible to do the latter. Anish Bhimani, CIO, Commercial Banking, JPMorgan Chase, has filled both roles. He discusses how they interact—and how they are evolving—with McKinsey's James Kaplan.

This interview is part of a series of interviews on the evolving relationship between the CISO and CIO. (See "Protecting the business: Views from the CIO's and CISO's offices," on McKinsey.com.)

James Kaplan: Tell us about your cybersecurity journey.

Anish Bhimani: I joined JPMorgan Chase in 2003, nominally as the CISO. I say "nominally," because when I got here, we were heavily outsourcing our cybertechnology. My role was largely a policy-vetting job, and I had 12 people working for me.

Everything changed dramatically when we merged with Bank One. The role became much more technology oriented and transformed into execution as well as policy. We were initially responsible for issues such as threat response, vulnerability management, security infrastructure, and so on. At that point, we didn't have a CISO, so the challenge was getting the right level of buy-in from the CIOs, and we were pushing hard to get people to pay attention to cybersecurity matters.

In 2009, the role was made into a proper CIO-level role, as it is today. It was at that point that cybersecurity had more visibility. Cyber became visible across the entire organization, with leadership driving the tone. It felt like a remediation exercise. We began to see an increase in denial-of-service attacks and malware, and leadership said, "This is more than a technology problem; it's a business problem. Let's fix it."

James Kaplan: What happened when internal stakeholders realized that cybersecurity was a business-critical issue?

Anish Bhimani: We began putting the right resources behind it. Businesses were trying to find a balance between security and the growth of new digital platforms. And as regulatory scrutiny intensified around technology, we paid more attention to technology control than to security. Since then, our level of focus on cybersecurity in the entire organization has been fantastic.

James Kaplan: Are there things you know now that you wish you had known then in your CISO role that could have made you more effective?

Anish Bhimani: What I realize now is that a lot of the things we try to do centrally have a tremendous impact on people. I can now set and drive the tone for the organization so that we get in front of security issues, remediate, and move on to the next challenge. I also did not fully appreciate the transition from developing policy to implementing policy. Finally, we probably should have pushed business leaders harder much earlier by stressing that security was not just a technology issue, but a business issue as well.

James Kaplan: Technology has changed. In years past, it was a 15-minute conversation in passing. By the early 2000s, you'd have a daylong strategy session. How is the topic being addressed at the highest levels of the organization?

Anish Bhimani: I used to go to the board of directors and the audit committee annually for about 20 minutes. We now meet with the board eight times a year for at least an hour each time.

James Kaplan: Discuss your transition from CISO to CIO.

Anish Bhimani: I spent my entire career aspiring to be the CISO of a large bank, and when I got the job, it was a significant accomplishment in my career. When I then became a CIO, it meant shifting to more of an implementation approach, and I was eager to work with the business. But despite my excitement, I was clear that job number one is having a secure and resilient operating environment. If you don't do job one, you don't earn the right to do job two, which is to deliver value to the business.

James Kaplan: What do you miss about your CISO role?

Anish Bhimani: You always miss the cat-and-mouse challenge, the game theory, as well as the problem solving and intellectual curiosity. There is also a very active peer and industry community for best-practice sharing, since everyone is facing many of the same challenges. It's amazing how the CISO role has evolved.

James Kaplan: How do you see the CIO role evolving?

Anish Bhimani: The ongoing debate is where security should report. Some say security can't report to IT, because it's a conflict of interest. Others say there's no way you can get the job done reporting outside of IT. I think that, in years to come, security will become more embedded within the IT fabric of any organization as standard operating practice.

There is also the client impact. As we become better at securing systems, the point of vulnerability moves from the system to the person. Security becomes every employee's responsibility. Cyber organizations are now building frameworks, working across infrastructure with developers on systems such as cloud. So the architecture of how the CIO goes about implementing infrastructure and security policies will evolve with the role itself. A security organization will always attempt to be agile, but it's very challenging when you're moving at the speed of light.

James Kaplan: Do you see the CISO and CIO roles integrating?

Anish Bhimani: Every CIO should spend time in a security role, since it makes you think differently. Regardless of your role, you're never out of security. With new technologies, including automation, security is a layered process. It's built into the fabric of the organization, from process to people.

James Kaplan: What advice can you offer on breaking down silos and managing talent?

Anish Bhimani: Understand how to navigate the organization. Manage conflicts. Keep your objectives in mind while managing these conflicts. Understand your business's priorities. One of the things I am most proud of is the professional development of my direct reports. During my time as CISO, 21 of the people I managed went on to serve as CISOs elsewhere. So you must develop the people, not just their roles.

James Kaplan: It sounds like one of the biggest priorities is security remediation.

Anish Bhimani: It's less remediation and more about how you proactively build controls. For example, several years ago, when we found a serious issue with some systems, we would run a remediation program that took days or weeks. Now, a similar incident is opened and fixed before people go home.

James Kaplan: Talk about the movement to cloud applications.

Anish Bhimani: When moving to the cloud, the first priority is figuring out your technology and business priorities and then striking a balance. Services and architecture templates need to be validated and automated for cloud configuration. Second, cloud security can be a business enabler, and we know that businesses need to grow and thus must move fast.

Why do you have brakes on a car? It's not just to stop. It's so you can go fast, secure in the knowledge that you can stop whenever you want or need to. Security done right enables businesses to go at the speed they want while being able to manage risk appropriately.

James Kaplan: What type of advice would you offer someone who is just beginning their career in cyber?

Anish Bhimani: My first advice is that life never moves in a straight line. You need to be able to adapt to constantly changing circumstances. Well-roundedness is critical, and everything you do should get you a step closer to your goals. Rotations are valuable in gaining experience in security and infrastructure.

James Kaplan is a partner in McKinsey's New York office.