McKinsey Digital

Robust cybersecurity requires much more than great technology

Security is increasingly an interdisciplinary capability.

March 2020

It's easy to view the 21st-century "threatscape" through a purely technological lens. But today's chief information security officers (CISOs) and chief information officers (CIOs) need to understand and appreciate the people and process elements as well. George Sherman, CIO of Global Technology Infrastructure, JPMorgan Chase, discusses his multiprong outlook on information security 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: How does your security background shape your approach to your current role?

George Sherman: I use my technical-security skills on a daily basis. With new technology and connectivity platforms, many of our older security paradigms are being stressed. In the past, you could get away with not having the most robust identity or authorization constructs and authentication and authorization metrics. This is no longer the case, as the dynamic nature of these modern technologies requires dynamic management of the trust chain.

If you add to this the complexity of the multivendor cloud environments connecting into our companies, you must have a strong understanding of the "threatscape" and how you deal with cybersecurity issues. Everyone within the organization must understand that cybersecurity is non-negotiable. *We* have to get it right all the time. The bad actors only have to get it right once.

James Kaplan: What makes for a good CISO?

George Sherman: I think the best CISOs are the ones who have learned about policy and controls but at their core are very strong technologists. The CISO role must evolve with the threat landscape and technologies. You must understand the technical side of cybersecurity. But information security and protecting against cyberthreats are also about people and process, not just technology, so you have to understand all three dimensions in order to fully appreciate what you have to do to protect the firm.

Sometimes you have to go slow to go fast. It's the old race-car analogy. You can go really fast in a race car because you're wearing a fireproof suit, you're in a protective cage, you have an automatic fire-extinguishing system, and you were trained. This allows you to drive superfast. But getting to that point can feel slow. CISOs who "get it" spend a little bit more time up front being thoughtful about their execution.

James Kaplan: Does that need to understand the technology environment holistically at every layer in the stack provide a good background for a future business-unit CIO?

George Sherman: We are unique and fortunate in that three of our CIOs are former CISOs. This makes the CISO's life much easier, specifically as it relates to how you design, deliver, and execute the business-process automation efforts. Thanks to our security background, we tend to think about data protection and security earlier in our processes and require that security and controls be embedded into all the technology we deliver.

James Kaplan: Given all that's changing, particularly around cloud and digitization, how different will the skill set of a CISO be in a decade?

George Sherman: You can go back a decade and see how much has changed. Everything seemed much simpler. The successful CISOs of the future can't be process managers. They must have a deep understanding of technology. Imagine leading thousands of software engineers but never having actually written a line of code. At some point, you have to ask yourself how you can relate to that community. And how will that community relate to you? Those questions are just as relevant to today's and tomorrow's CISOs.

Also, the technology is going to become more segmented but also more hyperconnected. You can see that in the evolution of the private, public, and hybrid cloud, and with a combination of infrastructure-as-a-service, platform-as-a-service, and software-as-a-service providers clamoring to support new growth. But with this hyperconnectivity comes hypercomplexity, and with that comes fragility. Fragility leads to reliability and security issues. The enemy of a good security program is complexity. If we're not careful in our execution, CISOs could end up with a "least common denominator" problem where their environments are only as secure as their weakest controls.

James Kaplan: CISO and infrastructure responsibilities often overlap—for example, in patch management. How do you deal with this?

George Sherman: Having clear lanes of responsibility is important. If you view patching and life-cycle management as a tax or a duty, then you really don't understand the need to keep software current and manage it in a near-real-time way. This mindset translates into your organization's view of these functions as a burden. A CIO has the responsibility to design and direct their organization to understand that this isn't a burden but instead a core part of their team's job. Protecting the firm, keeping it patched and updated, is everyone's responsibility.

James Kaplan: Where does security fit into people's roles in IT?

George Sherman: Resiliency, availability, and security are everyone's responsibility, regardless of whether you're involved with infrastructure, applications, or both. Everyone must believe that operational risk and information security are core requirements of their role, so you need to invest in training and move this to the forefront of your team's minds, or you will end up with yet another remediation program.

Secure by design is critical. You can build systems that are reliable and available, but they may not necessarily be secure. But when you build secure systems, you often end up with ones that are both reliable and available. The disciplines around security tend to lend themselves to the same disciplines as resiliency and availability or operational efficiency and effectiveness.

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