

SECURITY LEADERS MUST BECOME STRATEGIC ADVISORS TO THE BUSINESS FOR DIGITAL TRANSFORMATION SUCCESS

CISOs and their teams have a unique opportunity to speed transformational efforts and achieve better, faster, secure, and more productive business outcomes.

Security leaders must become strategic advisors from the onset of digital transformation initiatives. Doing so enables transformational efforts to move faster with greater protections in place, according to global IDG research.

For that to happen, however, CISOs and security leaders must adopt an advisory position, giving guidance and strategy.

STRATEGIC ADVISORS, NOT TACTICAL MANAGERS

DX has taken off. Companies are leveraging the cloud, DevOps methodologies, Robotic Process Automation, and related technologies to digitize processes that speed customer service, application development, employee collaboration, and much more. That requires strategic thinking throughout the organization, including from CISOs.

However, they're now seen primarily as managers (see Figure 1), and overwhelmingly perceived as simply doing an "adequate" job when it comes to DX initiatives.

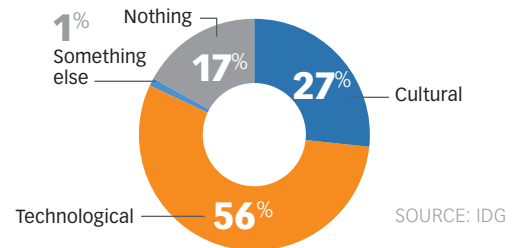
The stumbling block: 56% of survey respondents say technology is holding back security leaders from taking a more strategic role in DX.

FIGURE 1. HOW CISOs ARE PERCEIVED



SOURCE: IDG

FIGURE 2. ISSUES PREVENTING SECURITY LEADERS FROM TAKING A MORE STRATEGIC DX ROLE



SOURCE: IDG

MOVE FASTER BY STARTING EARLIER

To shift from being perceived as a manager toward being seen as an advisor, technological issues must be addressed. CISOs should move away from simply managing technologies and anticipate security technology needs. That means getting involved at the early design phase of DX projects and forging greater alignment with lines of business and IT peers.

Survey respondents agree that, by getting involved sooner, CISOs reduce the risk of incurring security gaps in the future.

For example, if it turns out that a DX project will pose an unacceptable risk, 69% of IT respondents say their company would then need to conduct additional technology research. That additional time slows the pace of DX and the ability to achieve business outcomes like boosting productivity and increasing revenue opportunities.

WHAT'S NEXT

Security leaders must become more proactive and build a thorough business case for security technologies, then embed them into DX initiatives.

In addition, security leaders should:

- Lean on technology providers to help mitigate risks without adding complexity.
- Vendors are increasingly ensuring that their security solutions "focus on a business outcome for the customer," according to IDC.
- To that end, CISOs should seek partners that will boost their advisory capacity.

CyberArk is focused on privileged access management in the cloud, in hybrid environments, at endpoints, and in DevOps environments, while helping CISOs manage security and risk. Find out more: www.cyberark.com