WHITE PAPER

Market Pulse

3 CISO STRATEGIES FOR DIGITAL TRANSFORMATION SUCCESS

CISOs and security leaders can make a strategic difference with digital transformation initiatives. What's key: help mitigate risk, align with the business, and be proactive.

COMPANIES ARE INCREASINGLY LEVERAGING THE CLOUD, DevOps methodologies, automation, and related technologies as part of their digital transformation (DX) efforts.

All of these areas require that security is embedded from the start. When it is bolted on after-the-fact, projects risk security gaps, delays, and cost overruns.

For the best results, CISOs and security leaders must proactively:

✔ Provide risk mitigation;

✔ Align with business goals; and

✔ Proactively get involved with DX initiatives.

In short, they must become strategic, versus simply managing technologies and systems. This report examines global IDG research about the role of security and the CISO amid DX efforts, and provides strategies for improving success.

WORRISOME TREND: RISK NOT HIGH ON THE PRIORITY LIST

Digital business transformation is well underway. Companies are digitizing processes to improve customer service, application development, supply chain collaboration, and much more. To get there, decision makers are using a mix of foundational and emerging technologies — from cloud storage and AI to DevOps, Internet of Things, data analysis, and private cloud (see Figure 1).

That said, there are interesting differences between the priorities of IT and line of business (LoB) leaders — both in terms of initiative types and the goals behind them. Most notably: Senior IT leaders are targeting productivity, while business executives most want to reduce costs (see Figure 2).

On another front, however, it's worrisome how few survey respondents prioritize risk exposure. Overall, only 34% cite this as a priority; among LOB and IT respondents, the need to mitigate risks ranks at #8, respectively.

Considering that digital information is directly impacted by the expanding cyber threat landscape, this is where CISOs can make a strategic difference. But first, they must overcome the perception that their role is simply to "manage the security tools and technology" (cited by 60% of respondents). Only 7% of survey respondents say these security leaders are advisors, helping to guide digital strategy.

FIGURE 1. **Top DX Technologies of Choice: IT vs. LoB**

	IT	LoB
Cloud storage	#1	#1
Artificial intelligence	#2	#4
DevOps	#3	#6
Internet of Things	#4	#3
Data capture & analysis	#5	#2
Private cloud	#6	#5

Source: IDG

CYBERARK

IDG Communications, Inc.

SPONSORED CONTENT

IDG

FIGURE 2. **Top DX Goals: IT vs. LoB**

	IT	LoB
Boost productivity	#1	#3
Improve customer relationships	#2	#5
Increase revenue opportunities	#3	#2
Improve decision-making speed & accuracy	#4	#6
Improve competitive position	#5	#4
Reduce costs	#6	#1
Optimize the supply chain	#7	#7
Minimize/reduce risk exposure	#8	#8

Source: IDG

CISOs must do a better job of inserting themselves into DX initiatives — in part by educating IT and LoB leaders about specific risks and ensuring that security is embedded throughout. After all, the volume of data is expected to grow to 463 exabytes by 2025[1], making the business environment increasingly susceptible to new risks.

Here are three strategies that can help CISOs heighten and enhance security in transformational projects.

1. PRIORITIZE RISK MITIGATION

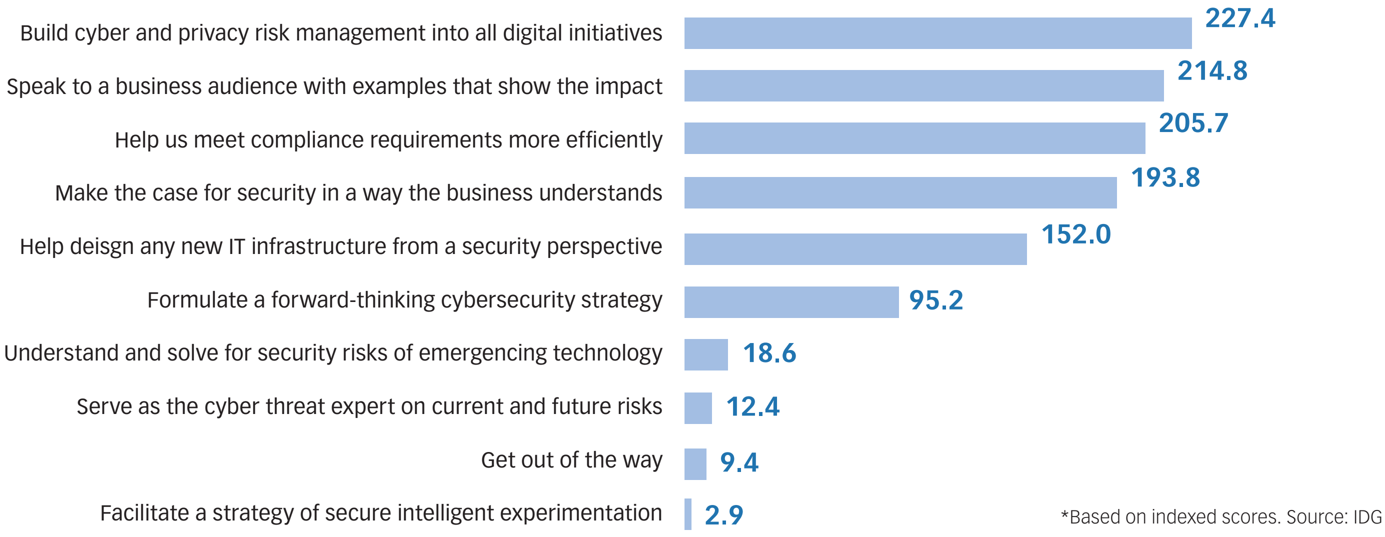
Although minimizing or reducing risk exposure is not among top DX priorities, when asked where CISOs can most add value to transformation efforts, the top answer is: Build cyber and privacy risk management into all digital initiatives (see Figure 3). In fact, among the worst things CISOs can do is to "get out of the way," respondents say.

In a recent IDC report[2], analysts suggest that risk mitigation in digital transformation projects is the perfect opportunity for CISOs to "play a role in the strategic direction of the business." By improving risk confidence, security leaders can "make waves at the Board level."

Risk mitigation must work across any and all transformational efforts, no matter whether they're focused on cloud, robotic process automation (RPA), DevOps, or business-critical apps. The common theme among all projects is secure access. It's critical to provide credentialed protection across an organization's entire digital business — on premises, in the cloud, and in hybrid cloud environments.

"Companies must be able to move fearlessly into the new digital landscape," says Adam Bosnian, executive vice president, Global Business Development at CyberArk. "Privileged access security provides CISOs with the ability to proactively address the expanded digital attack landscape, secure data, and strategically address risk mitigation for their companies."

FIGURE 3. **How Security Leaders Can Most Add Value to DX Projects***



*Based on indexed scores. Source: IDG

[1] Raconteur, Future of Data, www.raconteur.net/future-data-2019

[2] IDC, "Enterprise CISOs Seek Relief from Complexities Prompted by Emerging DX Risks," March 2019

2. GET CLOSER TO BUSINESS STAKEHOLDERS

CISOs have a unique opportunity to demonstrate their ability to act as strategic business advisors and consider the “big picture.” This means getting closer to the business stakeholders in order to understand their needs and challenges, then thinking like a business person first (and a security person second).

Many survey respondents (55%) say that CISOs are held back from taking a larger role in DX by technological issues or, in other words, they don’t have the right security tools. CISOs can solve for this by keeping up with trends in technology, business needs, and market segments — and discussing this information with key LOB stakeholders. In addition, they should take note of new digital technologies in use by their industry and/or competitors, and bring those ideas to their business counterparts.

CISOs can also conduct thorough research into security tools and how they relate back to business objectives. These insights can then be parlayed into a solid business case, including clear examples that show how security impacts DX projects.

Doing so achieves two things:

- **Helps avoid delays.** If it turns out that a DX project will pose an unacceptable risk, for example, 69% of IT respondents say their company would need to conduct additional technology research. That additional time slows the pace of DX and the ability to achieve business outcomes.
- **Demonstrates alignment with business goals.** Strategic thinking and planning shifts the perception of security as “a cost center with little noticeable impact,” according to IDC analysts, toward directly enabling the business goals of digital transformation.

3. EARLY IS NOT EARLY ENOUGH

Currently only 38% of CISOs are brought in at the very beginning design phase of DX, according to the IDG survey. And yet, 44% of respondents say digital business projects would move faster with security leaders involved from the onset. As one survey participant explained: “The projects would move faster because the time required to implement security measures are significantly reduced.”

38% OF CURRENT CISOs ARE BROUGHT IN AT START OF DX PROJECTS

44% SAY DX WOULD MOVE FASTER WITH CISOs INVOLVED AT THE ONSET

Some might even argue that early is not early enough — as CISOs work across the business and forge relationships with other C-suite colleagues, they should learn about DX projects as soon as they’re hatched. With business acumen in hand, they can proactively drive projects on their own by asking LOB managers about key technologies as they relate to market dynamics or industry trends.

“CISOs should be able to predict when the CEO, CMO, or CFO is going to need digital transformation technologies and be the one who spearheads or be part of a team that leads this,” says Bosnian. “They should bring this technology to the table and say, ‘we need robotics or DevOps or cloud to help leapfrog our competition, cut costs, and so on.’”

Beyond speeding the process, there are other benefits to having security leaders involved earlier in DX projects. Respondents cited:

- ✔ Improved quality of outcomes
- ✔ Avoidance of being blindsided by requirements and risks late in the game
- ✔ Greater collective appreciation of the role of security
- ✔ Boosted confidence in security

Early engagement with digital transformation projects also allows the CISO to understand the parameters for success. The IDG survey revealed that companies equally look for financial, operational, and customer experience improvements as measurements of DX accomplishments. For example, security leaders should be able to demonstrate that:

- ✔ Productivity or revenue has increased (financial);
- ✔ Employees are using the tools provided (operational);
- ✔ The brand value from each customer relationship can be measured (customer experience).

THE BOTTOM LINE

The evolving and expanding cyber threat landscape has proven that “security concerns, nowadays, need to be considered at the very beginning of any IT project,” says one IDG survey respondent.

Transformational initiatives deserve heightened security consideration, as users, customers, partners, and suppliers increasingly collaborate to expand digital business. DX efforts provide a great opportunity for CISOs and security leaders to prove their strategic capabilities.

“They have an overall concept of what the company is trying to achieve,” says one IDG survey respondent, “and possibly the best knowledge of the appropriate strategies to take.”

To learn more, visit **www.cyberark.com**

ABOUT THE SURVEY: IDG surveyed 330 IT and LOB decision makers at companies with 500+ employees. CyberArk sponsored the survey, which was conducted online between May 21 and June 13, 2019.