Hey! What's New? 2025-13

A New Era of Transformational Cyber Strategies

The powerful connection between cybersecurity and business impact comes into sharp focus in Deloitte's 4th Edition of *The Global Future of Cyber Survey*, which asked nearly 1,200 leaders in various industries worldwide to share their views on cyber threats, enterprise activities and the future. The survey included C-suite executives across the enterprise, as well as other senior leaders with responsibility for IT, security, risk and the business.

According to the survey report, "despite the growing focus on cybersecurity, only about half (52%) of all respondents are very confident in the C-suite and board's ability to adequately navigate cybersecurity. And specifically among C-suite respondents who are focused mainly on cybersecurity, only 34% are very confident – suggesting that they have less confidence in their abilities than others do."

But when we look just at organizations that Deloitte has classified as having high cyber maturity, we see two important findings: "Cybersecurity is recognized at senior levels, and there is a strong correlation between organizations' cyber maturity and having greater confidence in adequately navigating cybersecurity. In fact, among high-cyber-maturity organizations, that confidence in the C-suite and board grows to 82% – compared to 52% and 39% for medium- and low-cybermaturity organizations, respectively.

The survey's findings indicate that, "on average, 86% of respondents are implementing actions to a moderate or large extent to increase cyber strategies and actions, embracing cyber as an essential component of the enterprise. And, on average, 85% of respondents expect to achieve their desired business outcomes to a moderate or large extent. While this underscores the critical role cyber plays in driving successful strategy implementation, not all organizations will realize those benefits equally."

And, notes the survey report, "the more cyber-mature the organization, the bigger the potential impact. The survey found that respondents in high-cyber-maturity organizations anticipate almost two times the positive business outcomes compared with their peers. How these highcyber-maturity organizations view cybersecurity – and how they are taking action – provides insights and a potential path for others to follow as they seek to increase their own cyber maturity."

The report stresses that "the leaders of high-cyber-maturity organizations understand that being prepared to respond to and recover from the inevitable attack – to get their businesses back up and running quickly, and to serve their customers – is what matters most."

What are organizations hoping to prepare for (or avoid) as they become more resilient – and how has the picture changed? "Compared with the previous edition of the survey, a loss of confidence in tech integrity (i.e., reliability, accuracy and availability of systems and data) has risen to the top of the list as the number one negative consequence of cybersecurity incidents or breaches – becoming increasingly important as organizations accelerate their digital transformation journeys."

Operational disruption, including supply chain or partner ecosystem disruption, remains high on the list, in the number two spot, underscoring the importance of business continuity across partners and infrastructure. However, says the report, "there is also a notable shift, as this was the top concern in the previous edition of the survey. Reputational loss climbed up one place as the number three concern."

The report stresses that "the steps organizations take today should focus on how cyber investments can optimize, preserve, protect and create value for the organization. That includes laying a strong foundation for future growth through cyber practices that enable data security and integrity across digital products and infrastructure. That foundation also should incorporate the fundamentals of a responsive infrastructure and digital ecosystem – for enabling future growth and business resilience." This edition of the survey shows a marked trend toward cyber programs and CISOs gaining greater strategic influence across all these value streams through more integrated technology transformation strategies – especially among the most cyber-mature organizations.

The report suggests that "an effective approach to cybersecurity should extend beyond the traditional focus on incident response. It should delve into the core of how businesses need to integrate cyber – risk, security and trust – into their overall strategy. Adopting a holistic, business-oriented perspective allows you to bridge broader business objectives and operational needs. This approach ensures that cyber is not just a reactive measure but a proactive, integral part of the organization's strategic business, technology and operational framework. Moreover, Deloitte's research illustrates that the most cyber-mature organizations in the market are gaining significant value through a similar business-oriented approach."

For a whole lot more, get the report at Global Future of Cyber Survey, 4th Edition | Deloitte Global.