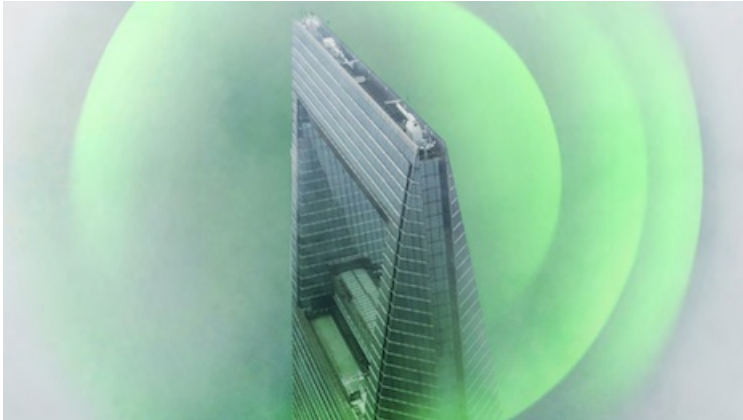SOFTWARE AND TECHNOLOGY

91pc of organizations reported at least one cyber breach or incident in 2022: Deloitte

June 13, 2023

With consumer industries lagging behind, there seems to be a gap between virtual risks and how brands across the market are taking action. Image credit: Deloitte

By EMILY IRIS DEGN

When it comes to scaling growth and fostering stability in today's business landscape, a secure virtual presence is no longer negotiable.

Findings from the latest edition of global consulting firm Deloitte's annual cybersecurity survey reveal that 91 percent of organizations experienced at least one cyber breach or incident in 2022, up from 88 percent per 2021 results. Despite the challenge, a gap between virtual risks and how brands across the market are taking action prevails, with consumer industries lagging behind, both issues that company boards matching the description are increasingly looking to address.

"This year's report shows how cyber is now woven more tightly into business operations, outcomes, and opportunities," said Emily Mossburg, global cyber leader at Deloitte, in a statement.

"Chief information security officers (CISOs) are most successful when they are connectors across their organization, focused on enabling their organization's highest business priorities," Ms. Mossburg said. "Cyber has become an enabler for business and embedding it into all business practices has shown nothing but success.

"Advancing cyber will only become more critical as the global economy faces a potential downturn and businesses navigate a looming recession."

Findings from the survey were gathered through a poll of more than 1,000 cyber decision-making leaders at a director's level or higher, spanning six industries and 20 countries in 2022. Respondents were limited to those sourced from companies employing at least 1,000 people and bringing in at least $500 million in annual revenue.

Cyberspace considerations
Deloitte's Global Future of Cyber Survey 2023 uncovers the occasions in which the digital world's heightened influence can hurt businesses.

Of those who saw at least one related breach or incident, 56 percent stated that moderate or large consequences

ensued as a direct result, according to the firm's biggest cyber survey to date.

"With cyber threats growing and advancing around the globe, there is no architecture or approach that can guarantee absolute security and risk mitigation," said Ms. Mossburg, in a statement.

> Find out how your industry is embedding cybersecurity across their business strategy and how organizations prepare for an evolving cyber landscape based on #Deloitte's 2023 Global Future of Cyber Survey. https://t.co/3ggOoKiK1e
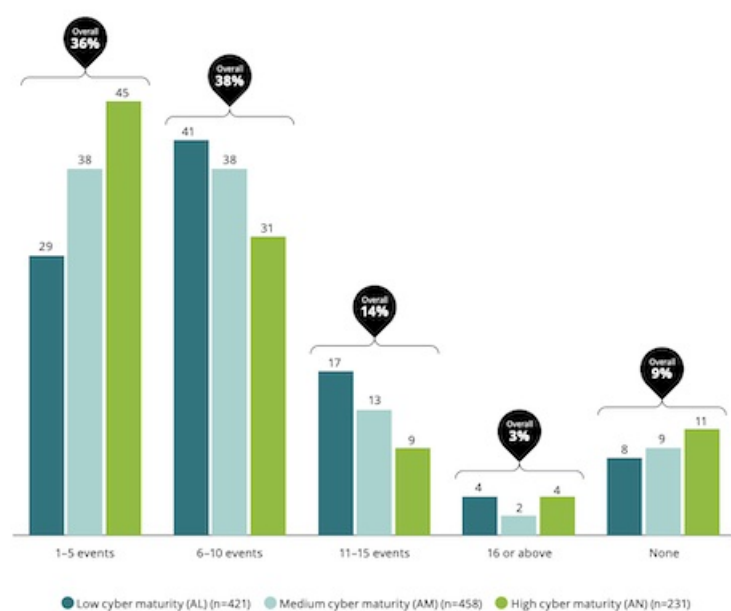>
> Deloitte (@Deloitte) June 9, 2023

"We're now seeing cyber transcend its traditional IT roots and become an essential part of future-proofing businesseswhich will be critical in the year ahead as digital transformation continues to be a top investment."

High-profile leaks have tempted many boards and cyber-decision makers to plan ahead, rather than falling victim to reactionary measures following a cyber event.

Though fully realized in the face of an incident, data suggests that it does not take disaster striking for business communities to acknowledge the perks of heightened cybersecurity. In fact, 86 percent of respondents told Deloitte that centralizing these efforts has made a significant and positive impact on business.

Attempting to avoid the consequences that come along with hacks, companies are stepping up and modernizing on a digital front. Seven of every 10 respondents said that cybersecurity topics appear on board meeting agendas at least once a quarter.

Figure 2: Number of significant cybersecurity events
(Precentage)

Low cyber maturity (AL) (n=421)   Medium cyber maturity (AM) (n=458)   High cyber maturity (AN) (n=231)

Data from last year suggests cybersecurity threats are on the rise. Image credit: Deloitte

Represented by the survey, hospitality group Marriott International serves as an example of an entity making cybersecurity a priority.

"Projects, initiatives, business objectives can't be met without thinking through information security and privacy impacts, and having that embedded into the appropriate processes," said Arno Van Der Walt, senior vice president and chief information security officer at Marriott, in a statement.

"We're brought in during the ideation phase as it relates to business components and aspects," Mr. Van Der Walt said. "Our strategy is 100 percent focused on supporting the business, recognizing that cyber and privacy do not exist without the business.

"We want to ensure that we are meaningfully contributing to moving the business forward, driving growth, and doing

so in a manner that's compliant and secure."

Heading the cloud
So long as brands continue to pivot and adapt to disruption, use cases for technological alternatives will not cease to expand (see story).

As far as digital transformation goes, optimizing organizational approaches to cloud technology ranked highest among a list of priorities for leaders surveyed, compared to 2021, when it slotted in second on the list. While businesses are at varying levels of integration, of those investing in the capability, 83 percent report positive outcomes for risk regulation and mitigation.

The cloud has become the main focus for organizations this year, while 5G has entered conversations. Image credit: Deloitte

Luxury is also beginning to embrace cloud computing on an internal and executive level, launching virtual campuses and the like to match digital infrastructures with the demands of remote work (see story), making security measures that much more important.