Global CISO Survey Finds Digital-First Economy Introduces Unforeseen Risks for 89% of CISOs

CISOs struggle to cost justify security investments despite known security gaps, face increasing personal risks, and worry about the rapid adoption of AI.

Salt Security Logo

LONDON, UNITED KINGDOM, June 21, 2023 /EINPresswire.com/ -- Salt Security, the leading API security company, today released key findings of the new "State of the CISO 2023" report. Conducted by Global Surveyz for Salt, the global CISO survey gathered feedback from 300 CISOs/CSOs around the world on issues resulting from digital transformation and enterprise digitalization. The results highlight significant CISO challenges including the biggest security control gaps they must manage, the most significant personal struggles they face, and the impact that broader global issues are having on their ability to deliver effective cybersecurity strategies.

> These findings reinforce that organisations must prioritise assessing their API security strategy to ensure they are solving today's risk and not yesterday's risk."
>
> *Roey Eliyahu, CEO and co-founder of Salt Security*

Today's digital-first economy has transformed the role of the modern CISO, increasing threats and changing security priorities. Key findings include:

89% of CISOs report that the rapid deployment of digital services has generated unforeseen risks to securing critical business data

Digital initiatives have produced new individual concerns, the top being the risk of personal liability and litigation resulting from security breaches, with 48% of CISOs citing that challenge
94% of CISOs worldwide say the speed of AI adoption is the macro dynamic having the greatest impact on their role
95% of CISOs plan to prioritise API security over the next two years, a 12% increase compared with that priority two years ago

As the glue connecting all of today's digital transformation initiatives, APIs stood out as a key

focus area for CISOs. 77% of CISOs acknowledge APIs are already a higher priority today vs. two years ago. In addition, API adoption presented the second highest security control gap, after supply chain/third party vendors, resulting from organisations' digital initiatives.

"The findings from this worldwide survey clearly show that CISOs face more pressures than ever before as a result of the acceleration of the digital economy over the past two years," said Roey Eliyahu, CEO and co-founder of Salt Security. "APIs are the building blocks of every digital service and a significant amount of risk has shifted towards them. These findings reinforce that organisations must prioritise assessing their API security strategy to ensure they are solving today's risk and not yesterday's risk."

Biggest CISO challenges in a digital-first economy
The 2023 report shows that the digital-first economy has brought new security challenges for CISOs. Interestingly, most of the challenges cited by CISOs represent nearly equal levels of concern, forcing CISOs to address multiple challenges at the same time.

CISOs cite the following top security challenges:

Lack of qualified cybersecurity talent to address new needs (40%)
Inadequate adoption of software (36%)
Complexity of distributed technology environments (35%)
Increased compliance and regulatory requirements (35%)
Difficulties justifying the cost of security investments (34%)
Getting stakeholder support for security initiatives (31%)

Also notable, while most CISOs (44%) report security budgets are about 25% higher than two years ago, nearly 30% identify "lack of budget to address new security challenges" from digital transformation as a key challenge, and 34% of CISOs cite difficulty justifying the cost of security investments as a challenge. Examining the responses more closely, 82% of CISOs say the security budget is higher than two years ago, while 87% say company revenue is higher. This disparity indicates that CISO spending power, as a percentage of revenue, has decreased in the last two years.

Supply chain and APIs top security control gaps
Two thirds of CISOs state that they have more new digital services to secure compared to 2021. In addition, 89% of CISOs state that the rapid introduction of digital services creates unforeseen security risks in protecting their companies' vital data. API adoption and supply chain/third party vendors presented the two highest security control gaps in organisations' digital initiatives.

CISOs rank security control gaps resulting from digital initiatives as follows:

Supply chain/third party vendors (38%)
API adoption (37%)

cloud adoption (35%)
Incomplete vulnerability management (34%)
Outdated software and hardware (33%)
Shadow IT (32%)

Because APIs are embedded throughout all of today's modern digital applications, including integrated third-party services and cloud applications, the above findings underscore the particular importance of API security to close the above cited security control gaps. In addition, most organisations lack a complete inventory of their APIs, making APIs another component of "shadow IT."

Global trends impacting the CISO role – speed of AI adoption ranks number one
The vast majority of CISOs admit to feeling the impact of a number of global trends. More CISOs cited the speed of AI adoption as having significant impact, followed by macro-economic uncertainty, the geo/political climate, and layoffs. Specific CISO responses regarding the impact of global trends were:

Speed of AI adoption (94%)
Macro-economic uncertainty (92%)
Geo/political climate (91%)
Layoffs (89%)

Threat of litigation and increased liability top CISOs' personal concerns
The digital-first economy has also impacted CISOs on a personal level. Among the personal challenges reported were:

Concerns over personal litigation stemming from breaches (48%)
Increased personal risk/liability (45%)
Expanded responsibilities and not enough time to fulfil (43%)
Increased job-related stress (38%)
Bigger teams to manage (37%)

Nearly 50% of CISOs cite litigation concerns. With several high-profile CISO lawsuits making waves recently, CISOs are fearful of being found personally liable in the event of a breach, putting their livelihood at risk.

CISOs say their boards of directors are knowledgeable about cyber risks and mitigation
On a positive note, 96% of CISOs worldwide report that their boards of directors are knowledgeable or very knowledgeable about cybersecurity issues. In addition, the survey showed that 26% of CISOs present to the board on cyber risks mitigation and business exposure once a quarter or more, and 57% present to the board at least once every six months.

CISO and industry analyst quotes on survey findings

“As organisations accelerate their digital transformation efforts, they naturally increase the use of APIs in many areas of business and AI. So it's promising to see that their API security efforts are finally moving upward. Sometimes companies can be penny wise but pound foolish when it comes to security investments. But given the high cost of major personal data breaches, API security has to rise in prominence, and do so sharply, in the near future.”
–Anton Chuvakin, security advisor at Office of the CISO, Google Cloud

“These findings underscore the new reality of the “AI era” of cyber. CISOs know that AI attacks are evolving and becoming increasingly sophisticated – and that they’re growing at an unprecedented rate. With security teams already at capacity defending a broad attack surface, the impact of escalating AI threats – as well as the necessity to implement an AI offence –clearly weighs heavily on today’s CISOs.”
–Ed Amoroso, founder and CEO of TAG InfoSphere

“Given the growing importance of APIs over the last several years for enabling modern businesses, it is surprising that API security has become mainstream only recently, with 95% of CISOs prioritising API security during the next two years,” The fact that security frameworks and regulations are slow to evolve is partly to blame, but I see hope on the horizon. The Federal Financial Institutions Examination Council (FFIEC), which usually takes years to issue a new mandate, in just one year explicitly called out APIs as a separate attack surface, requiring financial institutions to inventory, remediate, and secure API connections.”
–Jeff Farinich, SVP technology and CISO at New American Funding

“The impact of AI has captured the imagination of all the CISOs I’m talking to, so I’m not surprised to see it cited as the global trend most impacting CISOs. We all realise that cyber attackers are already using AI – we as CISOs need to map out our game plan for using AI as part of our fabric of defences to counter these threats.”
–George Gerchow, CSO and SVP of IT at Sumo Logic

“Given the importance of APIs for modern businesses, it doesn’t surprise me that 95% of CISOs are prioritising API security over the next two years. I’m curious about the 5% of organisations that have not made API security a priority. With APIs as the connectors for the digital-first economy, security today hinges in API security.”
–Ryan Melle, CISO, SVP at Berkshire Bank

“These survey results really validate what I've been experiencing for the past couple of years. Security requirements have grown exponentially with digitalization, and we’re moving faster than ever with those digital projects. Objective data like these brings more awareness to the problem set and helps us craft ways to work together to create a stronger and safer cybersecurity culture.”
–Julie Chickillo, VP, head of cybersecurity at Guild Education

“In addition to upending many traditional security approaches, the digital-first economy has impacted a lot of us CISOs on a very personal level. The fact that my peers highlighted ‘concerns over personal litigation stemming from breaches’ as their top personal concern should be alarming to everyone in the industry. Qualified leaders may decide not to pursue the role if organisations don’t have the right cyber tools or processes, or if they consider the personal risk too high.”
–Mike Towers, Chief Digital Trust Officer at Takeda Pharmaceuticals International.

Methodology
Conducted by Global Surveyz in April 2023, the State of the CISO report surveyed 300 CISOs/CSOs worldwide, including in North America, EMEA, the United Kingdom, and Latin America. Those surveyed held CISO or CSO roles across multiple industries, including financial services, healthcare, insurance, pharmaceutical, retail and ecommerce. Headquartered in Tel Aviv, Israel, Global Surveyz is a global research company that gathers, analyses, and interprets B2B and B2C data from diverse industries and markets. A copy of the report can be downloaded here.

Charley Nash
Salt Security
+44 20 7183 2849
charley@eskenzipr.com
Visit us on social media:
Twitter
