proofpoint.

REPORT

2023 Voice of the CISO

Global insights into CISO challenges, expectations and priorities

proofpoint.com

Table of Contents

A Reality Check for CISOs

It's no overstatement to say that the past year was a busy one in the world of cybersecurity.

Ransomware continued to wreak havoc across the globe. New and increasingly devastating attacks upended organizations of every size, across every industry and in every jurisdiction. For example, a single ransomware attack contributed to the permanent closure of Lincoln College, a 157-year-old educational bastion in rural Illinois.[1] On the other end of the spectrum, a series of attacks paralyzed the government of Costa Rica, forcing officials there to declare a national emergency.[2]

The supply chain also found itself firmly in the sights of cyber criminals. Attackers doubled down on compromising third party, cloud and privileged identities to infiltrate networks and exfiltrate data.[3]

Meanwhile, critical infrastructure hung in the balance amid a backdrop of unrelenting attacks and geopolitical unease. Russian attackers targeted U.S. airports,[4] and Chinese-aligned threat actors exploited telecoms' vulnerabilities.[5]

The prior year, with most pandemic disruption overcome, CISOs for a brief time appeared to feel a sense of calm, composure and confidence in their security posture. Astoundingly, that feeling has already vanished, replaced by elevated concern.

As we look to 2023 and beyond, we can expect a return to a harsher reality. Ransomware looks set to wreak more disruption as data extortion becomes the rule rather than the exception. At the same time, increasing commercialization of dark-web exploit tools, initial-access brokers and "as-a-service" attack infrastructures threaten to make cyber crime even more open to anyone with a few dollars and ill intent.

Amid growing concerns around cyber risk and organizational preparedness, navigating this threat landscape remains a matter of protecting people and defending data. Modern CISOs know that users are at the center of cybersecurity. And they understand how critical it is to safeguard their organization's sensitive information, especially in light of an uncertain economy and employee churn.

To gain deeper insight into the mind of the CISO during this pivotal time, Proofpoint surveyed 1,600 of them from around the world. They graciously shared their experiences over the last year and their outlook for the years ahead.

In this summary of our findings, we explore how the global recession is applying pressure to security budgets and how CISOs must remain steadfast in pressing the C-suite for critical controls to protect their organizations. We also learn how boards are increasingly becoming part of the cybersecurity conversation and the impact this is having on their understanding of security issues and their relationships with CISOs. Finally, we unpack the issue of burnout among CISOs as many struggle with the pressures of personal liability and excessive expectations.

Once again, this report would not have been possible without the insight offered by cybersecurity and information security professionals across the globe. We offer our sincere thanks for your time and your feedback.

Lucia Milică Stacy, Global Resident CISO at Proofpoint

1 Kris Hold (Engadget). "A US college is shutting down for good following a ransomware attack." May 2022.
2 Kevin Collier (NBC News). "Costa Rica declares state of emergency over ransomware attack." May 2022.
3 Zack Whittaker (TechCrunch). "Okta says hundreds of companies impacted by security breach." March 2022.
4 Alyssa Blakemore (Daily Caller). "Russian Hackers Take On Major US Airports In Cyberattacks: REPORT." October 2022.
5 CISA. "People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices." June 2022.

Chapter 1: Back to "Business as Usual"

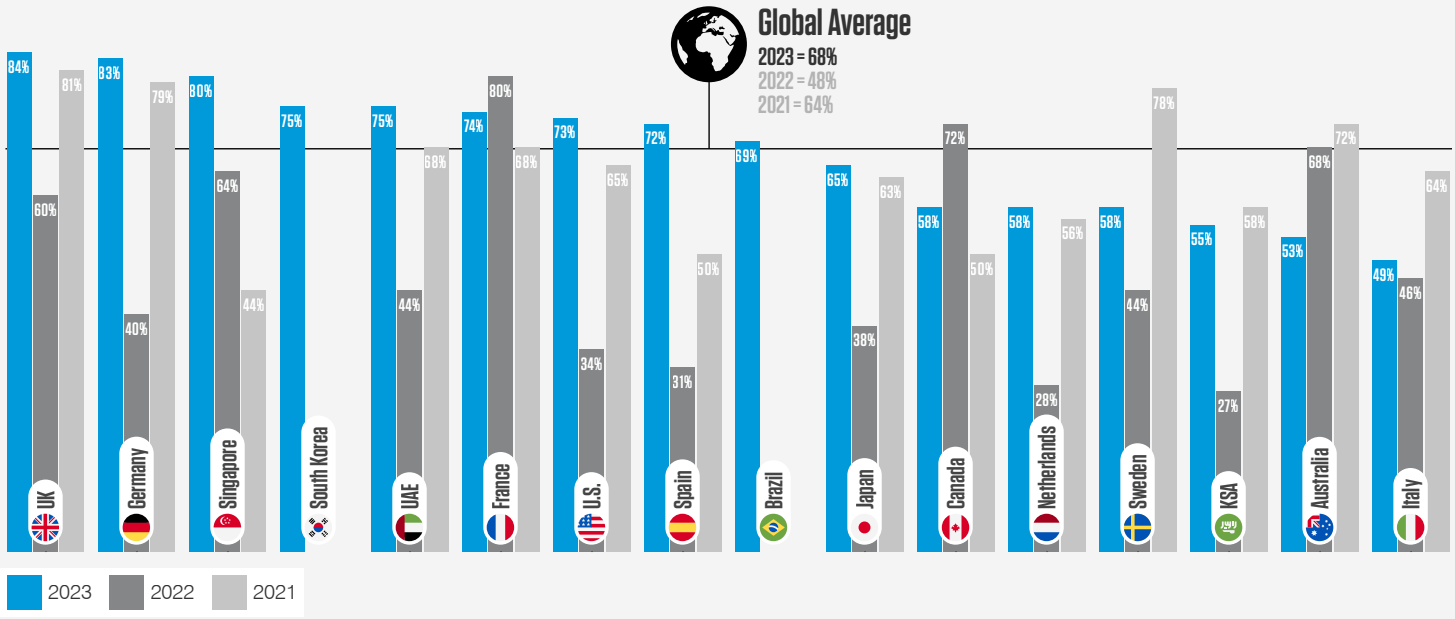
Last year's report uncovered a palpable feeling among CISOs that there was a period of calm after a once-in-a-generation crisis. With the pandemic disruption finally subsiding and hybrid work setups a mainstay for most, CISOs felt comfortable that the worst was behind them. At the time, just **48%** believed that a cyber attack was on the horizon within the coming year.

That's changing. In this year's survey, over two-thirds (**68%**) of CISOs said they feel at risk of a material cyber attack in the next 12 months. This pronounced shift suggests that security professionals see the threat landscape heating up once again, and have recalibrated their level of concern to match.

68%

of CISOs feel their organization is at risk of experiencing a material cyber attack in the next 12 months, with 25% rating the risk as very likely.

Percentage of CISOs who agree that their organization is at risk of a material cyber attack in the next 12 months



CISOs in the UK (**84%**), Germany (**83%**) and Singapore (**80%**) are most concerned about experiencing a material cyber attack.

Italy's CISOs are the most optimistic, with just **49%** fearing an attack.

CISOs (**68%**) and board members (**65%**) both feel that a material cyber attack is likely in the next 12 months.

Retail (**77%**), manufacturing (**76%**) and finance (**71%**) lead the way for cyber attack concerns across industry verticals.