NIGHTDRAGON

SPECIAL REPORT: CYBER LEADERS ON 2023 TRENDS AND 2024 OUTLOOK

Top cybersecurity leaders in the NightDragon Advisor Council provide perspective on 2023 trends and 2024 spending outlook

Foreward

As our digital age continues to expand and become ubiquitous across every piece of our life, it has become inevitable that cyberattacks continue to expand. Attackers continued to target healthcare, retail, casinos and other verticals with ransomware, bots, supply chain attacks, and other forms of attack, while geopolitical tensions continued to heighten cyber risk around the world, most recently with the recent outbreak of the Israel-Hamas war.

On the front lines of these continued challenges are Chief Information Security Officers (CISOs) and their teams, who are charged with defending the organization from attack. This is an essential job, one that is not only expanding in responsibility as threats rise but also scope, as threats expand across both digital and physical systems. For a sense of scale of the challenge at hand, there are an estimated 32,000 CISOs globally fighting against cyberattacks that occur on average every 39 seconds.

The good news? Budgets are going up, according to a NightDragon survey of CISOs from leading global organizations. Nearly 80% of CISOs said their budgets increased or significantly increased from 2022 to 2023, up from 66% last year. These budgets went to categories such as ransomware resiliency, managed detection and response, identify, cloud security, operational technology security, endpoint security, artificial intelligence, new team members and more.

80%

CISOs say they expect cyber budgets to increase in 2024

What's more, the vast majority of CISOs said they expect their budgets to increase again in 2024, with 80% reporting growing budgets, up from 67% last year. While the threat continues to rise in all areas and damages from cyberattacks expected to reach $10.5 trillion by 2025, according to Cybersecurity Ventures, it is encouraging to see our world's cyber leaders increasing their defenses of our most essential assets and fighting back against bad actors wishing to do harm. This trend also shows the continued importance of cyber budgets as part of the overall business. While other budgets may be feeling the long tail of the economic downturn we've experienced in the last few years, cyber budgets appear to be one area that remains resilient.

It's clear that our landscape will continue to evolve, a dynamic that's critical as we face new upcoming threats around elections, bots, artificial intelligence, ransomware and more. In

short: a world of heightened cyber risk appears to be our new permanent reality. In response, CISOs said they are looking at technologies like AI (for defense) and other emerging technology. trends that were not as clear priorities in previous years. What's more, we continue to see focus on new categories, such as passwordless, new data security areas, cloud security and more. As an investor, that gives me great optimism, but also as a long-term cybersecurity industry professional, it gives me hope for a bright and secure future together as an industry.

Read on in this report for further insights from some of the world's most important CISOs, including where they are investing, what technologies excite them in today's market, and what risk areas they view as most significant in the coming year.

Dave DeWalt
Founder and CEO of NightDragon
Former CEO of FireEye, McAfee and Documentum
Board Director at Delta Airlines, Five9 and other organizations

Table of Contents

Introduction

The NightDragon Advisor Council includes 100 leading CISOs, cyber experts and former government officials. These leaders come from Fortune 500 and other large enterprise organizations from a variety of critical verticals, including healthcare, finance, travel, critical infrastructure and more.

In this survey, NightDragon Advisors anonymously provided input into spending trends for 2023 and 2024, as well as what technology investments they were making (and some they weren't). They also provided insights into what risk areas concerned them the most last year, as well as what areas of risk they were prepping for in 2024.

A select outline of the findings can be found below:

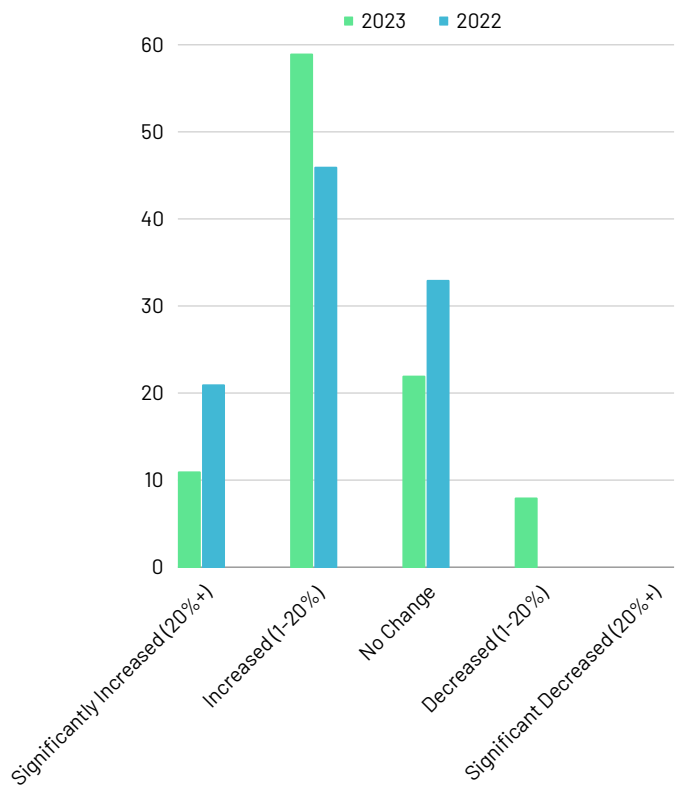
Findings

Respondents reported that cyber budgets continue to rise, with 80% saying that budgets increased or significantly increased in 2023. These increases demonstrated resilience of the cybersecurity line item in the budget, even as other budgets saw cuts or flat year over year trending for many organizations this year.

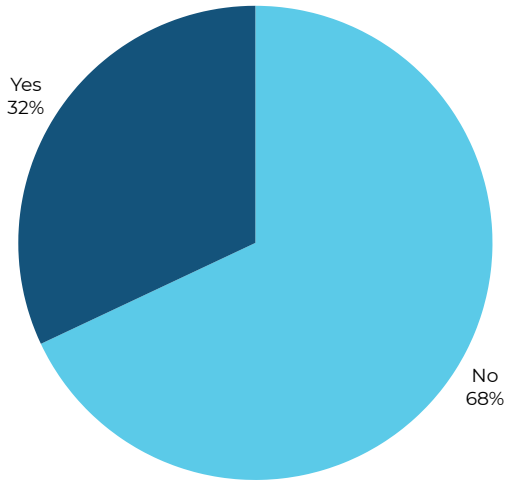
Additionally, many CISOs described net new investments in areas such as Zero Trust, data security, automation, artificial intelligence, talent and more.

Read on for more findings from the survey.

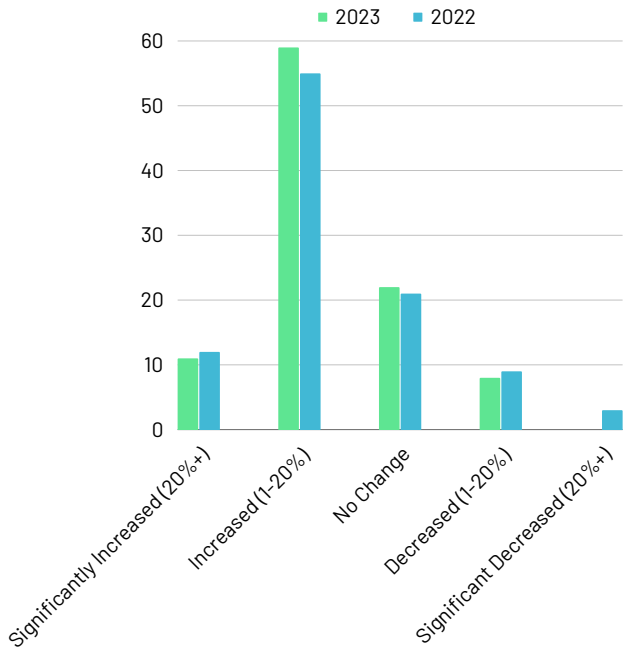
Did Your Cyber Budget Increase or Decrease YOY?



Did you Decrease Spend on any Cyber Category in 2023?



I Expect my Budget Next Year to..



*Note 2023 answers reflect perspective on 2024 budget and 2022 answers reflect perspectives on 2023 budget

What Were Your Three Biggest Risk Areas in 2023?

CISOs provided perspective on what three biggest risk areas they were concerned about in 2023. Below is a selection of the most popular answers (in no particular order).

- Third-party risk
- Ongoing geopolitical risk concerns from around the world
- New artificial intelligence threats
- Cyber talent and personnel skills gaps
- Ransomware
- Cloud security
- Data security
- Risk to critical infrastructure
- Lack of visibility into inventory connected to networks
- Social engineering and phishing
- Regulatory risk (ex. new SEC Cyber rule, privacy rules, etc.)
- Identity and authorization

"As a whole, 2023 was a reset reckoning for the industry. As a result, we continue to invest heavily going into 2024 on how we can better monitor and analyze risk and how we can quantify that risk over time."

- ADAM GLADSDEN

SVP Product, Cyber Risk Intelligence, Marsh

What do you Expect to be Your Biggest Cyber Investment Areas in 2024?

CISOs provided perspective on what areas they expect to pour money into in the coming year. Below is a selection of the most popular answers (in no particular order):

- Identity and identity management technology
- Threat detection and response
- Network modernization
- Cloud security
- People and enhancing talent
- Getting more value from existing technology stack
- Network segmentation
- Improving automation for tooling and reporting
- Application security testing
- Advocacy on cyber legislation and regulation
- Third party data and threat intelligence
- Operational Technology (OT) security
- Building security strategy around AI
- Data protection and data security

"The two biggest challenges we're watching in 2024 are insider threats and supply chain risk. Going forward, it is more important than ever to educate and raise awareness among teams that work on critical infrastructure, like that in clean energy, that cybersecurity is an essential component of their enterprise security. What's more, the cost associated with that cybersecurity will be a major challenge and major opportunity."

-BILYANA LILLY,
PhD, CISSP, Chair, Resilience Track, Warsaw Security Forum

Perspective From CISOs

"In 2024, what must be top of mind for CISOs include, continuing to build trust with critical infrastructure by focusing on data-driven supply chain security initiatives and collaboration to drive secure operations. The industry will work to further the "security by design" principles by articulating the collective responsibility of all actors along the supply chain. Additionally, CISOs must embrace the development of AI while exploiting its potential to improve security postures."

– CHRISTOPHE BLASSIAU, SVP, Cybersecurity & Product Security, Global CISO & CPSO, Schneider Electric

"Enablement and adoption are the keywords. If we don't enable advanced technologies like AI, we are not moving forward and are instead falling behind. We need to be focused as CISOs on enabling these technologies with great potential with the right legal and security frameworks behind it. That's hard with how much movement there is, but incredibly important as we look towards the future."

– HANAN SZWARCBORD, VP/ CSO, Micron

"2023 proved that no organization is immune from cyber terrorism and I don't think 2024 will get better unless we act. From multi-billion dollar casinos to rural school districts and water treatment facilities, new publicly available AI software and an increasingly volatile global threat landscape are expanding the physical and cyber threats posed to us all. The good news is that there is unprecedented technology innovation and awareness of the need to invest in cybersecurity, but as CISOs, we must continue to advance these areas together if we want to continue defending our organizations effectively."

– TIM ROEMER, Chief Security Officer, GMI.

Perspective From CISOs

In 2023, it became apparent that the lack of a geo-politically resilient digital environment, coupled with the effectiveness of certain cybercriminal actors wielding minimal entry costs for executing rapidly scalable and sophisticated attacks, underscores the imperative for organizations to resolutely pursue their journey towards cyber resilience. The observed supply chain attacks further highlight the systemic nature of cyber risk, emphasizing the critical importance of adopting an ecosystem approach.

In 2024, three key priorities should shape our cybersecurity focus:

- Stress Testing Cyberdefenses: Validate assumptions about defense in depth to limit the blast radius of attacks and avoid catastrophic losses
- Rethinking Control Stacks: In light of modern attacks, it is essential to reassess and adapt controls to enhance overall cybersecurity posture and improve cyber operation effectiveness.
- Smart Cyber Economics: Apply an outcome first approach and integrate cyber economics rigor into the selection and adoption of cybersecurity solutions for more effective risk management.

– RAMY HOUSSAINI, Founder and Chair, The Cyber Poverty Line Institute

Market Perspective: Impact of Government Actions on the Cyber Industry

Government actions in 2023 had and will continue to have major impacts on cybersecurity in 2024 and beyond.

AI WILL BE EXPLOITED BY ATTACKERS AND LEVERAGED BY DEFENDERS

In December 2023, Google Cloud released its Cybersecurity Forecast for 2024. The report predicted that generative AI and large language models (LLMs) will be utilized in various cyber-attacks such as phishing, SMS, and other types of social engineering. At the same time, defenders will also use AI to enable faster detection, response, and attribution of adversaries at scale, as well as faster analysis and reverse engineering. Government leaders are aware of the potential impacts of AI and have begun to develop governance mechanisms and frameworks to ensure its safe use. Specifically, National Institute of Standards and Technology (NIST)'s Artificial Intelligence Risk Management Framework (AI RMF 1.0) and President Biden's AI Executive Order (EO) are recognized for promoting the "safe, secure, and trustworthy development and use of artificial intelligence." The AI EO exceeds 100 pages and will significantly impact how AI is deployed and developed across organizations, some yet unknown. We will be watching how the AI EO translates into the President's Fiscal Year 2025 budget.

RELENTLESS TARGETING OF OUR INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE IS SERIOUS PROBLEM

Our adversaries' persistent and active penetration of U.S. computing systems is a significant cause for concern. While regulated critical sectors have made noteworthy progress, too many private sector companies have not adequately secured their data and information technology systems. Large and small companies fail to do the "cybersecurity basics" recommended in well-known and long-standing cybersecurity risk frameworks like NIST or Mitre Att&ck.

ADVERSARIES ENGINEER SOPHISTICATED AND WIDESPREAD DISINFORMATION

Our adversaries flood our digital communications channels with disinformation, accelerated exponentially by AI, to exacerbate the polarization of our society and

undermine Americans' confidence in our institutions. Our government and industry leaders understand this challenge and recognize that we must organize a more effective public-private response. We expect increased interest in technologies that combat disinformation by the government and investors.

CORPORATE DIRECTORS EXPECTED TO ENGAGE MORE IN CYBER GOVERNANCE

Last year, the Securities and Exchange Commission (SEC) approved new rules for publicly traded companies that require these entities to report material cyber incidents within four days. Concurrently, the SEC's recent legal action against a former corporate Chief Information Security Officer has sent a strong message that scrutiny will be applied to management.National organizations representing the corporate governance community recognize the need for directors to be more engaged in cybersecurity matters and to secure the resources to address this need.

THE GOVERNMENT WANTS MANUFACTURERS TO PRODUCE SAFER HARDWARE AND SOFTWARE

The federal government is flexing regulatory and procurement powers, along with its market influence, to get manufacturers to produce more secure hardware and software. The National Institute of Standards and Technology (NIST) has outlined the process wherein manufacturers may provide a Software Bill of Materials (SBOM) to accompany their products. SBOMs will eventually be incorporated into the procurement requirements of federal agencies' contracts. The White House directed the creation of a labeling system for Internet of Things (IoT) devices called "Cyber Trust Mark" that will signify that devices adhere to certain design principles and have certain baseline security features to allow consumers to buy such devices with security in mind. Another initiative, Secure by Design (SBD), led by the Cybersecurity and Infrastructure Security Agency (CISA), will allow consumers to know when manufacturers have followed certain security principles in their product design, development, configuration, and maintenance.

THE GOVERNMENT IS TIGHTENING CYBERSECURITY REQUIREMENTS FOR THE CRITICAL SECTORS

While the White House has called for more consistency, or "harmonization," of the cybersecurity requirements critical sector companies must follow, some regulators

have moved forward in tightening and clarifying what requirements these companies must follow. TSA has updated cybersecurity requirements for its sectors, including rail systems, commercial aviation, and pipelines. With the approval of the long-awaited "Cybersecurity Maturity Model Certification" (CMMC) rule, defense contractors will soon have to follow a derivative of the National Institute of Standards and Technology (NIST) cybersecurity controls and have their implementation of these verified by a third party. The advancement of CMMC suggests a growing belief by federal regulators that compliance regimes that rely only on self-attestation are inadequate to support the cyber-resiliency of critical sector companies.

POLITICAL AND BUDGET CHAOS IMPACTS OUR FEDERAL CYBER READINESS

The federal government has operated under a stop-gap spending measure, a "Continuing Resolution" (CR), since the new federal fiscal year began on October 1, 2023. The current CR expires on March 1 or March 8 (different dates for different groups of appropriations bills). While a deal on overarching budget numbers has been reached, if Congress cannot pass these appropriations bills, some agencies could be forced to shut down on those dates. Cybersecurity personnel are often deemed critical and, therefore, exempt from a shutdown; however, many could still be sent home during a shutdown. Reduced capacity would offer adversaries an opportune time to attack, and teams may also be unable to manage incidents as effectively. During the last government shutdown in 2018-2019, stories came to light about how basic cyber measures like routine patching of vulnerabilities, updating applications, and auditing of logs lapsed.

Katherine Hennessey Gronberg
Head of Government Services, NightDragon

Market Perspective: Evolving Go-to-Market Needs

Uncertainty in 2023 led to widespread unease and challenges, yet we adapt, and from that comes growth.

This uncertain macro environment had multiple effects on the startup and venture capital ecosystem. Global fundraising for 2023 was around $150B, down 50% from $300B in 2022 and marking the lowest total since 2015. Valuations also came down in 2023, although remain elevated relative to historical levels. Finally, while there were a handful of IPOs including ARM, Instacart and Klaviyo in Q3, lackluster post-IPO performance has generated little momentum for the market, marking the year as an underwhelming one for IPO exits.

Against this challenging backdrop, the tech startup ecosystem has been compelled to adapt and evolve their go-to-market strategies and overall businesses in ways that make them more resilient than ever before.

$150B

Global Fundraising in 2023, down 50% YOY

IN 2024, RUNNING A TIGHTER BUSINESS IS KEY TO SURVIVAL

The once abundant funding available to startups continued to become less reliable in 2023, compelling firms to reevaluate and optimize their cost structures while emphasizing self-sustaining cash flow generation. This shift marks a departure from the previous growth-at-all-costs strategy, steering startups toward a model of sustainable growth and profitability.

We've observed companies across sectors and of all sizes making strategic optimizations in key areas, including headcount reductions. This shift necessitates thinking differently about sales strategies and increasingly investing in channel and strategic partnerships, which allows companies to reduce direct selling costs while achieving greater scale. This approach not only conserves resources but also taps into the existing networks and strengths of partners, creating a more cost-effective and expansive reach.

INDUSTRY CONSOLIDATION: PARTNERS ARE YOUR ACQUIRERS

Following the IPOs of ARM, Klaviyo, and Instacart last September, the U.S. market has seen a scarcity of new listings and Klaviyo and Instacart notably underperformed against their IPO prices. This trend, in combination with the still uncertain macro environment mentioned above, suggests a continued slump in the IPO market in the near term, making M&A the predominant exit strategy for tech startups in 2024.

Here again, partnerships played a strategic role for startups in 2023, including those seeking exits. This was exemplified by CrowdStrike's acquisition of Bionic in Q3 and Palo Alto Network's purchase of Talon in Q4. In both cases, the target had existing partnerships/integrations with these larger tech platforms which increased their visibility and ultimately paved the way to acquisition. We expect to see this trend continue in 2024

INNOVATION LIKE WE'VE NEVER SEEN BEFORE: AI EXPERTISE REQUIRED

AI has created a paradigm shift in computing and business that will drive a new wave of investment in software. The software segment of the generative AI market alone was worth $3.7 billion in 2023 and is set to rise to $36.4 billion by 2028, a compound annual growth rate of nearly 58%. As the ecosystem explodes, entirely new categories of products and services are emerging around AI capabilities and AI-native businesses are being built and designed from the ground up with AI at the core. We're also seeing new leaders rise in various categories, as well as the emergence of developer tools and enablers that make it easier to build and leverage AI. Incorporating AI into products and leveraging LLMs is now table stakes for any business and those that don't get on board will be left behind.

In conclusion, the tech startup ecosystem, having navigated a year of challenges, is emerging more resilient and disciplined in approach. As we look to 2024 and beyond, the keys to success will lie in sustainable growth, strategic partnerships for scalable growth and paths to exit, and the embrace of new technologies. The future, though uncertain, is ripe with opportunities for those who are prepared to welcome change.

Joe Bubniak
VP, Corporate Development & Partnerships,
NightDragon

Market Perspective: A View From Israel

2023 was a year of recovery and resilience around the world, with new geopolitical, economic, social and other challenges emerging throughout the year. For Israel, these trends held true as well, if not more amplified with the country's war with Hamas that continues into 2024.

The impact of the war with Hamas has been significant on the Israeli people and economy. On January 7th (three months to the start of the war), it was reported that the war has already cost Israel 217M NIS, or $58B, so far. Despite these headwinds from the war and other factors, we continued to see strong innovation, exits, and opportunity coming out of the Israeli market. Israel has been known as the land of milk & honey for years, but really it is the land of milk, honey & resilience. The country currently stands as No. 1 in terms of R&D expenditure worldwide and counts many established companies, as well as innovative startups, amongst its ranks. High-tech accounts for 18.1% of Israel's GDP, for nearly 50% of its total exports, and about 12% of the workforce is high-tech, ranking Israel first globally. Additionally, the Israeli government continues to support growth, with a goal of 15% the total workforce in high-tech.

Venture Capital:
Israel funding took a bigger hit than the US in 2023, with $6.9B raised in Israel, down 50% YOY, and $170B raised in the US, down 17% YOY. This can be because the hype during 2021 was greater for Israeli companies or given the maturation of the US ecosystem. While Israeli funding amounted to only 4% of the total US funding, the exit value to capital invested ratio for Israel reached 1.58X compared to 0.4X in the US, making Israel an extremely attractive market for realized returns, even with a global decline in exits for 2023. Moreover, for the first time since 2018, the amount invested in Israeli startups for rounds with only foreign investors exceeded the amount raised in rounds with a mixture of foreign and Israeli investors, according to SNC's end of year report. Mega rounds totaled over $2B, with half coming from the fundraising rounds of Wiz, CATO, Snyk, Island, Cyera, and Cybereason.

Unicorns:
While Israel remains #1 in unicorns per capita, 2023 saw only two new unicorns compared to 21 and 40 in 2022 and 2021 respectively. This is not a surprise given normalization of valuations and the focus of later-stage startups on efficiency prior to their next fundraising round to avoid a potential down or flat round.

IPOs:
The IPO market has remained largely muted in the USA, and Israel has followed suit. Only 5 Israeli companies went public in 2023 compared to 17 in 2022. This is a decrease of about 70%, compared to a decrease of just 25% for USA-based companies.

M&A:
Out of the total realized value of exits in Israel, the vast majority was driven by M&A, rather than IPO or Buyout. 10 out of 15 of the top M&As in Israel for 2023 were in the security space, driven mostly by acquisitions by USA corporations in terms of quantity, but French multi-national Thales' acquisition of Imperva ($3.6B) trumped the value of all other top security M&As combined.

Israeli Influence on Global Cyber Companies:
On an analysis of the top 25 pure-play cyber companies listed in the US, 80% have an R&D center in Israel and 90% have acquired an Israeli company. The Israeli founded companies (PANW, CHKP, CYBR, S) amount to $130B (15% of summed $900B market cap) and have shown a YoY growth of 115%, 20%, 72%, 90%, respectively, with an average growth of 74% compared to the average YoY growth rate across the 25 companies of just 44%.

What remains to be seen is the impact from the current Israel-Hamas war, which continues to play out in the region. Factors potentially impacting GDP include the high costs of the war and the immediate call for duty of reservists. However, Israel's GDP growth has continuously outpaced the OECD average. Additionally, according to a report by Startup Nation Central, an analysis of Israeli companies funding during prior conflicts saw that the success of companies raising funds during the 2006 conflict (like Wix, SolarEdge, Taboola, Kaltura) was 63% and during the 2014 conflict (like JFrog, Forter, Argus, Payoneer) was 36% - both higher than conflict-free periods. So, it's important to keep a close eye on the companies that manage to raise funds during this time.

In sum: while Israel has faced its own challenges this year, it remains an extremely attractive market for investors as well as entrepreneurs looking to build their next company. Read more analysis on this market on the NightDragon blog.

Dorin Baniel
Principal and Head of EMEA, NightDragon

Media Contact

NightDragon
Sarah Kuranda Vallone, VP Marketing
sarah@nightdragon.com