wipro cybersecurity
by cybersecurists

STATE OF CYBERSECURITY REPORT #SOCR

AI STRENGTHENS AND DISRUPTS CYBER RESILIENCE

2025

SPOTLIGHT:
CYBER INVESTMENT AND FUNDING TRENDS

page 53

TABLE OF CONTENTS

A note from Tony Buffomante

TONY BUFFOMANTE

SVP & Global Head — Cybersecurity & Risk Services Wipro Ltd.

linkedin.com/in/buffomante

> **AI is driving continual innovation and disruption — acting as both friend and foe at a time when CISOs are under financial pressure to do more with less.**

Digital infrastructure transformation remains a top priority for today's business leaders. Increased technological complexity, constantly evolving regulations and a rise in sophisticated cyber threats across multi-hybrid cloud environments create daunting challenges for security teams. CISOs need to adopt a risk-adjusted, outcome-oriented mindset and transition from technologists who merely prevent and react to breaches to risk strategists focused on optimizing enterprise cyber resilience.

This report answers three key questions:

1. What is the current state of cyberattacks and breaches?
2. What is the state of enterprise capabilities for addressing evolving threats?
3. Which technologies are poised to impact enterprise cybersecurity in the near future?

The extensive data in this report reveal how global organizations are navigating today's cybersecurity environment.

Two big themes are at the forefront of these efforts:

AI and automation — AI is driving exponential productivity gains, enhancing threat detection, automating repetitive tasks, and remediating security vulnerabilities. By providing deeper insights than human analysis alone, AI empowers teams to focus on strategic initiatives, transforming cybersecurity programs by strengthening defenses, optimizing costs, and enabling faster, more agile threat responses.

Cost optimization — CISOs face growing pressure to maximize security investments with limited financial resources. Cyber strategies are shifting from simple budget increases to a more outcome-driven approach, prioritizing the use of people, processes, and technology to deliver greater cybersecurity and risk-adjusted returns on investments.

We are helping our clients adopt secure AI models and strike a balance between growing the business and defending the operations with more efficient spending. As we continue to expand our cyber capabilities, we have made a strategic internal investment to develop CyberTransform℠ — our advisory and implementation services that strengthen security and drive business growth. We've achieved this milestone through both organic growth, with the hiring of top talent, and inorganic growth, by acquiring companies that broaden our capabilities.

Our expansion into advisory and consulting perfectly complements our foundational CyberShield℠ managed services expertise. With over 9,000 expert Wipro Cybersecurists and our strategically located Cyber Defense Centers around the globe, we are ideally positioned to secure the modern enterprise with innovative, end-to-end holistic cybersecurity services.

We've entered an age where AI is both innovator and disruptor. It's likely the biggest change wave we have seen in our lifetime and it's altering how we view the fundamental roles of humans and machines. I hope this latest State of Cybersecurity Report provides insights that help you better understand how to leverage these changes to modernize your cyber strategies and strengthen your company's cyber resilience.

Editor's Note

JOSEY V GEORGE

General Manager – Emerging Tech, CRS

linkedin.com/in/josey-george

> **"Organizations willing to endure the refiner's fire for AI safety and security, will extract lasting value from AI's transformative power."**

Wipro's premier State of Cybersecurity Report was first released in 2017. This 2025 edition marks our sixth report. The journey through these nine years has been incredible for the Wipro team. There has been an exponential growth in downloads and readership from the global cybersecurity community.

We've maintained the basic ethos of the report by tracking cyber trends from macro, micro and future perspectives. We continue to learn from the past and to peek into the future by leveraging a wide range of primary and secondary research.

Right up front, check out our opening Sankey graph on global nation-state attacks that reflects how the ground wars have spilled over into the fifth warfare domain.

The last section covers cyber patent findings which give you a quantitative view of the ongoing global AI arms race and why we are seeing a bipolar contest emerging. Of course, there is much more in between these sections.

Whether you are a security executive or are responsible for focused cyber domains, you will find useful information in this report that can help you strengthen your cyber resilience in a cost-optimized manner.

Happy reading and keep the feedback coming!

EXECUTIVE SUMMARY

The Big Picture

The interplay between AI and cybersecurity will have far reaching consequences as organizations continue their digital transformation journey. AI will make cybersecurity capabilities more efficient and impactful across functions like risk assessments, compliance reporting, data protection, cyber defense, incident response, and other critical domains. But this is the proverbial double-edged sword. AI models and systems will be severely tested by targeted cyberattacks.

This year's State of Cybersecurity Report highlights macro perspectives on global nation-state cyberattacks, provides micro views of how organizations are mobilizing their cyber defenses and looks at what the future holds for cyber by examining patent filings and cyber venture investment trends.

Nation-state attacks and trade wars ramp up

The world is waking up to the reality of a heightened trade war and growing protectionism. Even before the trade wars kicked off, the focus of 86% of global nation-state attacks has been on intellectual property theft, and we expect this to further escalate in the current environment. The private sector has experienced 32% of all public nation-state attacks while 42% of attacks targeted government entities.

AI Enabled Attacks

Email phishing continues to be the dominant vector threat actors are using to breach security defenses. We expect phishing campaigns to get increasingly more sophisticated with the use of AI-enabled attacks. Among organizations that have experienced a breach, 31% have fallen victim to repeat breaches within a three-year window. This highlights the cascading and long-term effects breaches can have on brand reputation and stakeholder trust.

Risk reporting to the board is becoming more frequent

The good news is organizations are getting better at dealing with cybersecurity risks. The percentage of organizations with proactive cyber governance from the board increased over enterprises relying on reactive governance. Cyber risk reporting to the board is happening more frequently and the reliability and quality of these risk reports are improving thanks to the use of strategic technology.

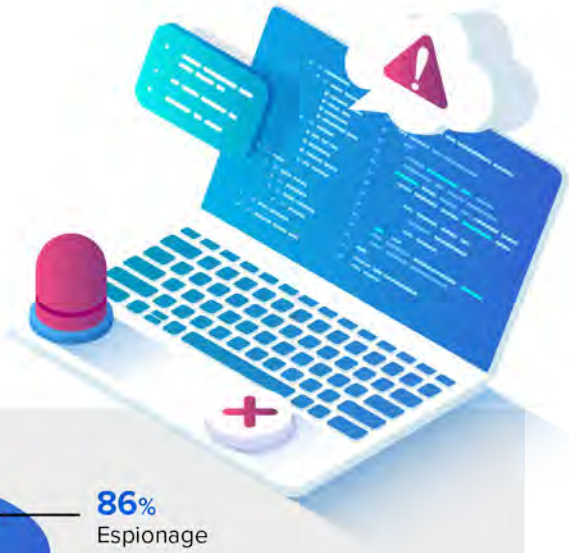
AI strengthens and disrupts

CISOs are evolving their security operations centers based on practical wins where GenAI can be realistically leveraged for speed and efficiency. When it comes to managing the safety and security risks of AI, organizations continue to struggle with fractured ownership, lack of AI expertise and an uncertain AI regulatory environment.

Agentic AI & PQC pave the way to the future

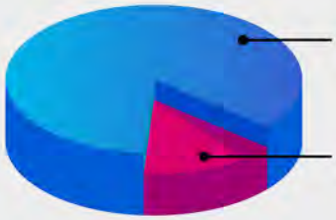
We examined future trends by reviewing global cyber patent filings and their geopolitical implications. While China has been leading the race in AI-related patent filings quantitatively, the bulk of their filings remain unprotected in patent realms outside of China. With the slew of competing GenAI models being released, the global AI arms race is heating up with the US continuing to be the driving force. Beyond AI patents, filings related to quantum computing and Post-Quantum Cryptography (PQC) are on the rise, indicating that we are closer to a seismic change in IT than what was previously thought. Venture investments in cybersecurity startups are also a great leading indicator for security teams to track. VC focus on Agentic AI and AI Guardrails standout. The US, Israel and Europe continue to dominate the security startup space based on the number of deals closed. The report highlights top research and investment trends in the future section.

STATE OF ATTACKS AND BREACHES

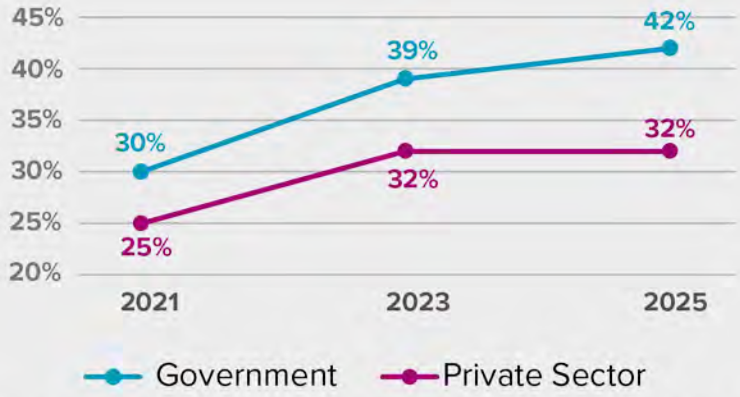


Espionage attacks dominate

Espionage attacks account for a staggering 86% of all nation-state cyber attacks.



SOCR 2023	SOCR 2025
82%	86%



Top target

Government and the private sector remain the top nation-state attack targets, with government experiencing a rising trend since 2023.

Top threats

Email phishing remains the top threat. Third-party risk surpassed ransomware attacks as second most significant threat.

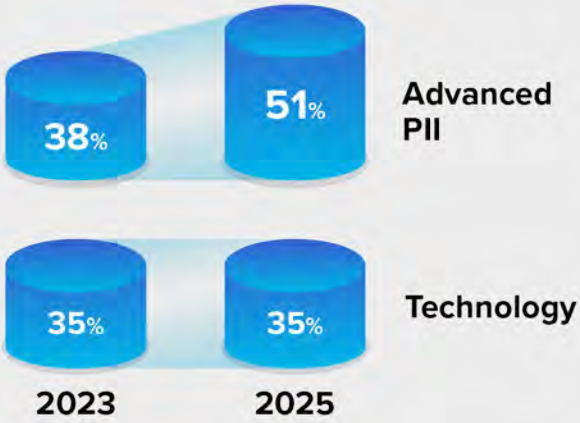
Email Phishing (2023 Rank 1st)

Third Party Risks (2023 Rank 3rd)

Security Awareness/Negligence (2023 Rank 4th)

Advanced PII is the most targeted data

Technology remains the most targeted sector.



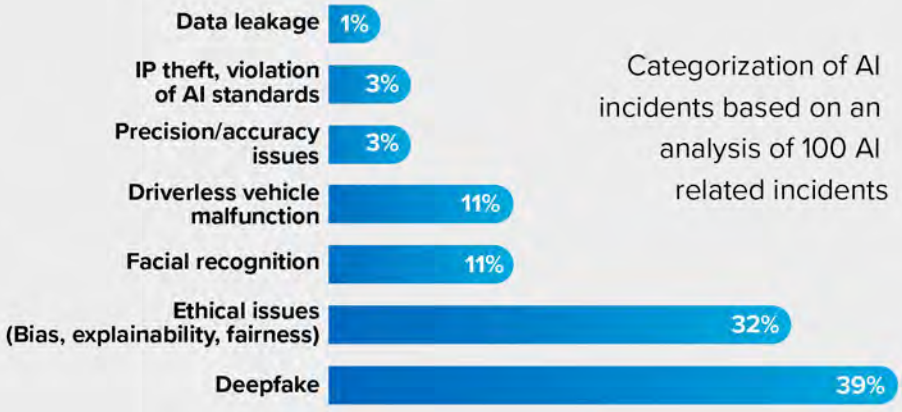
2023	2025
29%	31%

Repeat breaches

Around one-third of breached organizations (31%) faced repeat attacks within three years, a slight increase from 2023 (29%).

AI incident analysis

AI development needs to be accurate, ethical and responsible to safeguard against unintended consequences.



Categorization of AI incidents based on an analysis of 100 AI related incidents

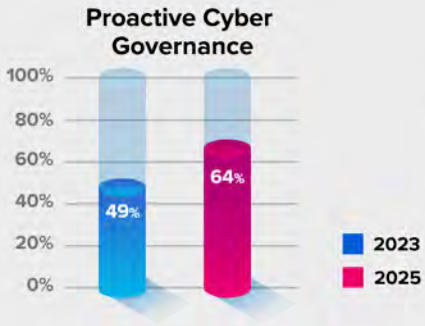
State of Attacks and Breaches

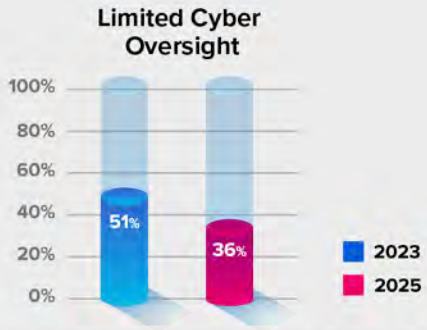
Read more on page 19

STATE OF CYBER CAPABILITIES

Board oversight: Momentum towards proactive governance

The number of organizations employing proactive cyber governance increased while those employing limited cyber oversight decreased.





Cyber risk reporting to the board is improving

2023

41% Quarterly
27% Monthly

68% of organizations report at least once per quarter

2025

50% Quarterly
25% Monthly

75% of organizations report at least once per quarter

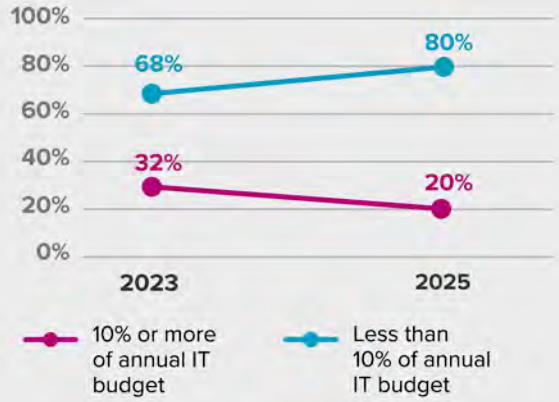
Compared to 2023, 7% more organizations are now reporting cyber risks to the board at least quarterly.

CISO reporting

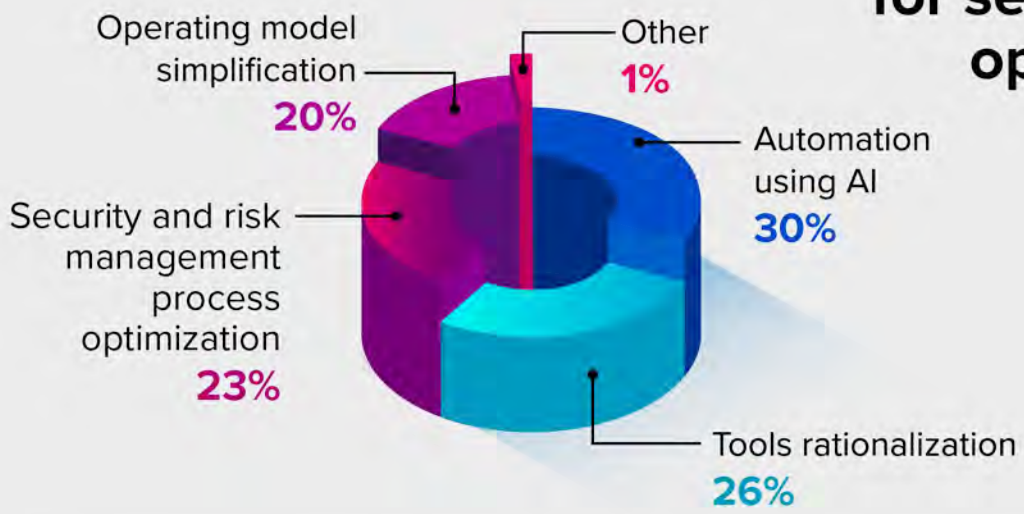
53% of CISOs report to the CIO but for the rest, "ownership of security" is scattered across various CXO functions.

Cybersecurity budgets under stress

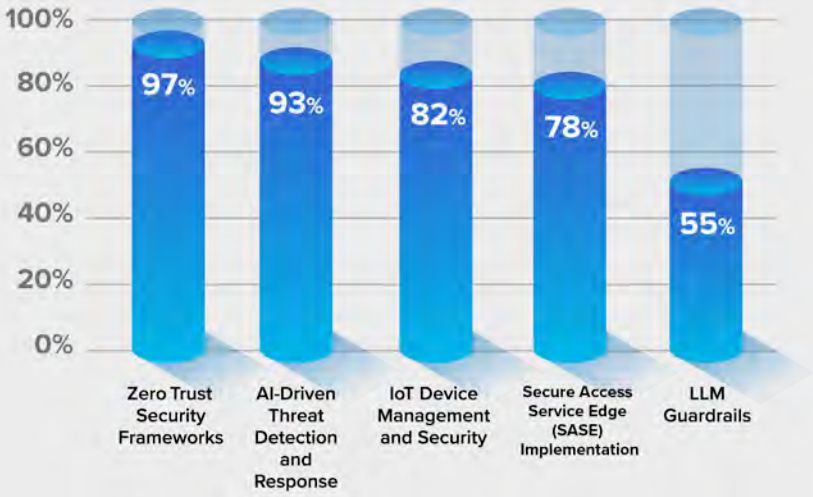
20% of organizations allocated more than 10% of their annual IT budget to cybersecurity, a 12% reduction from 2023.



Top focus areas for security cost optimization

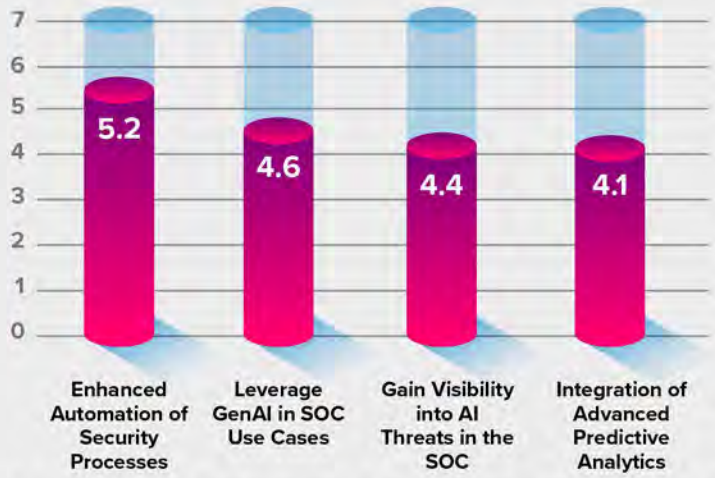


Zero Trust security, GenAI in cyber and AI guardrails are among the top investment priorities



Future priorities for SOCs

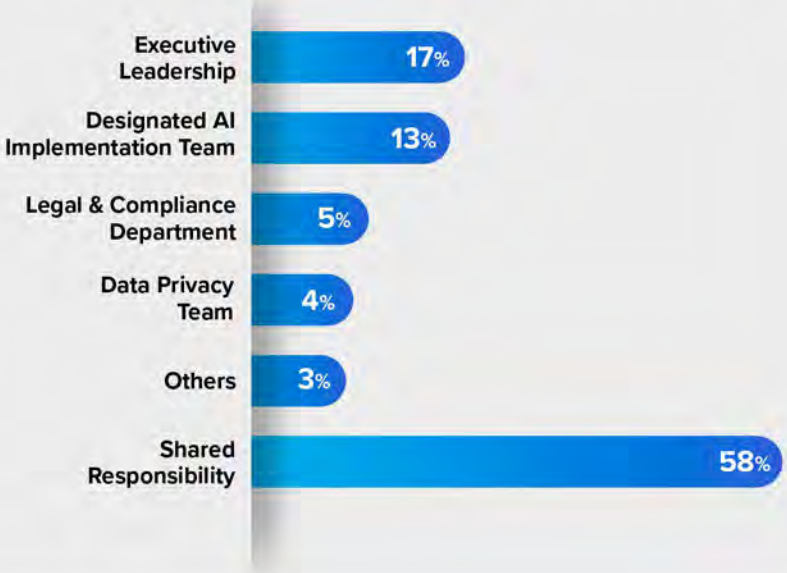
Security operation centers are adapting to new technology trends.



Challenges in implementing AI-driven cybersecurity

Cybersecurity teams are tackling foundational problems in implementing AI.

Who is driving the responsible AI charter?



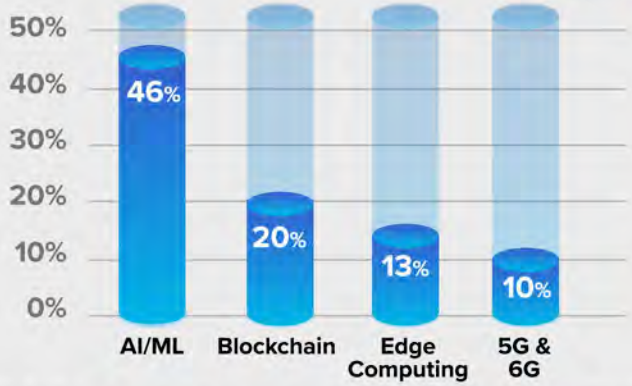
State of State of Cyber Capabilities

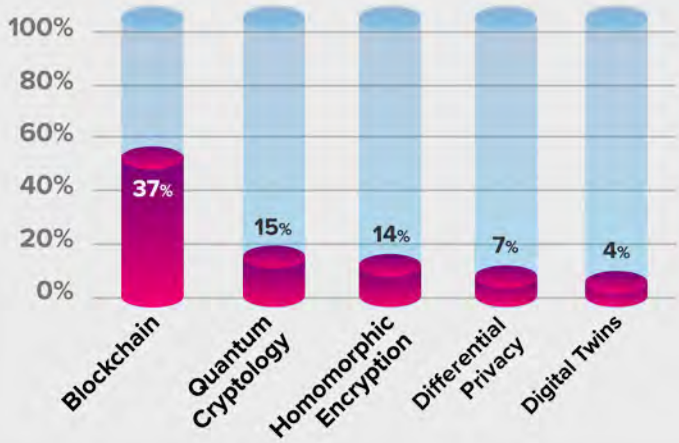
Read more on page 29

FUTURE OF CYBERSECURITY

Cyber technology patent trends

Patent filings in Data and Device Security along with technology categories like AI/ML, Blockchain and Edge Computing lead the way.



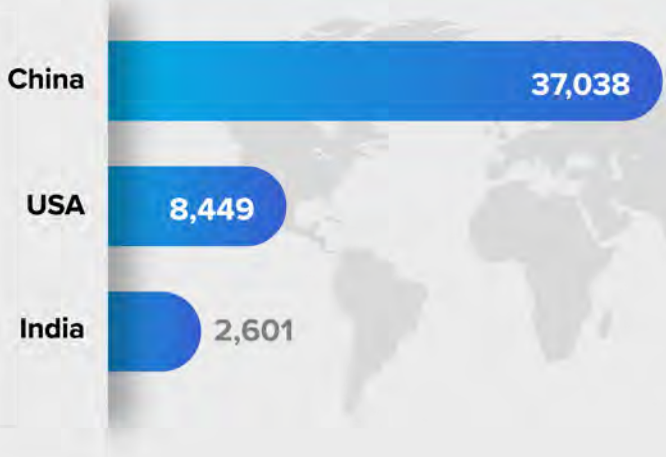


Top emerging technology domain patents (outside of AI/ML)

Blockchain leads submissions with over 11,000 patent families, followed by Quantum Cryptography with over 4,400 patent families (2019-2024 patent submissions).

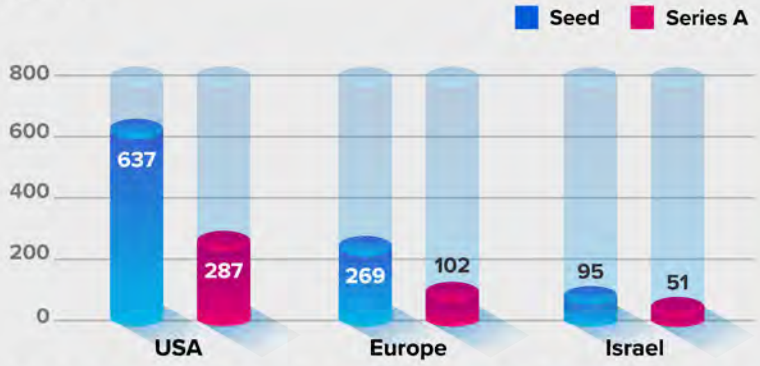
Global patent race

China continues to lead the global cyber patent submission race.



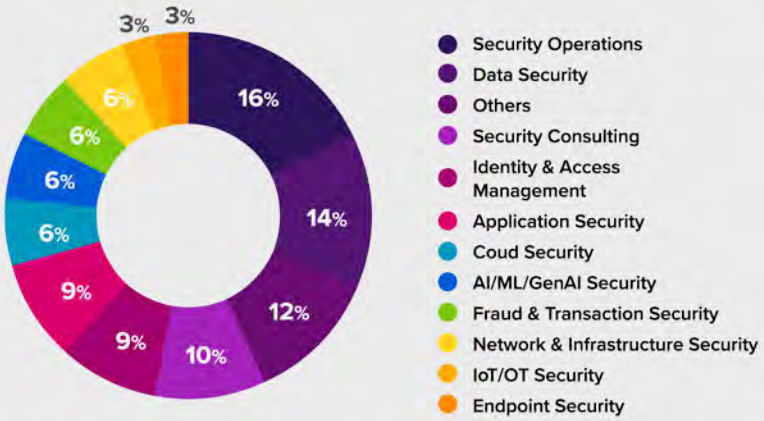
Top geographies in cyber investment deals

US, Europe and Israel remain the primary geographies where cybersecurity startups emerge, with 78% of the analyzed deals.



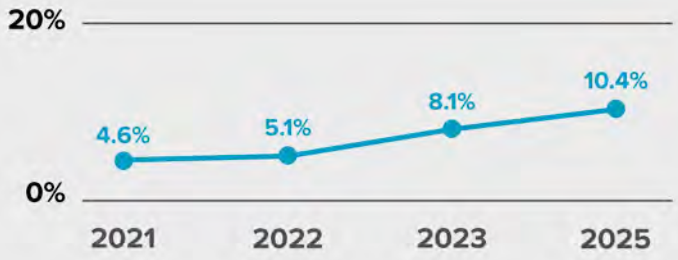
Top categories in seed deals

Security operations and data security startups dominate seed funding deals.



Increasing focus on AI/ML

Investors are betting on cyber startups that leverage AI/ML, with 10.4% of total seed funding deals.



Future of Cybersecurity

Read more on page 48

SECURITY TRENDS BY GEOGRAPHY

SECURITY TRENDS BY GEOGRAPHY

AMERICAS

Cyber Risk Reporting to the Board

45% of organizations report quarterly and **25%** report monthly

CISO Reporting

60% of CISOs report to the CIO and **15%** report to the CEO

Board's Cyber Expertise

75% of the boards have established some form of cybersecurity oversight

Recent Data Breaches

71% of organizations have experienced at least one breach in the last 3 years

Top 2 Cyber Risks

64% view email phishing as their top risk

55% view third-party risks as their top risk

SOC Evolution Priorities

Enhanced security processes automation is the top priority

Focus Areas for Cost Optimization

30% of organizations report tools rationalization is the top cost optimization focus

Security Budget

67% of organizations allocate less than **10%** of their IT budget for security

Top Investment Priorities

96% list Zero Trust security frameworks and AI-driven threat detection as top investment priorities

85% say IoT device management is their top priority

AI Implementation Challenges

85% view data quality and privacy concerns as top challenge

79% view lack of AI expertise within teams as top challenge

AI Implementation Responsibility

62% feel AI implementation is a shared responsibility

17% feel AI implementation is the responsibility of executive leadership

Impacts of Deepfake

Reputational damage is the top impact of deepfakes

SECURITY TRENDS BY GEOGRAPHY

EUROPE

Cyber Risk Reporting to the Board

57% of organizations report quarterly and **30%** report monthly

CISO Reporting

65% of CISOs report to the CIO and **17%** report to the CEO

Board's Cyber Expertise

70% of boards have established some form of cybersecurity oversight

Recent Data Breaches

52% of organizations have experienced at least one breach in the last 3 years

Top 2 Cyber Risks

61% view email phishing as their top risk

57% view ransomware attacks as their top risk

SOC Evolution Priorities

Leveraging GenAI in SOC use cases is the top priority

Focus Areas for Cost Optimization

41% of organizations list automation using AI as a top cost optimization focus

Security Budget

61% of organizations allocate less than **10%** of their IT budget for security

Top Investment Priorities

100% list Zero Trust security frameworks as their top investment priority

87% list AI-driven threat detection and response as their top priority

AI Implementation Challenges

96% view data quality and privacy concerns as top challenge

74% view Integration with existing security infrastructure as top challenge

AI Implementation Responsibility

70% feel that AI implementation is a shared responsibility

17% feel that AI implementation is the responsibility of executive leadership

Impacts of Deepfake

Reputational damage is the top impact of deepfakes

SECURITY TRENDS BY GEOGRAPHY

ASIA PACIFIC MIDDLE EAST AFRICA

Cyber Risk Reporting to the Board

47% of organizations report quarterly, **17%** report monthly and **17%** report biannually

CISO Reporting

40% of CISOs report to the CEO and **33%** report to the CIO

Board's Cyber Expertise

60% of the boards have established some form of cybersecurity oversight

Recent Data Breaches

40% of organizations have experienced at least one breach in the last 3 years

Top 2 Cyber Risks

70% view email phishing as their top risk

53% view security negligence as their top risk

SOC Evolution Priorities

Enhanced security processes automation is the top priority

Focus Areas for Cost Optimization

38% of organizations list automation using AI as a top cost optimization focus

Security Budget

73% of organizations allocate less than **10%** of their IT budget for security

Top Investment Priorities

97% list Zero Trust security frameworks as their top investment priority

93% list AI-driven threat detection and response as their top priority

AI Implementation Challenges

80% view integration with existing security infrastructure as the top challenge

73% view lack of budget/expertise and data quality and privacy concerns as top challenges

AI Implementation Responsibility

43% feel that AI implementation is a shared responsibility

16.5% feel that AI implementation is the responsibility of executive leadership/designated team

Impacts of Deepfake

Reputational damage is the top impact of deepfakes

STATE OF ATTACKS AND BREACHES

Nation-State Cyber Warfare

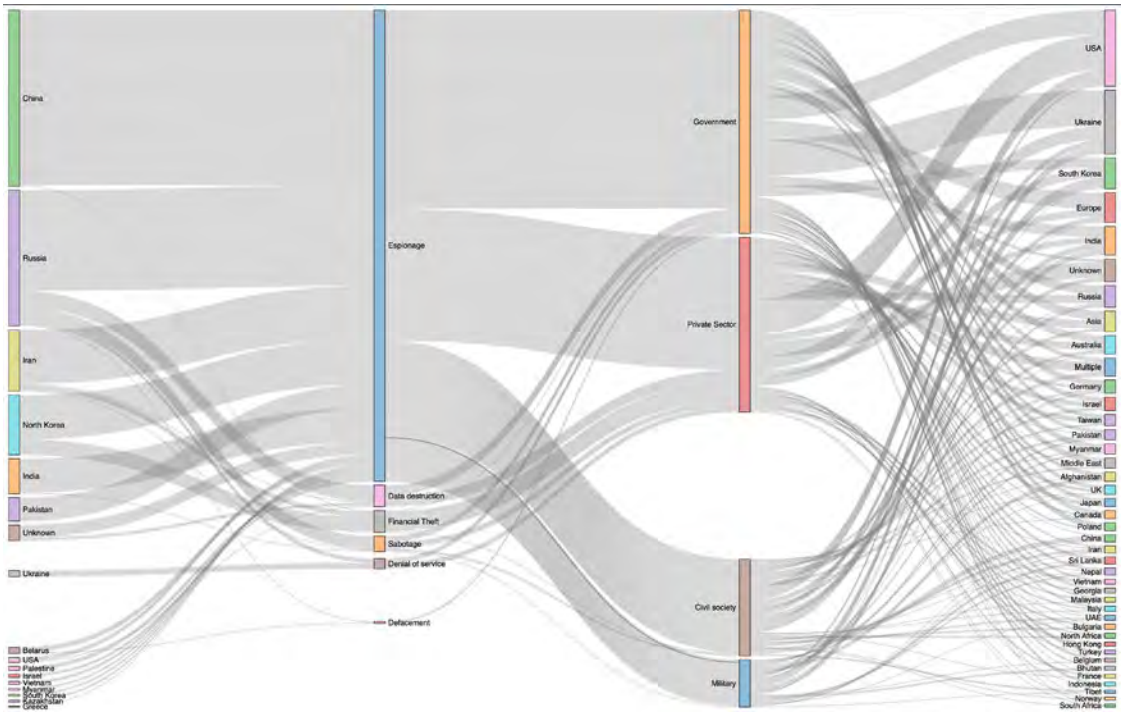
Nation-state cyberattacks are a major aspect of modern geopolitical conflicts. Nation-state actors are improving their cyber operations skills, creating sophisticated malware, taking advantage of weaknesses, and employing ever-more-advanced tactics to accomplish their goals. Primarily, these attacks aim to disable critical infrastructure, acquire or eliminate sensitive information, damage national security, and disrupt defense establishments.

To provide a macro view of the situation, we conducted a secondary data analysis tracked by the Council on Foreign Relations and the Center for Strategic and International Studies from 2022 to 2025. We analyzed the source countries and targeted countries along with the intents and types of attacks.

Data point summary

- 86% of all attacks are espionage related
- 42% of all targets are government entities
- The main aggressor countries are China, Russia, Iran and North Korea
- The most targeted country is the US, representing 12% of all attacks, followed by Ukraine at 11%

Figure 1: Nation State Attack Analysis



Top 5 trends:

1. Increased sophistication and persistence

Advanced persistent threats (APTs): Highly skilled and well-funded hacker groups backed by nation states can maintain long-term access to target networks. They often go undetected for an extended period while they siphon data, erase data, or conduct espionage activities.

Custom-built malware: Nation states are investing in sophisticated malware like zero-day exploits that are highly customized for specific targets, making them difficult to identify and defend against.

2. Targeting critical infrastructure

Disruption of essential services: Another common cyber warfare trend is the targeting of critical infrastructure like power transmission, goods transportation, healthcare, or payment infrastructure. These attacks aim to ensure services are either fully or partially disrupted.

Industrial control system (ICS) attacks: These attacks are focused on compromising the industrial control systems that operate critical infrastructures to inflict serious economic dam age, social crisis, or security concerns.

3. Cyber espionage and data theft

Intellectual property theft: Governments are waging cyber warfare against the private and public sectors to steal intellectual property, sensitive trade secrets, classified information, and military data. This poses significant risk to economic stability and national security.

Supply chain attacks: Governments are targeting critical supply chains to compromise sensitive information as well as cripple operations.

4. Weaponization of social media

Influence operations: Social media platforms are being used by adversary countries to spread disinformation, manipulate public opinion and influence election results. This can undermine trust in democratic processes and institutions and destabilize societies by furthering cultural and political divisiveness.

Harassment and intimidation: Social media is being used to harass and intimidate individuals or groups, with the intent of silencing dissent and suppressing free speech.

5. Offensive and defensive cyber capabilities:

Cyber arms race: Nation-states are developing offensive and defensive cyber capabilities. This is creating a cyber arms race with countries competing to develop the most advanced cyberattack tactics and malware, along with increasingly sophisticated threat detection methods.

As the threat of nation-state cyber warfare continues to evolve, governments and organizations around the world must invest in robust cyber defenses and develop effective strategies to protect against these adversaries. There is a growing need for international cooperation to develop common standards, share information and coordinate responses to cyberattacks.

Figure 2: Nation-State Attack Type Distribution

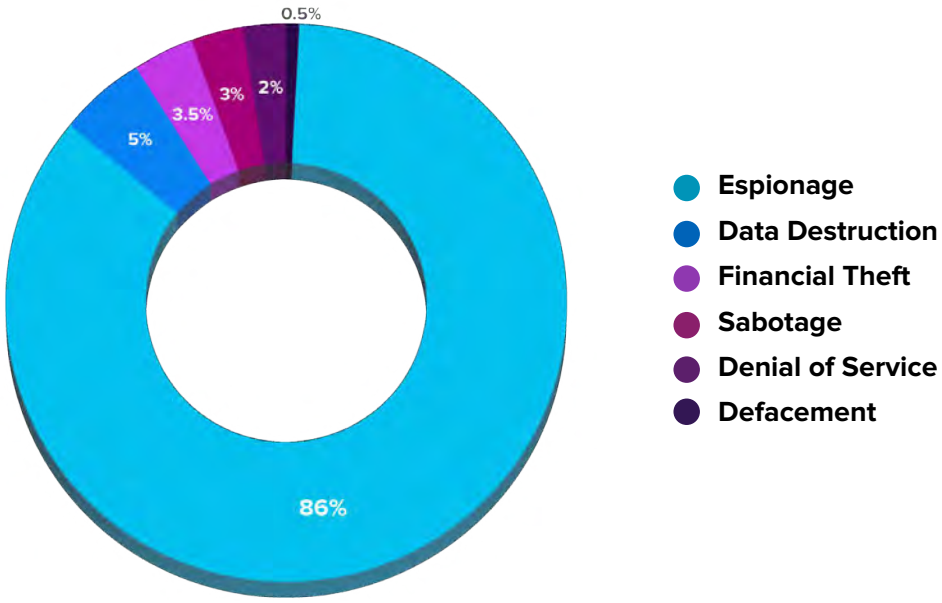


Figure 3: Nation-State Attacks by Target Categories

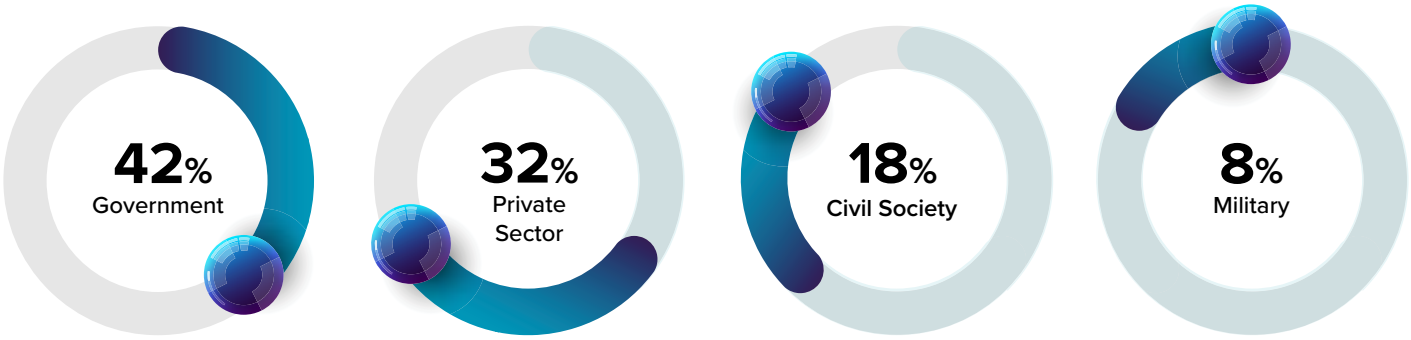
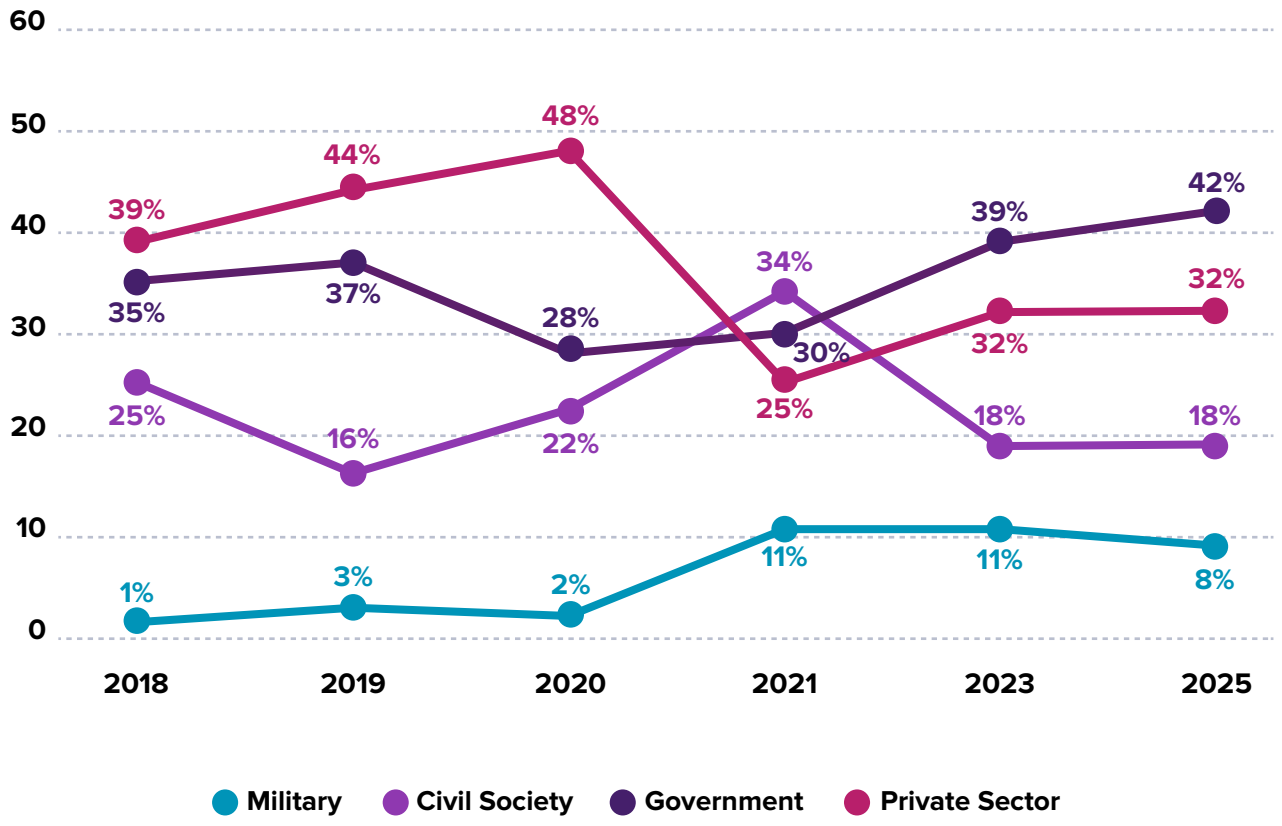


Figure 4: Nation-State Attack Trends by Target Category



Breaches – The Data and The Targets

Key data breach trends

Between 2022 and 2025, there was a notable increase in both the frequency and monetary impact of data breaches. Wipro's analysis of major breaches highlights key trends across various industries and types of data compromised, shedding light on attacker motives and evolving threat vectors.

Types of targeted data

An analysis of 84 major data breaches between July 2022 and June 2024 showed that different types of PII — personally identifiable information information — had distinct levels of economic value. We identified seven types of PII targeted by cyber attackers:

- **Basic PII** (name, contact number, email address, physical address)
- **Basic PII + financials** (tax information, payment card information, bank account statements)
- **Basic PII + IP address**
- **Basic PII + user credentials** (encrypted/unencrypted credentials)
- **Advanced PII** (Basic PII, gender, date of birth, identification numbers, driver's license numbers)
- **Advanced PII + financials**
- **Advanced PII + user credentials + IP address**

Approximately 51% of breaches involved advanced PII. This was an increase of 13% from statistics reported in our 2023 report.

16% of breaches involved basic PII data such as names, contact numbers, email addresses, and physical addresses.

15% of breaches included financial data often combined with advanced PII. This represents a decrease from the 20% reported in our 2023 data.

Figure 5: Classification of Compromised Data Across Top Breaches Worldwide

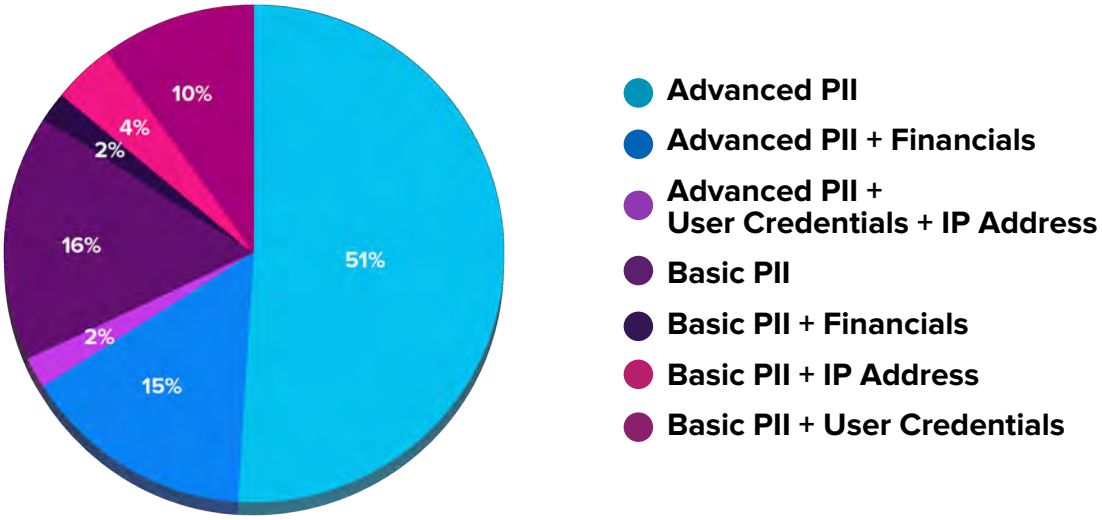
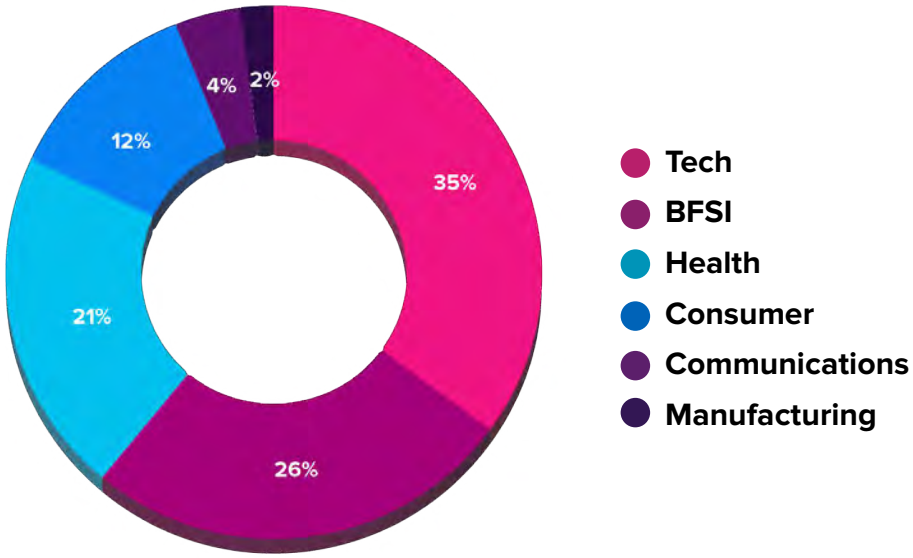


Figure 6: Distribution of Top Breaches Across Industry Sectors

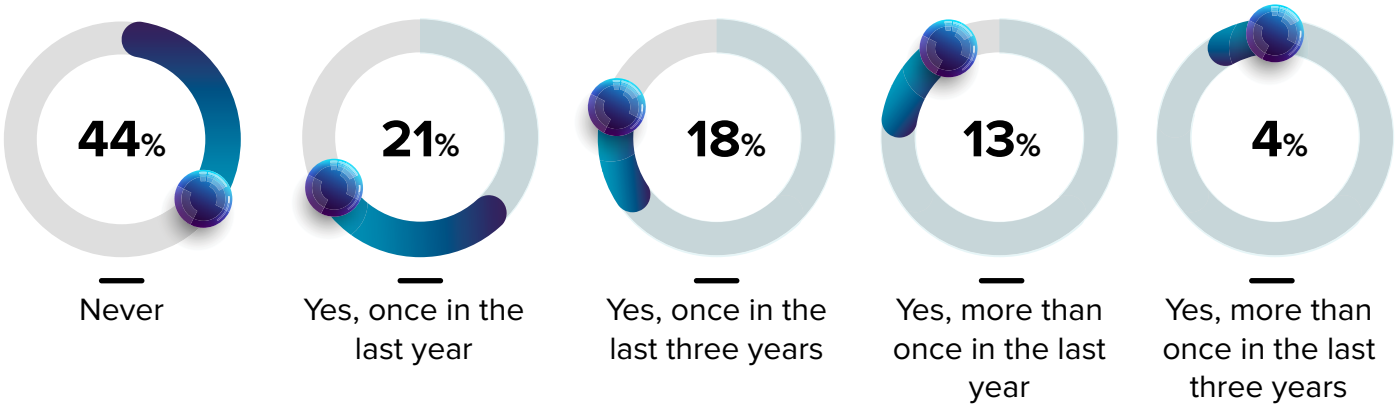


Motivations and attacker behavior

The motivations behind cyberattacks are diverse. The trends observed from 2022 to 2025 suggest a shifting threat landscape where attackers are targeting advanced PII for more long-term exploitation and focusing on sectors handling sensitive data, such as technology, BFSI, and healthcare. The growing complexity of attacks demands a stronger, more agile response from organizations, including robust security measures and continuous threat assessment to mitigate risks. The future of cybersecurity will depend on proactive measures, cross-industry collaboration, and technological advancements to keep pace with evolving threats.

Trends observed from 2022 to 2025 suggest a shifting threat landscape where attackers are targeting advanced PII for more long-term exploitation.

Has your organization identified a data breach in the recent past?



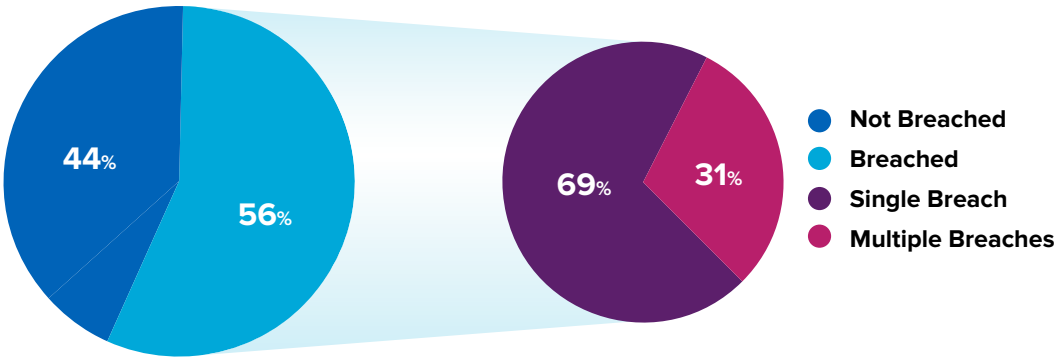


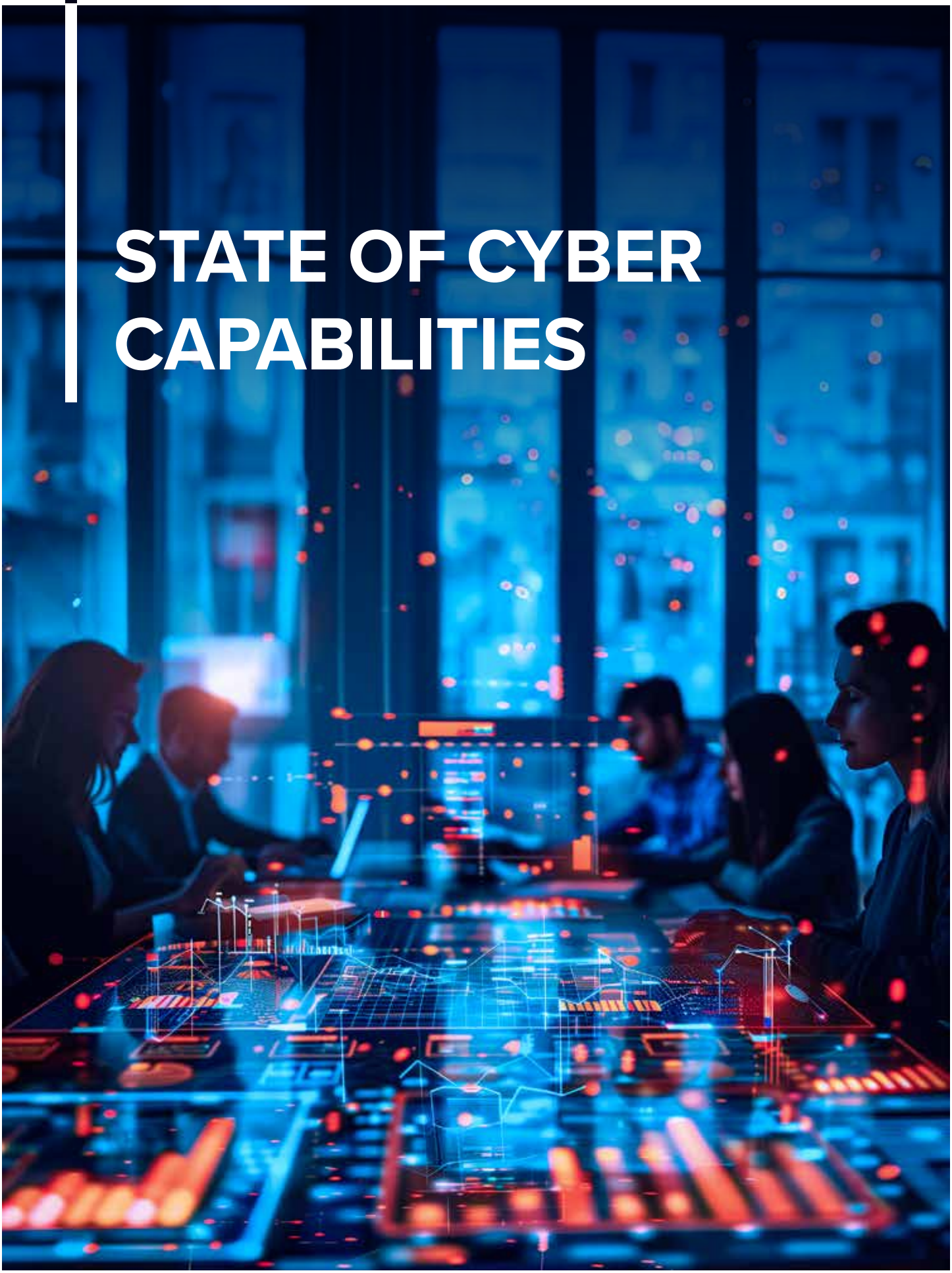
Figure 7: Data Breaches Identified in Recent Past Across Organizations

Among surveyed organizations, 56% identified one or more data breaches in the recent past. Around one third (31%) of these organizations experienced a repeat breach within three years of the first breach. Another concerning trend is that 13% of surveyed organizations experienced more than one breach in a span of just one year, up from just 8% revealed in the 2023 data.

Among organizations that experienced repeat incursions, often the subsequent breaches were not linked to the initial attack. After learning of a breach, new threat actors are motivated to attack, illustrating the ongoing harm that breach publicity can inflict on enterprises.
The flip side is that many breaches remain undetected for extended periods. This lack of visibility means that organizations may be unaware of repeat breaches, compromising their efforts to effectively secure their systems.
The data underscore the importance of robust cybersecurity measures and continuous monitoring to promptly detect and mitigate breaches.

Among surveyed organizations, 56% identified one or more data breaches in the recent past. 31% of these organizations experienced a repeat breach within three years of the first breach.

STATE OF CYBER CAPABILITIES



Top Cyber Risks

While the emergence of AI has reshaped the dynamic cyber threat landscape, the top risk in 2025—email phishing—remained the same as reported in 2023. Third-party risk emerged as the second significant risk, replacing ransomware attacks.

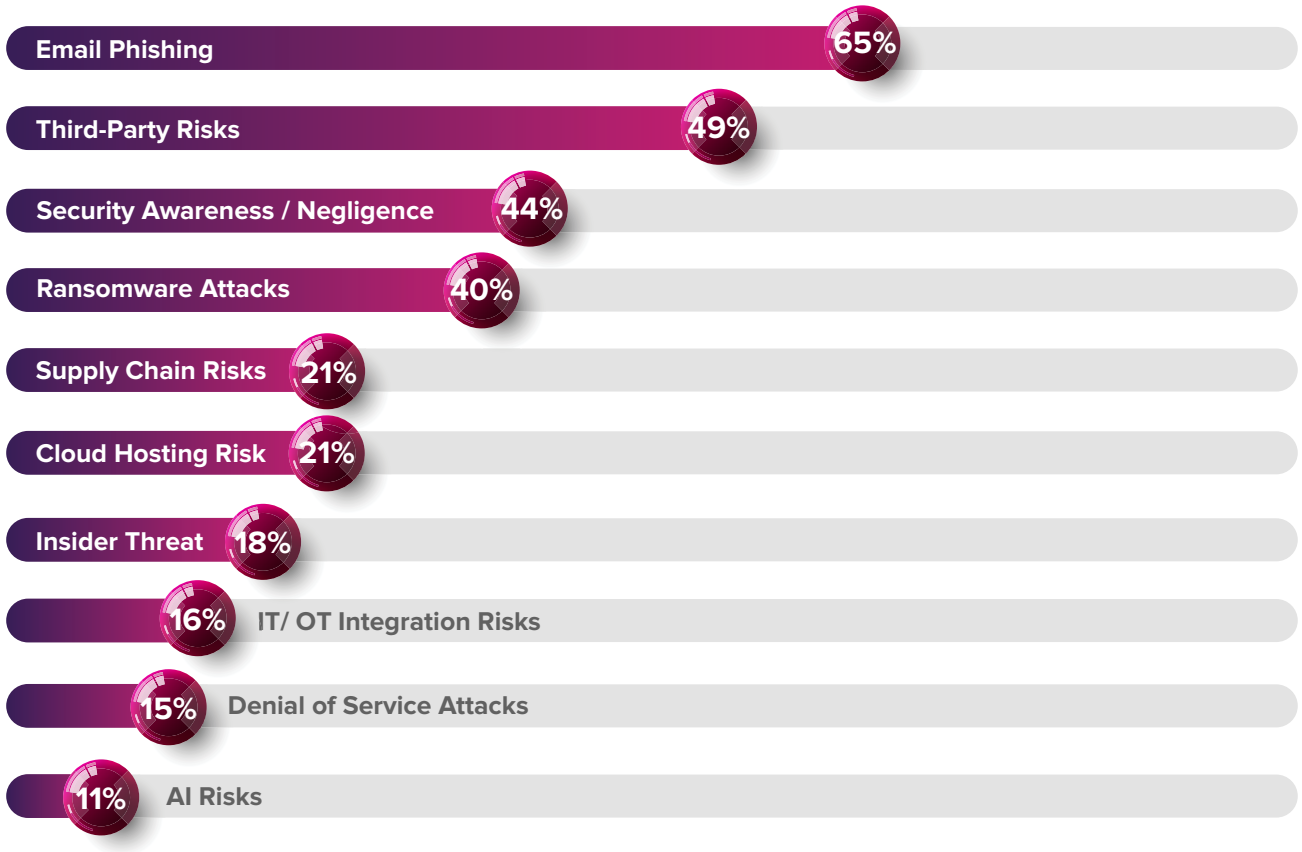


Figure 8: Top Cyber Risks

Email phishing (65%): Cybercriminals are increasingly using AI to automate attacks, develop sophisticated malware, and create highly convincing phishing schemes.

Third-party risks (49%): Interconnected ecosystems amplify third-party vulnerabilities, necessitating stringent risk management and continuous monitoring.

Security awareness / negligence (44%): As attackers adopt more advanced AI technologies, it is important to develop and practice a strong security awareness program so employees can identify and avoid potential security threats.

Ransomware attacks (40%): As targeted extortion tactics replace more widespread attacks, companies must implement robust backup, protection and incident response strategies.

To stay ahead of these threats, organizations must invest in advanced AI-driven security solutions, continuously monitor AI developments, and foster a culture of innovation and adaptation within their cybersecurity teams. This requires a proactive approach to cybersecurity, leveraging advanced technologies and fostering a culture of security awareness to safeguard digital assets.

Cybercriminals are using AI to automate attacks, develop sophisticated malware, and create highly convincing phishing schemes.

Board Alignment for Cybersecurity

As cyber threats continue to evolve in complexity and frequency, the role of corporate boards in overseeing and guiding cybersecurity strategies is also growing. Effective cyber governance is about ensuring the resilience and trustworthiness of the entire digital enterprise. This necessitates a strategic alignment between the board and cybersecurity functions that promotes proactive risk management and informed decision-making.

Boards must move beyond traditional oversight roles and become actively engaged in cybersecurity governance. This shift is driven by the need to address regulatory requirements, stakeholder expectations, and the increasing financial and reputational risks associated with cyber incidents. By integrating cybersecurity expertise at the board level and establishing dedicated subcommittees, organizations can better navigate the complexities of cyber risk and enhance the organization's overall security posture. The following analysis delves into the current state of board involvement in cybersecurity, highlighting key trends and the growing emphasis on proactive governance.

As regulatory pressures mount, it is anticipated that more boards will integrate dedicated cybersecurity experts and form specialized subcommittees.

According to our latest research, board involvement in cybersecurity is evolving in a positive direction. The survey responses can be grouped into two categories:

1. **Limited Cyber Oversight:**

   This group reflects a more hands-off approach to cybersecurity governance and includes organizations with an independent cyber advisor appointed by the board (5%) and those with no specific owner for cyber within the board structure (31%). In 2023, approximately 51% of organizations fell into the limited cyber oversight group. In 2025, that number fell to 36%, indicating a general improvement in board involvement.

2. **Proactive Cyber Governance:**

   This group reflects a higher level of dedicated cybersecurity oversight and governance within the board due to the inclusion of designated board members with cyber risk experience (23%) and/or a separate cyber risk committee to oversee cybersecurity preparedness (41%). Proactive cyber governance organizations increased from 49% in 2023 to approximately 64% in 2025.

As regulatory pressures mount, it is anticipated that more boards will integrate dedicated cybersecurity experts and form specialized subcommittees. This trend is expected to enhance business alignment, budgeting, and communication both within the enterprise and with external regulators. The presence of well-coordinated board expertise will be crucial in navigating the complex landscape of cybersecurity governance in the coming years.

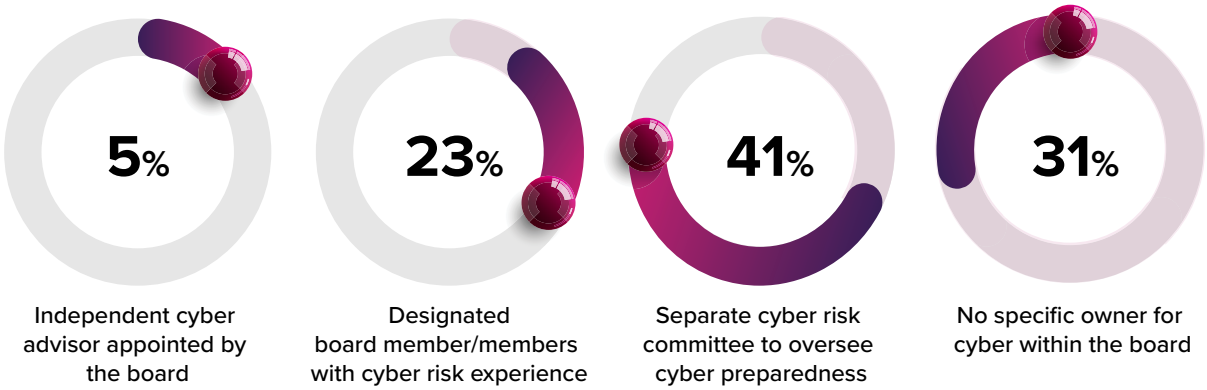


Figure 9: Board Alignment to Oversee Cyber Risks

CISO Reporting

As enterprises advance in their digital transformation journeys, cyber risk management and reporting strategies are evolving. We've shown that incorporating cyber expertise at the board level is critical. Given the pressures on IT departments to deliver innovative technology and keep pace with market demands, it is equally important to position risk management and reporting responsibilities in the most effective manner below the board.

For well over a decade, it's been most common for CISOs to report to CIOs. This has been reasonably effective for IT risk management.

Our survey data reveals that 53% of organizations still have their CISOs reporting to the CIO. 22% of organizations now have their CISOs report directly to the CEO or have regular CEO reviews, and 8% report to the CFO. Additionally, 17% of CISOs report to other C-level executives such as the COO, CRO or the general counsel.

Some organizations are transitioning cybersecurity into a business-risk-aligned management structure to enhance accountability at the board level, promote risk-aware behavior throughout the organization, and strengthen the case for necessary cybersecurity investments. This realignment ensures that cybersecurity is recognized not merely as an IT concern but as a vital element of the overall business strategy.

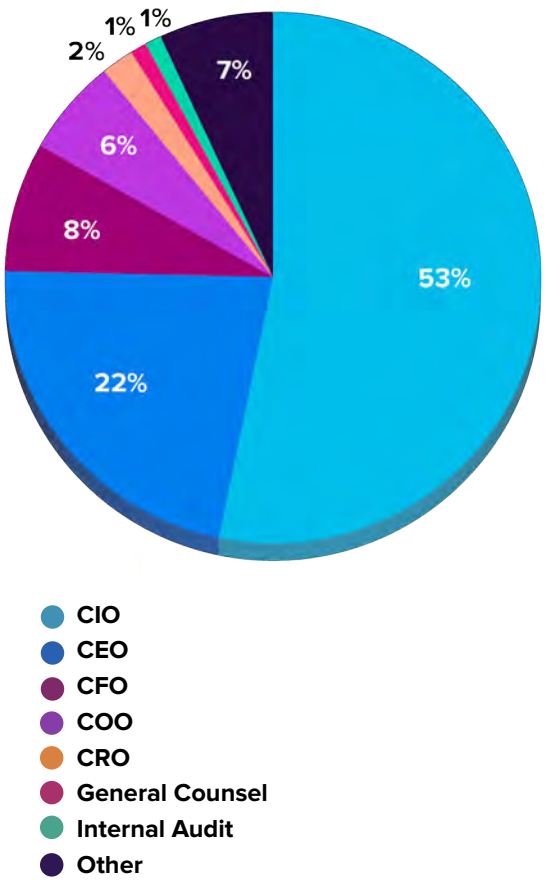


Figure 10: CISO Direct Reporting

Cyber Risk Reporting

Due to evolving regulations on cyber disclosures, board visibility on cyber risk reports is a critical factor in maintaining robust cybersecurity governance.

According to the latest survey, 50% of organizations now report cyber risks to their boards on a quarterly basis, a significant increase from 2023 (41%). 25% of organizations provide monthly cyber risk reports, while 11% report semi-annually. This upward trend shows growing emphasis on regular cybersecurity reporting to higher management. At the other end of the scale, 8% of organizations report on an annual basis, and 3% do so on an ad hoc basis.

Notably, 3% of organizations do not have a formal reporting mechanism in place. These findings highlight the diverse approaches organizations are taking to keep their boards informed about cybersecurity risks.

50% of organizations now report cyber risks to their boards on a quarterly basis, a significant increase from previous years.

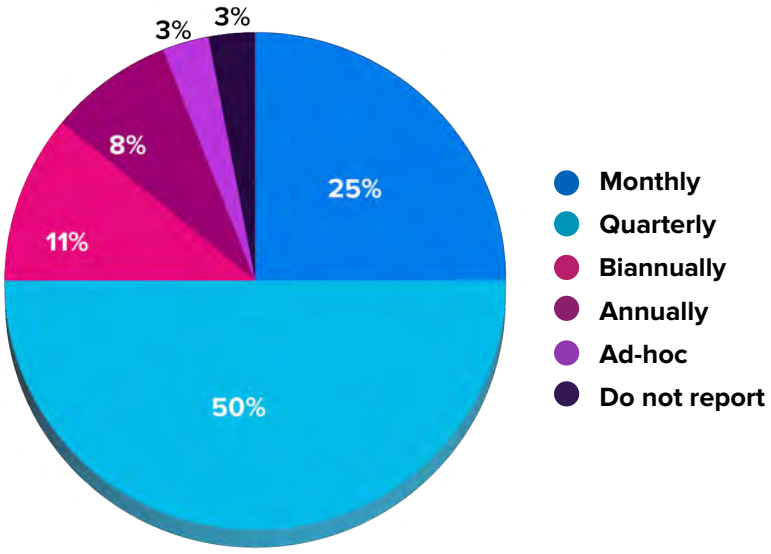


Figure 11: Frequency of Cyber Risk Reporting to the Board

Security Budget and Investment Priorities

In this latest survey, only 10% of organizations reported allocating more than 12% of their annual IT budget to cybersecurity, compared to 21% in2023. Looking at this another way, only 20% of organizations are allocating more than 10% of their annual IT budget for security compared to 32% in 2023.

This indicates that cybersecurity budgets may not be keeping pace with the growing sophistication of cyber threats.

The cybersecurity budget is a critical component if an organization expects to improve its risk management strategy. But it's clear that security budgets are experiencing a downturn due to general economic concerns and heightened scrutiny of corporate budgets across the enterprise. Organizations are gradually shifting priorities towards spending better rather than spending more. In this environment, cybersecurity spend needs to be well thought out, optimized and prioritized toward the most critical assets and vulnerabilities. Security leaders are under increasing pressure to follow a strategy that is both cost effective and aligned with the organization's strategic priorities.

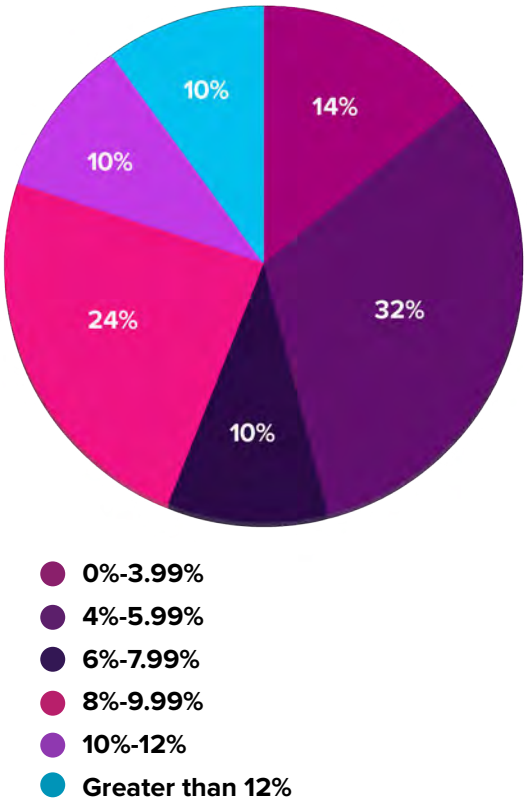


Figure 12: Percentage Range of Annual IT Budget Allocated for Security

Only 10% of organizations reported allocating more than 12% of their annual IT budget to cybersecurity, a significant decrease from 2023 (21%).

Strategic cybersecurity investment trends

Organizations are taking a strategic approach to cybersecurity, aiming to more efficiently bolster defenses and adapt to the evolving threat landscape by prioritizing the following key cybersecurity technologies:

- **Zero Trust** — 97% of surveyed businesses identified Zero Trust security frameworks as a top investment priority, underscoring its importance in highly networked environments.
- **AI** — 93% are focused on AI-driven threat detection and response to enhance security measures.
- **IoT** — 82% are investing in IoT device management and security to address the growing risks associated with the proliferation of connected devices.
- **Secure Access Service Edge (SASE)** — 78% of organizations are prioritizing investment in SASE to cope with rapid cloud adoption, the rise of remote work and the evolving threat landscape.
- **LLM guardrails** — 55% are prioritizing LLM guard rails, reflecting the need to manage and secure access to large language models for enterprise applications such as chat, summarization and other use cases.

97% of surveyed businesses identified Zero Trust security frameworks as a top investment priority, underscoring its importance in highly networked environments.

- **Quantum resistant encryption** — 36% are investing in crypto discovery, creation of crypto BOM and rollout of a hybrid crypto platform to support quantum-resistant encryption and legacy crypto in parallel to prepare for future threats posed by quantum computing.
- **Blockchain for enhanced security protocols** — 20% of organizations are investing in blockchain technology to bolster security. The decentralized and cryptographic nature of blockchain creates challenges for bad actors attempting to access sensitive information, making it a strategic option for implementing stringent data protection measures. Critical industries including banking, healthcare and manufacturing can benefit from the heightened data security, transparency and resilience against attacks offered by blockchain technology.

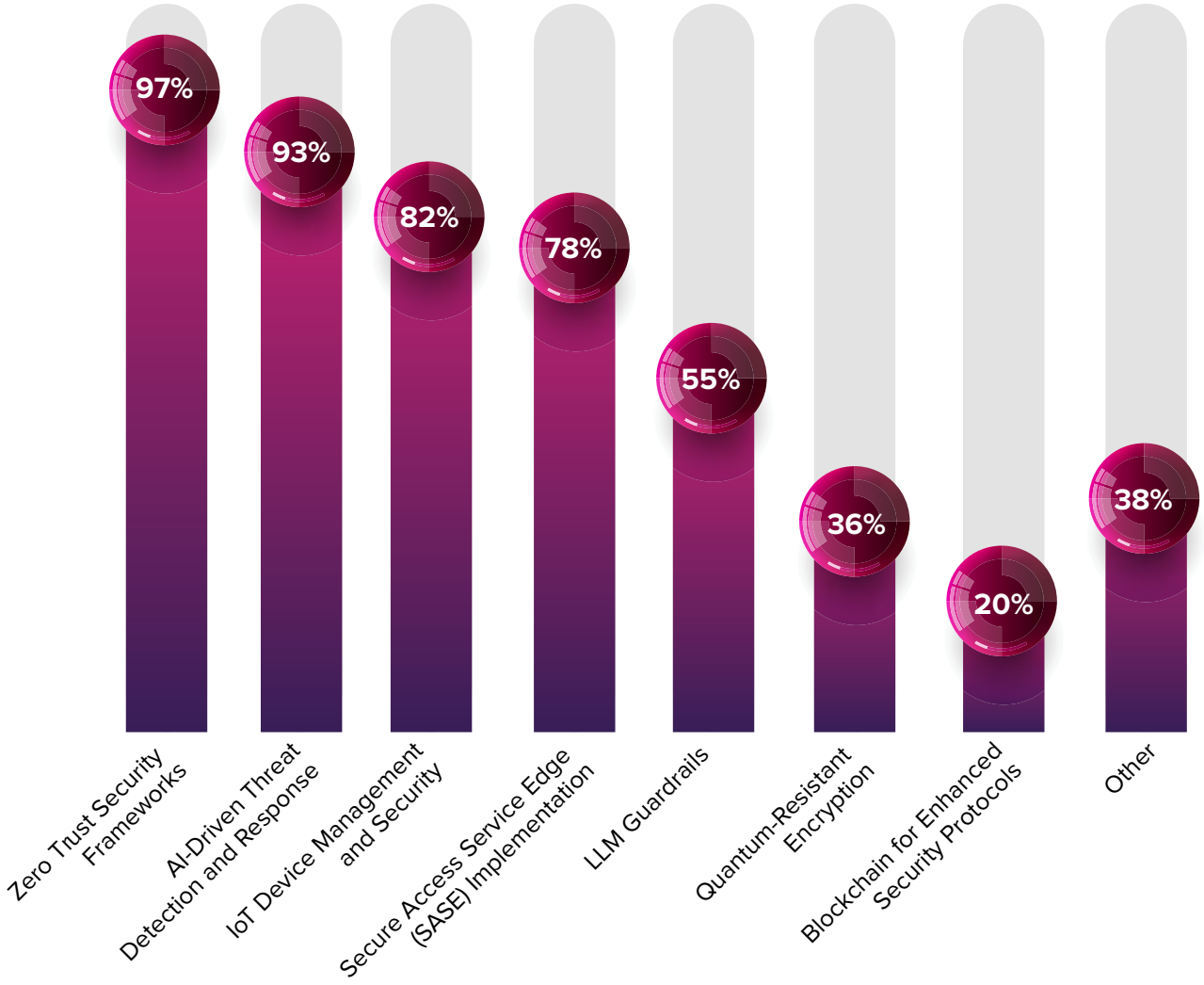


Figure 13: Security Investment Priorities

Technology Priorities

As overall IT budgets diminish, organizations are looking for ways to optimize costs in their cybersecurity technology investments by prioritizing key areas.

According to the latest survey, 30% of respondents are investing in AI automation to enhance their cybersecurity operations. AI-driven automation can help in detecting and responding to threats more quickly and accurately, thereby reducing the need for extensive manual intervention. 26% of respondents are focusing on tools rationalization. This approach involves evaluating and consolidating duplicate security tools across platforms to eliminate redundancies and improve efficiency while reducing costs.

Another significant area is security and risk management process optimization, with 23% of organizations targeting this for cost savings. Streamlining these processes can lead to more effective risk management and better allocation of resources. Apart from these priorities, 20% are focusing on simplifying operating models to achieve better visibility and faster response across reduced attack surfaces.

30% of organizations are investing in AI automation to enhance their cybersecurity operations in an effort to reduce costs.

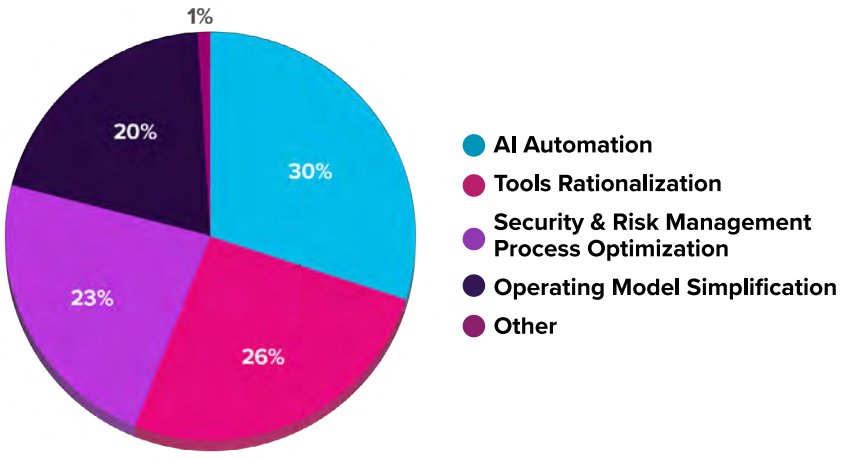


Figure 14: Top Technology Priorities

Future SOC Evolution

The Security Operations Center (SOC) serves as the nerve center for an enterprise's cybersecurity efforts, continuously monitoring and analyzing the digital landscape to thwart cyber threats. Many modern SOCs operate on a global scale, utilizing a round-the-clock approach with teams across different time zones working collaboratively on a unified technology platform. A well-functioning SOC requires a balanced mix of security operations, engineering automation across detection and response, contextual threat intelligence, proactive threat hunting, and effective incident response.

Our latest survey data suggest the priorities for SOCs have shifted. Respondents identified enhanced security process automation as their top priority while choosing leverage of GenAI in SOC use cases as priority number two. This reflects a growing reliance on automation to streamline security operations, improve efficiency and reduce costs.

Figure 15 shows the weighted average of seven SOC priorities ranked on a scale of 7, with 7 being the highest priority and 1 being the lowest.

27% of respondents identified enhanced automation of security processes as their top SOC priority for improving efficiency and reducing costs.

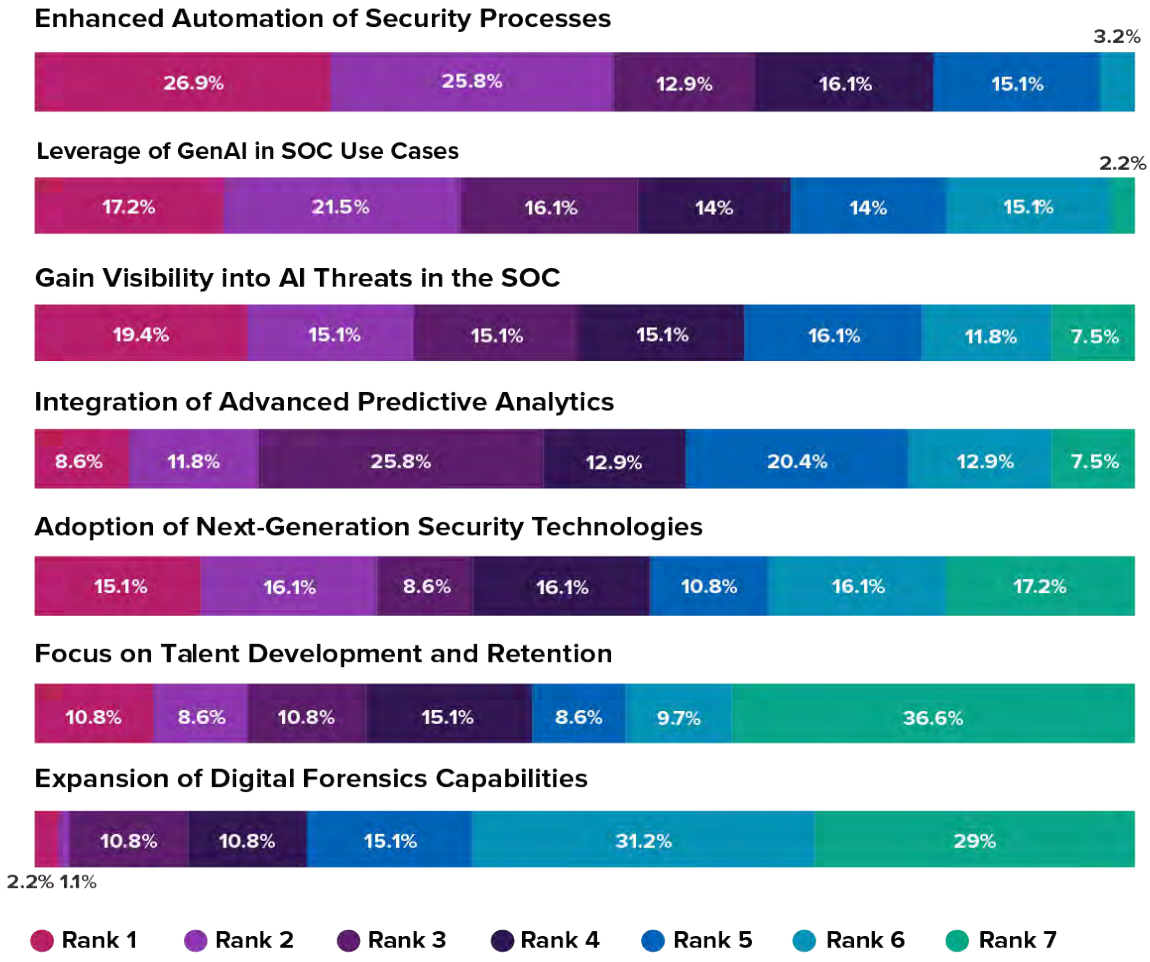


Figure 15: Top Priorities for the Future SOC

State of AI in Cyber

AI adoption challenges

AI adoption for cybersecurity teams has been challenging. Four prominent obstacles cited by respondents in our latest survey include:

1. Data quality and privacy: Effective AI models require high-quality and well represented data. Inaccurate, unverified and incomplete data compromise the detection capabilities, or worse, increase the rate of false positives. Additionally, handling sensitive cybersecurity data raises the risk of compliance non-adherence under cybersecurity regulations like GDPR, HIPAA and other regulatory frameworks which complicates data governance. AI-specific regulations entering an already complex and evolving regulatory landscape further increase AI-adoption challenges for security teams. 84% of respondents cited data quality and privacy as the biggest challenge in implementing effective AI-driven cybersecurity solutions.

2. Lack of AI expertise: AI adoption requires specialized skills such as the development of machine learning algorithms and implementation of LLMs with robust cybersecurity measures to ensure that the output is genuine and devoid of bias. Many organizations lack in-house expertise, forcing them to depend on external resources or costly upskilling efforts, which can slow down the pace of AI adoption. Lack of expertise was a challenge for 75% of survey respondents.

3. Integration with existing systems: AI-driven tools must integrate seamlessly with the legacy security infrastructure, including SIEMs, IDs, and firewalls to ensure a smooth transition. Compatibility with current systems can take time to implement. 72% of respondents listed integration with legacy systems as a prominent challenge.

4. Budgetary constraints: AI solutions require significant investments in various hardware components and software licenses, along with continuous system monitoring and maintenance. Budget was an obstacle cited by 69% of respondents.

AI-driven cybersecurity solutions offer unprecedented capabilities. But addressing these key challenges is essential for implementing a robust and resilient AI-enhanced security strategy.

Figure 16: Challenges in Implementing AI-Driven Security Solutions

84%

Data quality and privacy concerns

75%

Lack of AI expertise within the team

72%

Integration with existing security infrastructure

69%

Budgetary constraints

84% of respondents stated that data quality and privacy pose the biggest challenge in implementing effective AI-driven cybersecurity solutions.

AI adoption benefits

The integration of AI into cybersecurity has the potential to significantly change how organizations detect, prevent and respond to cyber threats and dramatically enhance their security posture. As shown in Figure 17, our research uncovered the top four benefits that organizations could expect to achieve from leveraging AI in cyber use cases.

1. **Increased efficiency in security operations (33%):** AI can help automate routine security tasks, such as log analysis and triaging, freeing up SOC analysts for more complex tasks and critical decision making. Automation in operations significantly reduces manual workloads and intervention for routine tasks, reduces errors, and enhances the overall efficiency of security operations.

2. **Improved threat detection and response times (31%):** AI-enabled agents can be implemented over existing security solutions and reduce the time required to analyze vast amounts of data in real-time. AI agents can detect anomalies and patterns that identify potential threats and identify potential cybersecurity blind spots. This proactive approach enables faster detection and response to both known and unknown attack vectors.

3. **Enhanced incident response capabilities (24%):** By integrating AI with security orchestration, automation, and response (SOAR) platforms, organizations can streamline workflows, improve response speed and effectiveness during critical security incidents, support remediation efforts and mitigate cyberattack damage.

4. **Staffing and training optimizations (12%):** AI agent systems can scale without requiring proportional increases in personnel and resources. Additionally, AI agents developed for security processes can assist in training by simulating threats and providing real-time insights. This can help to build skills development and incident response playbooks.

Figure 17: Benefits of Integrating AI in Cybersecurity

AI implementation responsibility

A majority of survey respondents agree that the secure and responsible implementation of AI systems is a shared responsibility that involves multiple key stakeholders and integration across four distinct units, as shown in Figure 18, and by forming AI Councils. A collaborative approach ensures that AI technologies are deployed seamlessly, safely and in compliance with both regulatory and ethical standards.

58% of survey respondents agree that the secure and responsible implementation of AI systems is a shared responsibility that involves multiple key stakeholders within an organization.

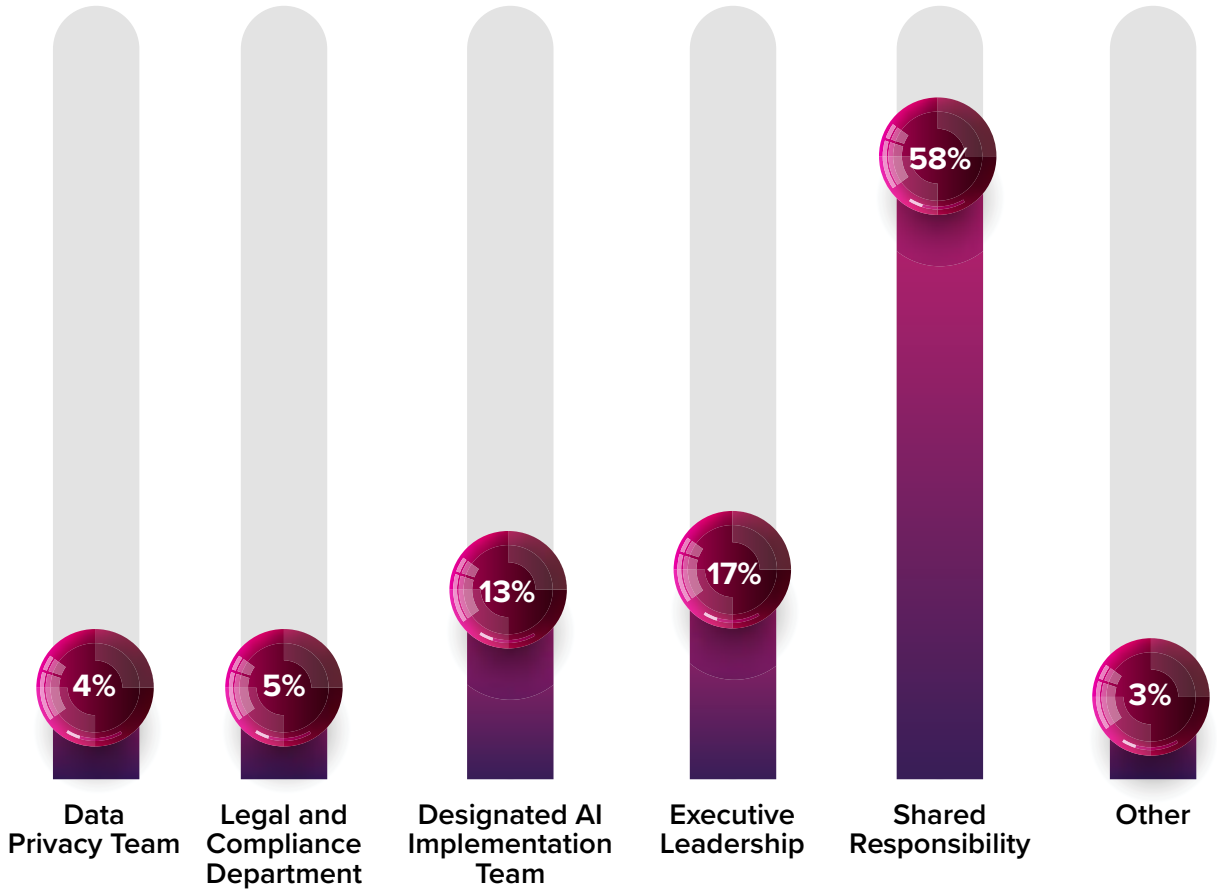


Figure 18: Stakeholders Responsible for Ethical AI Implementation

1. **Executive leadership (17%):** Senior leaders set the vision for responsible and ethical AI development, ensuring that AI initiatives align with the organization's values and strategic long-term goals. They also make risk management decisions that can impact public trust and the organization's brand image among various stakeholders.

2. **Designated AI implementation team (13%):** A designated team of AI specialists and data scientists focuses on the technical design, development, and deployment of responsible AI systems that are secure and bias free while adhering to ethical principles and technical best practices. The team also designs the AI incident response and triaging playbooks.

3. **Legal and compliance department (5%):** This team ensures that AI systems comply with rapidly evolving laws and regulations, such as data protection (GDPR, HIPAA, etc.), AI regulation (EU AI Act, etc.), and industry-specific regulations. Their oversight is crucial to mitigate legal risks and ensure the ethical use of AI technologies.

4. **Data privacy team (4%):** AI systems rely heavily on data making privacy a key concern. The data privacy team ensures that the collection, storage, and usage of data comply with privacy laws and that individuals' data rights are respected throughout the entire AI lifecycle. They work closely with the legal department and AI implementation team to enforce data governance and compliance.

Failure to adopt responsible AI can result in biased outcomes, privacy violations, regulatory penalties, and loss of public confidence. A collaborative AI implementation approach across the organization ensures that AI systems drive innovation and operate within a framework of trust, transparency and compliance.

The business risks of deepfakes

Deepfakes are AI-generated synthetic images, videos, or audio which mimic real people. They pose enormous risks to real-time communications processes and messaging for businesses and can lead to significant financial and reputational impact. Survey respondents assessed and highlighted the negative impacts of deepfake technology across the following four major business risk areas:

1. **Market manipulation:** Deepfake videos of company executives making misleading statement can cause financial impacts by spreading misinformation, manipulating stock prices and inducing panic among investors. For example, a deepfake of a CEO announcing a false bankruptcy could cause the company's stock value to plunge.

2. **Operational disruption:** Deepfakes can be employed to impersonate key personnel in communication channels, causing disruptions by issuing fake directives or accessing sensitive systems that can affect BAU activities.

3. **Reputational damage:** A deepfake scandal involving an important person associated with an organization can tarnish its reputation, erode trust, and alienate customers. Even after proper clarifications, reputational damage is hard to reverse. In many cases it can create lasting impacts and in some extreme cases a full recovery is never achieved.

4. **Financial Loss:** Fraudsters can use deepfakes in spear-phishing attacks, impersonating executives to authorize fraudulent transactions or influence business decisions resulting in financial losses.

As shown in Figure 19, survey respondents identified damage to brand reputation as the most adverse effect of deepfakes, followed by financial loss, operational disruption and market manipulation.

These findings highlight the multi-faceted threats posed by deepfakes, emphasizing the need for comprehensive strategies to mitigate the risks.

Figure 19: Impacts of Deepfakes on Businesses

Impacts were scored on a scale of 4 (4 being the worst impact and 1 being the least)

AI in cybersecurity is a double-edged sword. It can enhance both cyber defense and cyberattack mechanisms. AI is being used to accelerate the effectiveness of cybersecurity processes, which, in turn, helps to reduce risks and costs. But on the other side, threat actors are utilizing AI to increase the effectiveness of their attacks so that they can more easily penetrate and avoid defensive measures. Organizations must stay on top of rapidly evolving AI innovations — on both sides of the sword — and implement the latest best practices in a responsible, secure, and cost-effective manner.

FUTURE OF CYBERSECURITY

Cyber Patent Trends

The cybersecurity field is evolving at a rapid pace, driven by advancing technologies, increasing sophistication of cyber threats and a growing regulatory focus. As organizations grapple with the challenges of protecting their digital assets, there is a heightened need to focus on innovative solutions and strategic investments. Examining key trends in cyber patent submission and investments helps to identify the areas of cybersecurity that are likely to experience significant growth and innovation in the coming years.

Research scope

This research focused on nine cybersecurity practice areas, including Data Security, Application Security, Network Security, Cloud Security, and Endpoint Security, among others. We analyzed patents submitted from 2019 onwards till mid July 2024 across all geographies, with a specific focus on 25 countries and the following 10 emerging technologies:

- Artificial Intelligence/Machine Learning (AI/ML)
- Generative AI
- Blockchain
- Edge Computing
- 5G and 6G
- Quantum Computing
- Digital Twin
- Robotics
- Mixed Reality
- Software-Defined Vehicle

Cybersecurity patent submissions

Since 2019, nearly 46,000 patent families (technology inventions) related to cybersecurity have been submitted, highlighting the growing intersection of cybersecurity practice areas and emerging technologies. Each year, there has been an upward trend in patent submissions, indicating increased cybersecurity research, technological advancement and adoption. It's important to note that data for 2023 and 2024 is incomplete due to the time lag in patent publication, so the actual numbers for these years are expected to be higher. As a result, the aggregated patent submission figures for 2020, 2021 and 2022 may surpass those reported in previous SOCR editions.

Our data indicates that China currently leads in the total number of patents filed, with over 37,000 submissions. The U.S. follows with more than 8,000 patents filed. Notably, only 4.7% of Chinese patent families were filed in the U.S. and other international jurisdictions, which indicates that most Chinese patents are primarily domestic and lack protection outside of China.

Many of the patents filed by China and the U.S. focus on the same functional and technology domains — Data Security, Device Security, and Network Security. Similarly, most U.S. and China patents are utilizing emerging technologies like AI/ML, Blockchain, Edge Computing, and 5G/6G.

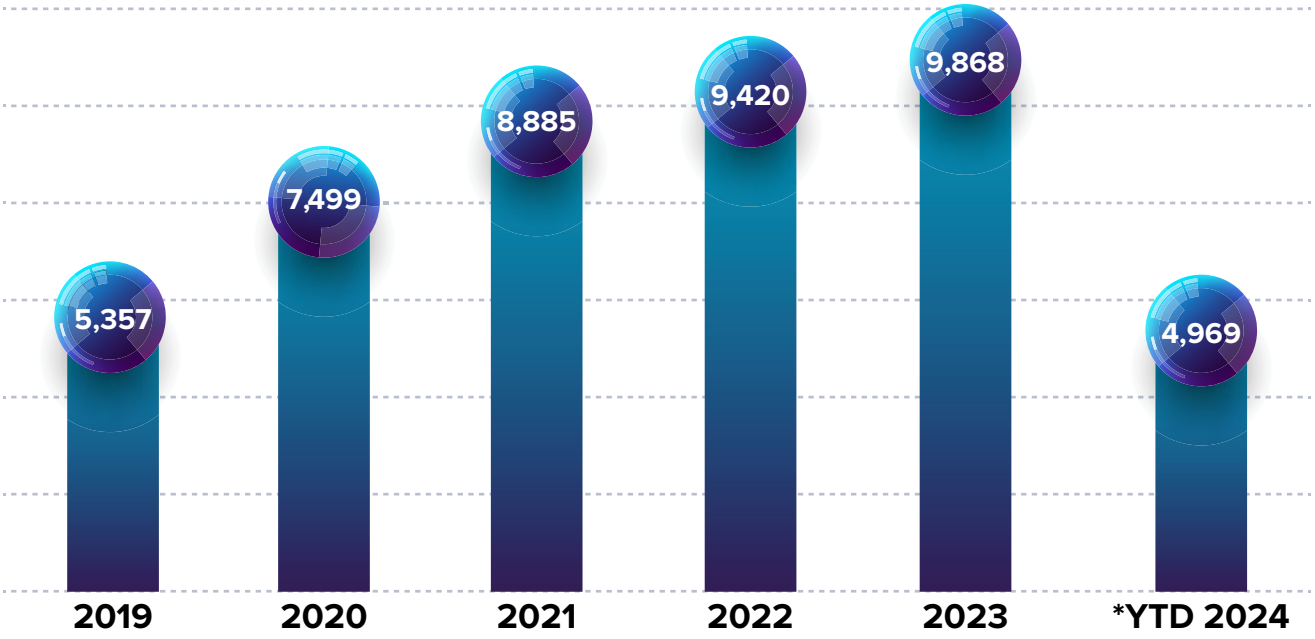
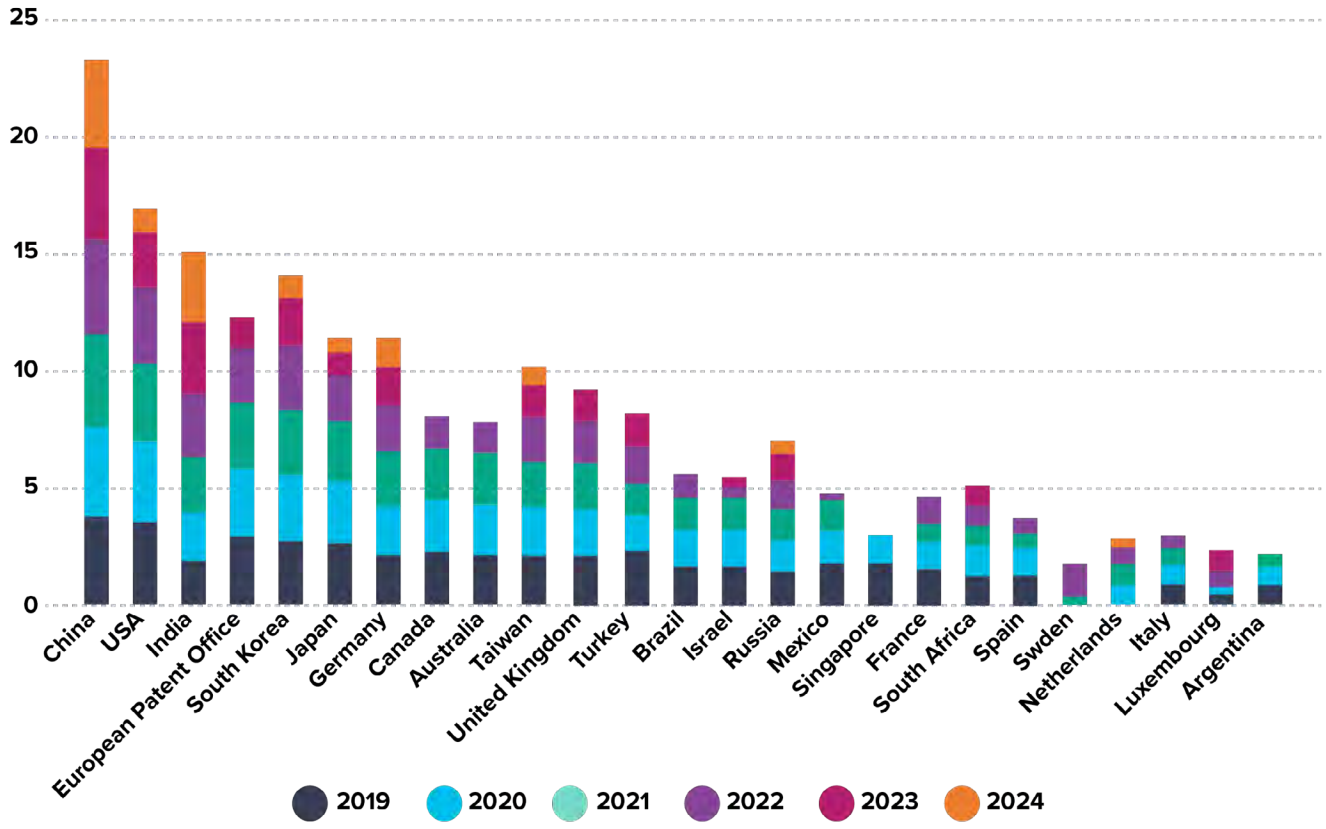


Figure 20: Cybersecurity Patent Submissions by Year

Despite China leading in overall patent submissions, only 4.7% of Chinese patent families were filed in international jurisdictions. This indicates that most Chinese patents are primarily domestic and lack protection outside of China.



The table below shows patent data through 15 July 2024

	China	USA	India	European Patent Office	South Korea	Japan	Germany	Canada	Australia	Taiwan	United Kingdom	Turkey	Brazil	Israel	Russia	Mexico	Singapore	France	South Africa	Spain	Swden	Netherlands	Italy	Luxembourg	Argentina
2019	4128	2783	62	695	478	390	120	158	117	106	100	12	44	35	24	51	55	33	18	18	1	1	4	3	7
2020	6027	2311	119	699	541	365	106	151	121	114	99	15	35	42	21	23	14	12	17	13	0	7	7	2	6
2021	7198	1808	192	628	528	296	184	146	158	79	92	34	21	20	20	18	0	6	7	4	2	8	10	0	3
2022	7404	1276	427	157	362	94	89	20	18	72	47	18	8	3	15	2	0	13	7	0	24	5	3	4	1
2023	8301	263	957	19	116	8	34	0	0	23	17	37	1	2	14	0	0	1	6	4	0	1	0	7	0
2024	3980	8	844	0	8	3	17	0	0	5	0	23	0	0	3	0	0	0	0	0	0	2	0	1	0

Figure 21: Cybersecurity Patent Count on a Logarithmic Scale by Geography

Key tech radar areas

Our research mapped patent submission activities within the cybersecurity tech radar areas that include new technologies such as Homomorphic Encryption, Differential Privacy, Ring Signature and Decentralized Identity.

Tech radar also includes additional emerging technologies where cybersecurity plays an important role, such as Private 5G and AI Chips.

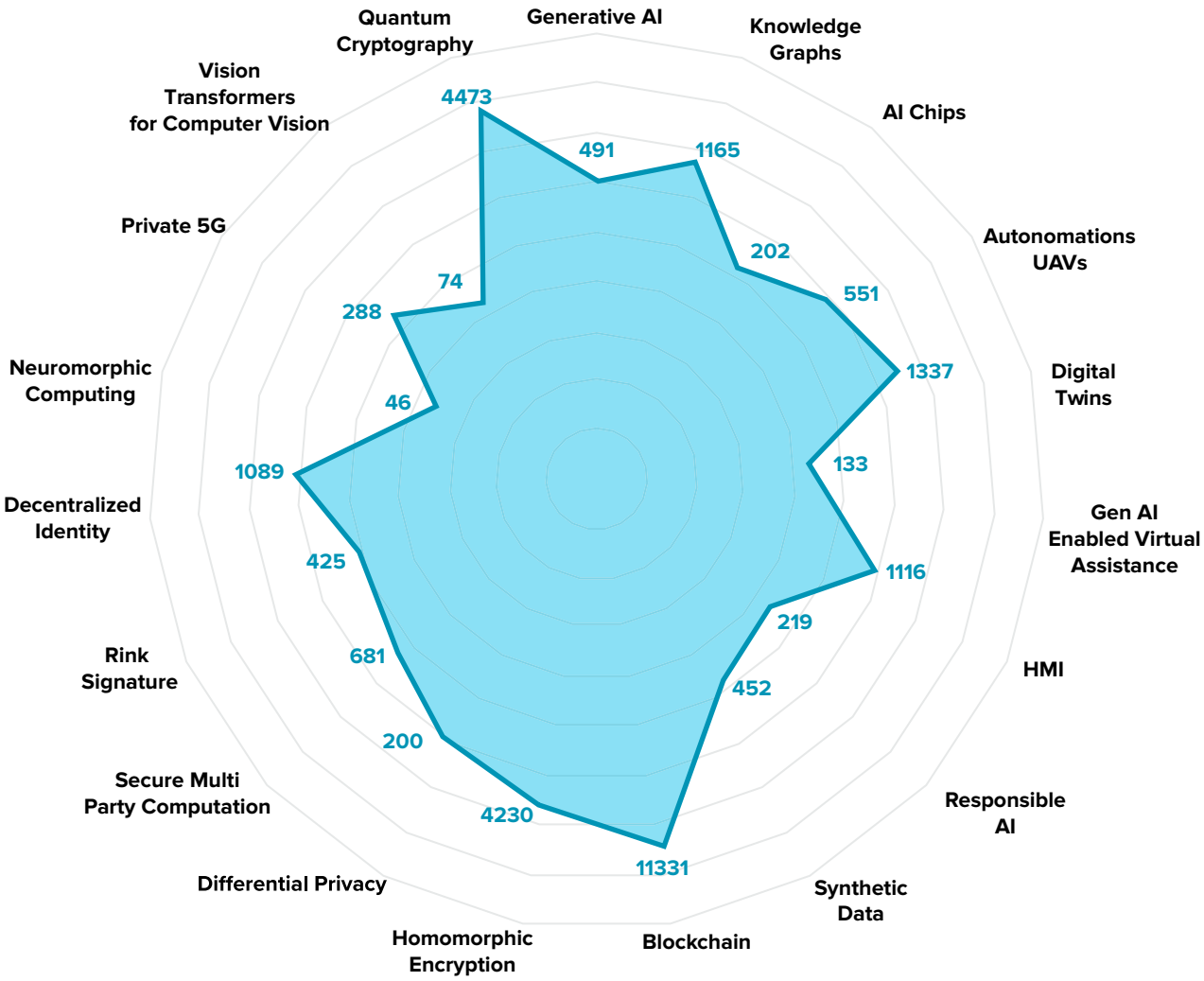


Figure 22: Cybersecurity Patent Tech Radar

Figure 22 shows that Blockchain led the field from 2019 to 2024, with over 11,000 technological inventions. Quantum Cryptography followed with more than 4,400 patent families, and Differential Privacy accounted for 2,000 patent families. The adoption of Quantum Cryptography, Differential Privacy, Digital Twins, Knowledge Graphs and Decentralized Identity significantly contributed to the growth in patent filings. Other areas have experienced more modest growth, while newer technologies like Generative AI, AI Chips, Responsible AI, and Synthetic Data are beginning to gain momentum.

It is noteworthy that Blockchain and Quantum Cryptography are leading this analysis. These technologies can adapt to significant architectural shifts in modern IT so it is essential for CISOs to closely monitor them.

AI/ML, Blockchain and Edge Computing, three of the most disruptive technologies to emerge in recent years, are set to have a significant impact in the future. Other key contenders include 5G and 6G, Robotics and Digital Twin. Figure 23 breaks down patent filings across these and other core practice areas.

The top three domains for new cyber patents since 2019 are Blockchain, Quantum Cryptography and Homomorphic Encryption.

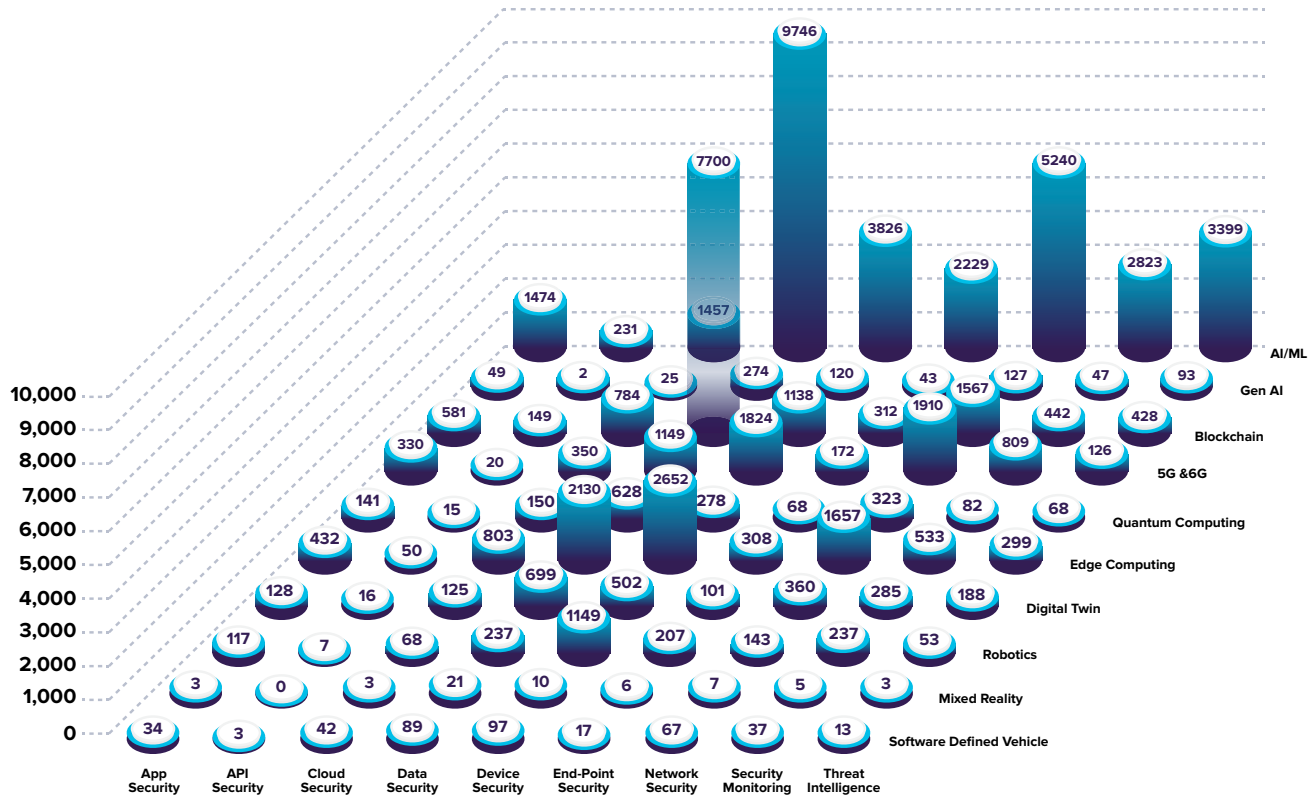


Figure 23:
Patents in the Cross-Section of Cybersecurity Practice Areas and Emerging Technologies

SPOTLIGHT:

Cyber Investment and Funding Trends

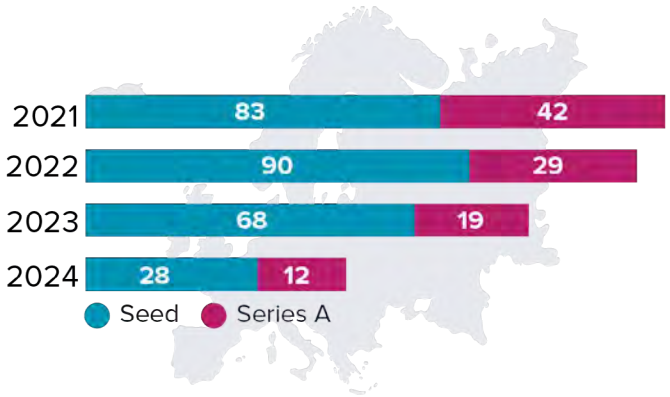
We explored current global cybersecurity startup investment trends collaboration with Pitchbook (www.pitchbook.com). The research examined the investment trends across geographies and cybersecurity areas over the last four years (2021 - Mid August 2024). These trends allow cybersecurity professionals to gain insights into the future of cybersecurity and potential opportunities for leveraging upcoming innovations and investments.

Cyber investment trends highlights

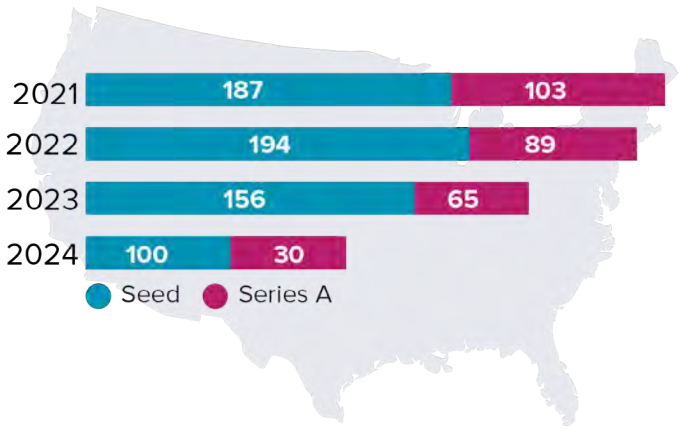
- There was a significant uptick in financing activity in 2021 and early 2022 before markets corrected in 2H 2022. Both deal count and dollars invested have dropped significantly since 2H 2022, however they are trending upwards in 2024.
- The total number of cybersecurity deals dropped from approximately 600 in 2021 and 2022 to 429 in 2023 and 230 through August 2024. Dollars invested were $4B in 2021, $4.6B in 2022, $3.1B in 2023 and $1.7B through August 2024.
- The U.S., Europe and Israel remained the primary geographies for cybersecurity startups.
- The percentage of seed deals in subsequent Series A rounds year over year went down — from 45% in 2022 to 30% in 2023 — and are on track to remain at a similar level in 2024.
- Cybersecurity product players have been undertaking bolt-on acquisitions as a way to build their platformization strategy.
- Innovation in emerging companies continues to be in niche areas considered 'features' rather than 'standalone products,' driving market consolidation as product strategies take advantage of the fragmented segments and their distribution capabilities.
- Enterprises that provide technology consulting and services primarily acquired companies in the Security Consulting/MSSP category in different geographies to expand their presence.
- Among product players, the categories that saw the greatest number of acquisitions were SecOps/Threat Intel/Incident Response, Cloud Security and Data Security.
- Solutions aggregating data from the security stack and providing enhanced context and insights with GenAI are helping security teams reduce MTTR. Cloud security solutions spanning multi-cloud environments have driven acquisitions of startups offering relevant cloud security capabilities.
- We expect security market consolidation to continue throughout 2024 and beyond as large players take advantage of emerging and fragmented security segments, such as AI security, and continue to supplement growth through acquisitions.

Figure 24 shows the number of significant venture investment deals in seed and series A stages across different geographic areas.

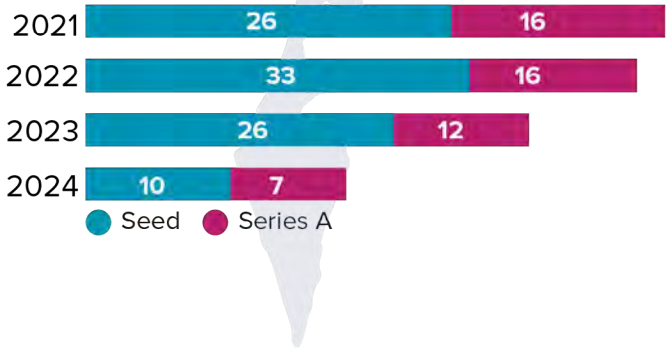
Europe				
Year	2024	2023	2022	2021
Seed	28	68	90	83
Series A	12	19	29	42



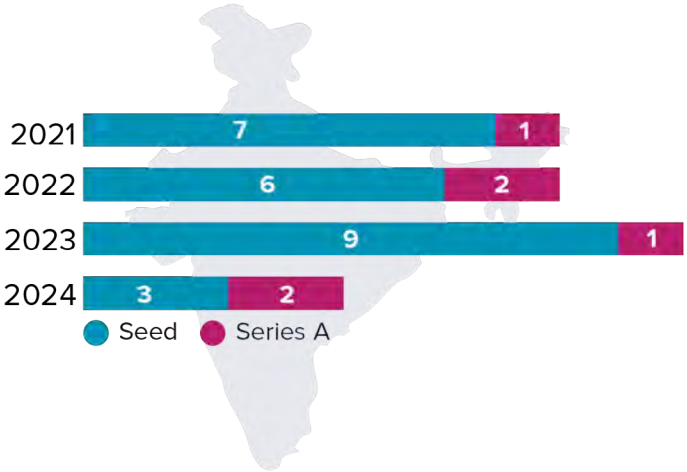
United States				
Year	2024	2023	2022	2021
Seed	100	156	194	187
Series A	30	65	89	103



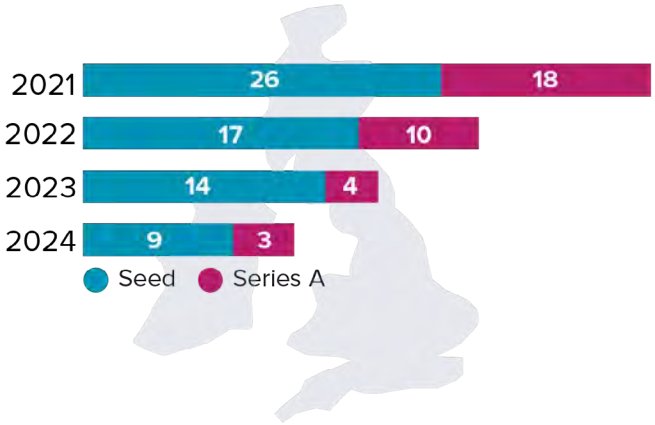
Israel				
Year	2024	2023	2022	2021
Seed	10	26	33	26
Series A	7	12	16	16



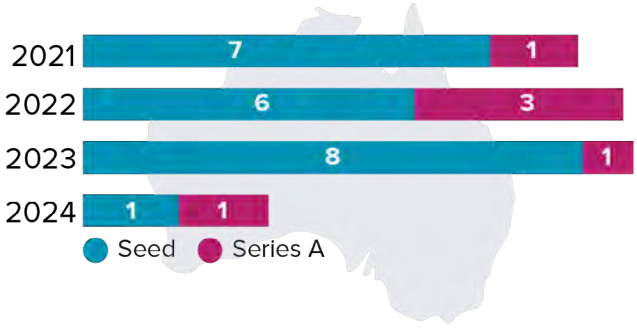
India				
Year	2024	2023	2022	2021
Seed	3	9	6	7
Series A	2	1	2	1



United Kingdom				
Year	2024	2023	2022	2021
Seed	9	14	17	26
Series A	3	4	10	18



Australia				
Year	2024	2023	2022	2021
Seed	1	8	6	7
Series A	1	1	3	1



Rest of the World				
Year	2024	2023	2022	2021
Seed	28	68	90	83
Series A	12	19	29	42

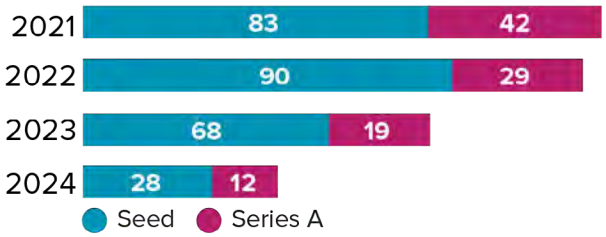


Figure 24:
Venture Investment Deals by Geography
* The data for 2024 is through mid-August.

Category trends

Overall, cybersecurity funding activity levels have declined compared to the higher levels in 2021 and 2022. Within this environment of declining growth in financing deals, SecOps, Security Consulting (including GRC), AI/ML/GenAI Security, Fraud and Transaction Security, and Identity and Access Management declined less than many other areas, indicating that enterprises still consider these categories important.

In contrast, some of the categories that saw significant declines in growth include IoT/OT Security, Data Security, Endpoint Security, Application Security, and Cloud Security. This may indicate a certain level of maturity for these areas.

- **Security Operations / Threat Intelligence / Incident Response**
  Intelligence and incident response enterprise security teams are being inundated with cyber alerts. Many emerging companies are adopting the 'Security Data Fabric' approach that aggregates data from all enterprise security tools to gain enhanced context and insights. This helps security teams reduce false positives and lower MTTR, while optimizing their security stack. Enterprises are consolidating budgets and allocating funds toward sectors within attack surface management, including CAASM, Exposure Management, CTEM, PTAS, and ASM, leading to consolidation in the vendor landscape, as well.

- **Identity and Access Management**
  Identity is considered the new perimeter for enterprise security, making it a top priority for CISOs to manage and secure the expanding technology sprawl. As an organization grows, it becomes more difficult to follow rule-based access and governance policies. This has led to innovative solutions that enable automated, just-in-time and ephemeral access for workforce SaaS platforms and cloud infrastructure resources. With the proliferation of cloud and AI agents, securing non-human identities (including workload access) is gaining importance. Startups addressing these problems have received significant investor interest in H2 2023 and 2024.

- **AI/ML/GenAI Security**
  AI is in its infancy, with most enterprises still experimenting with the technology. But it's moving very fast and many organizations are poised to deploy AI solutions in 2025. The landscape of security vendors for AI/GenAI is diverse, with many new startups adopting a platform approach rather than creating a niche product. Current risks being addressed primarily center around sensitive data moving protection, model hallucinations and prompt injections.

- **Security Consulting and GRC**
  Security Consulting and GRC primarily consists of GRC startups with solutions focused on risk quantification, management, compliance and reporting. GRC continues to be of interest for CISOs,especially with increased pressures around potential personal liabilities. CISOs are asking for solutions that can provide a consolidated view of enterprise security, tools and risk posture to maintain transparency and enable management reporting, particularly as AI regulatory compliance is added to the mix.

- **Data Security**
  Although funding activity at the earlier stages has dropped, Data Security, Privacy and Governance continues to be one of the top concerns for CISOs. With the increase in enterprise adoption of GenAI applications, organizations are seeking solutions that ensure security and privacy of sensitive data being exposed to large language models and other GenAI applications. Next-gen data security solutions have emerged that take the AI-first approach to discover and classify sensitive data, enabling run time actions to redact and block sensitive data from leaving the enterprise environment.

> **U.S., Europe and Israel continue to propel cybersecurity startup investments, accounting for 78% of the analyzed deals. The percentage of seed deals in subsequent Series A rounds went down — from 45% in 2022 to 30% in 2023.**

Figure 25 breaks out the percentage distribution of seed deals by all researched practice areas and Figure 26 lists the number of acquisitions in each practice area.

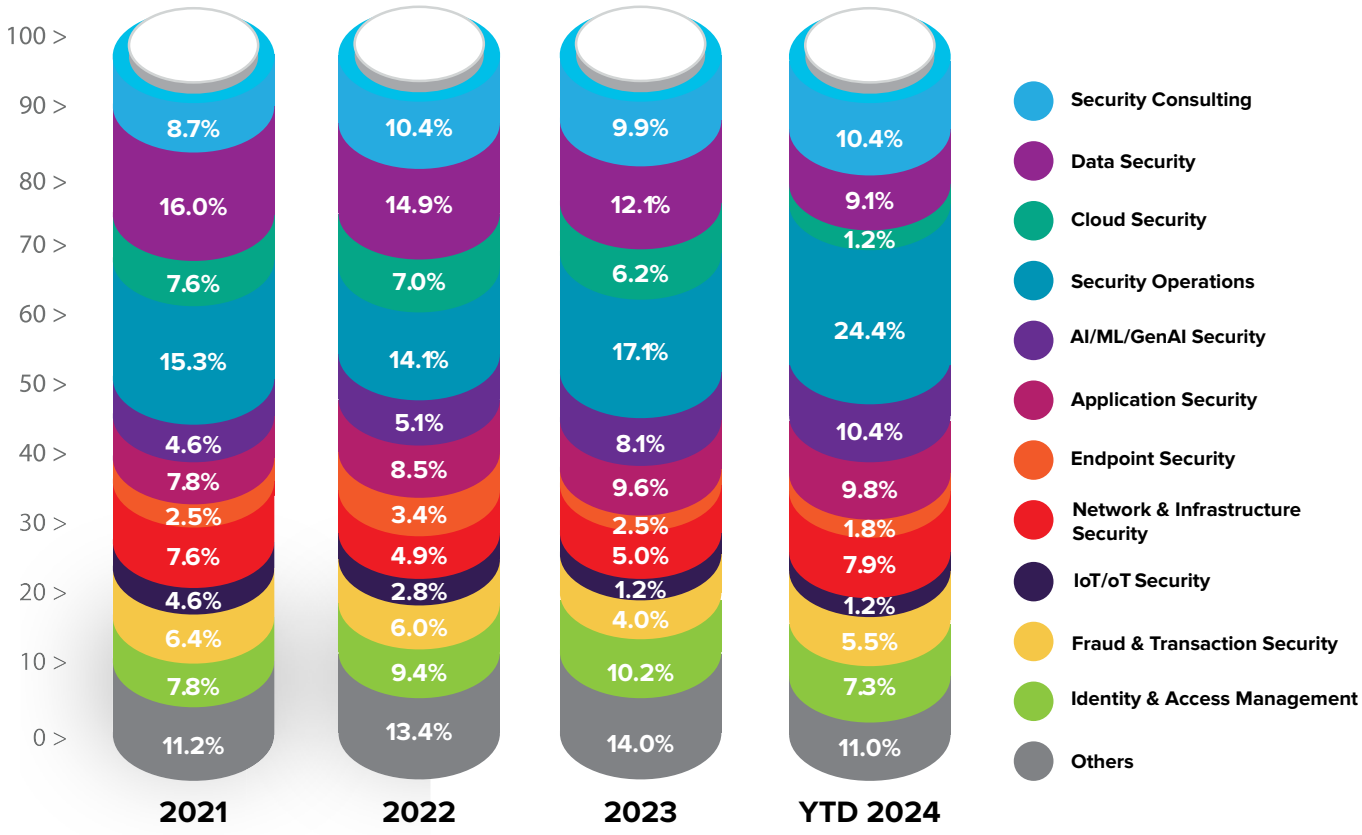


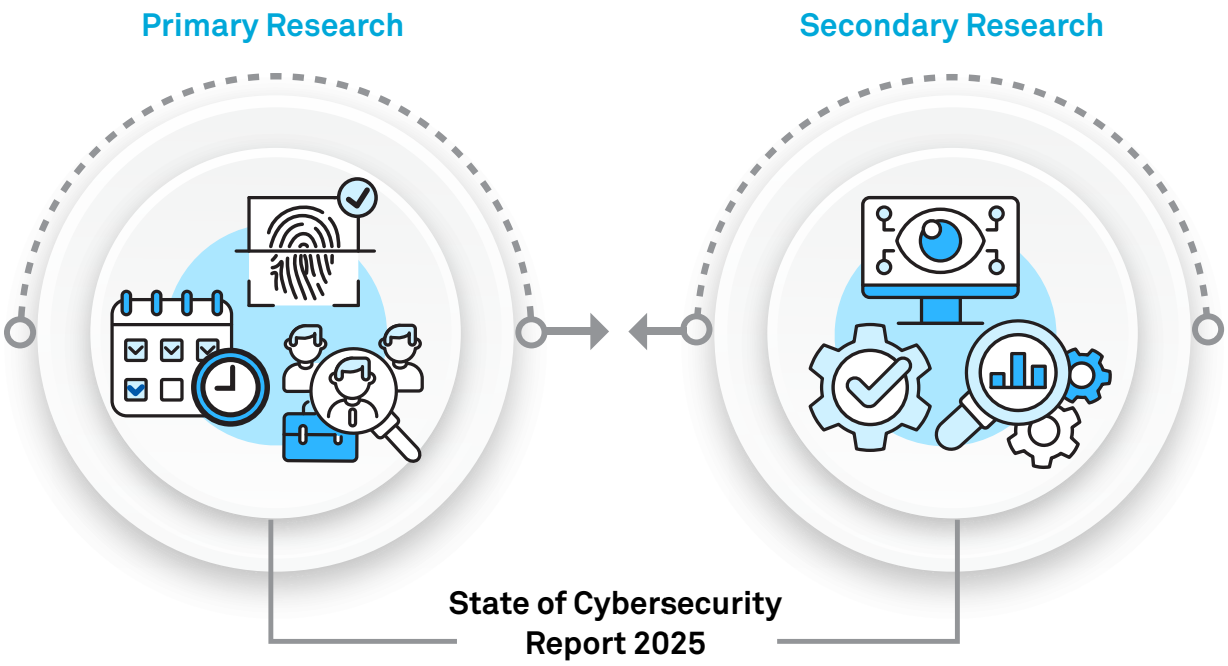
Figure 25:
Distribution of Seed Deals by Category

Practice Area	Number of acquisitions
Security Operations/Threat Intelligence/Incident Response	18
Security Consulting/MSSP	10
OT/IoT Security	1
SaaS Security	2
Email Security	2
Network & Infra Security	9
Application Security	3
Cloud Security	8
Data Security & Governance	6
Endpoint Security	1
Identity & Access Management	2
Others	1
Total	**63**

Figure 26:
Strategic Acquisitions Across Cybersecurity Practice Areas

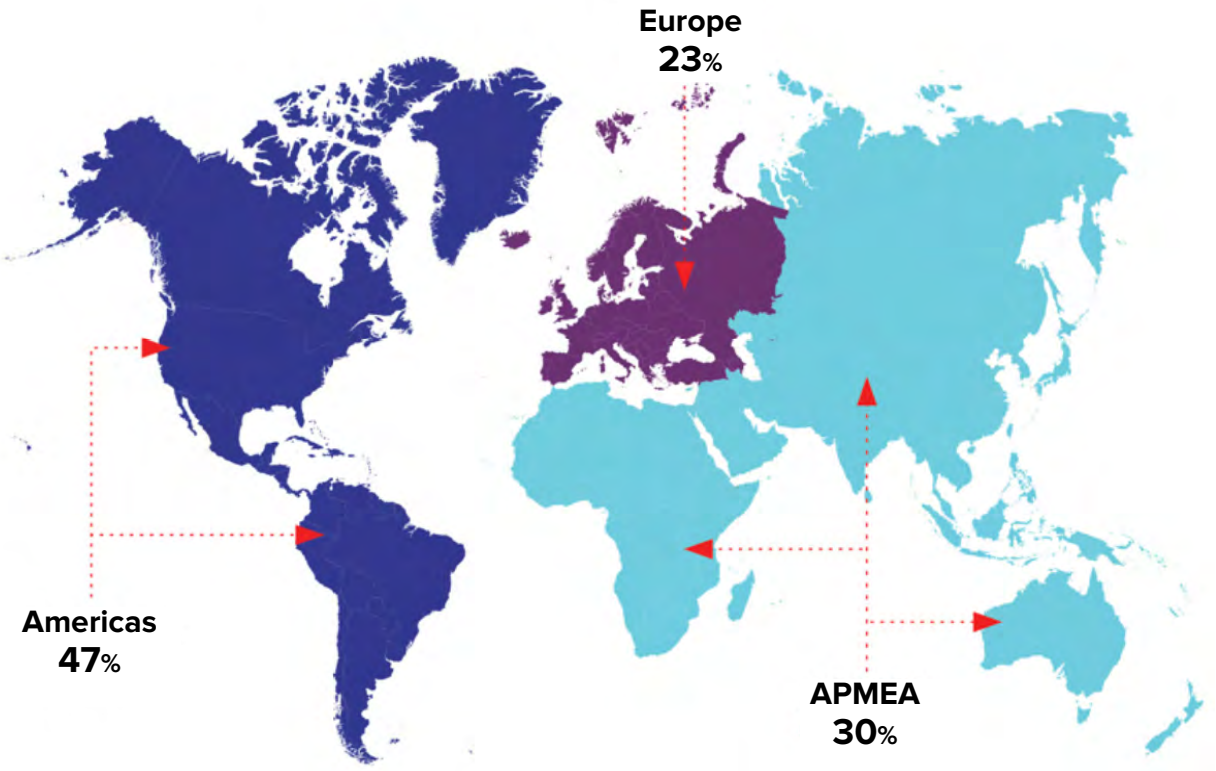
METHODOLOGY & DEMOGRAPHICS

Wipro developed the State of Cybersecurity Report 2025 following a two-pronged approach

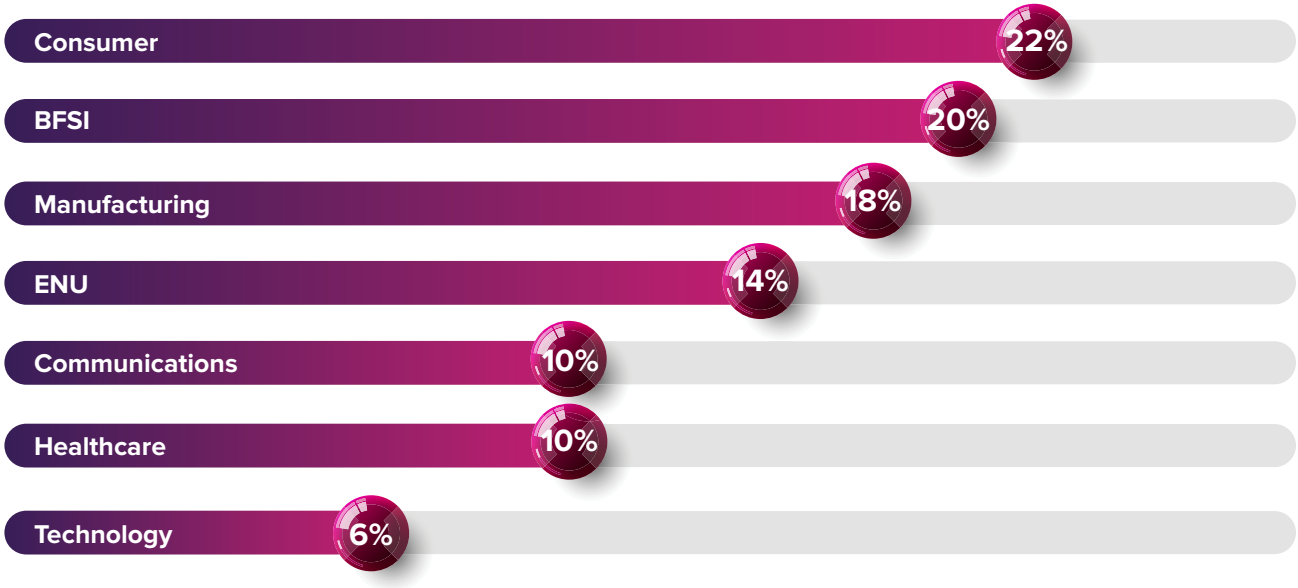


The primary research involved conducting surveys with security leadership and consultants across North America, Europe, the Asia-Pacific, Middle East, and Africa (APMEA) regions. A questionnaire covering cyber governance, security practices, collaboration and best practices was administered over a month. The survey was anonymous, and the responses were processed at an aggregated level to arrive at insights.

The secondary research, carried out by the SOCR core team, involved studying various public databases and research platforms to supplement the primary research and correlate trends in the cybersecurity domain. We collaborated with the Wipro CTO and Lab45 teams to compile a detailed analysis of cyber patent trends around the globe. This year we also presented cybersecurity investment trends analyzed by the Wipro Ventures team in collaboration with PitchBook Data Inc.



Organizations Surveyed: By Vertical



Key Statistics: Making of SOCR 2025

The primary research involved surveying over 100 security leaders and consultants across 21 countries in the North America, Europe, and the Asia-Pacific, Middle East and Africa (APMEA) geographies.

102
Organizations from 21 countries surveyed

244
Cyber venture deals analyzed

580+
Nation-state attacks analyzed

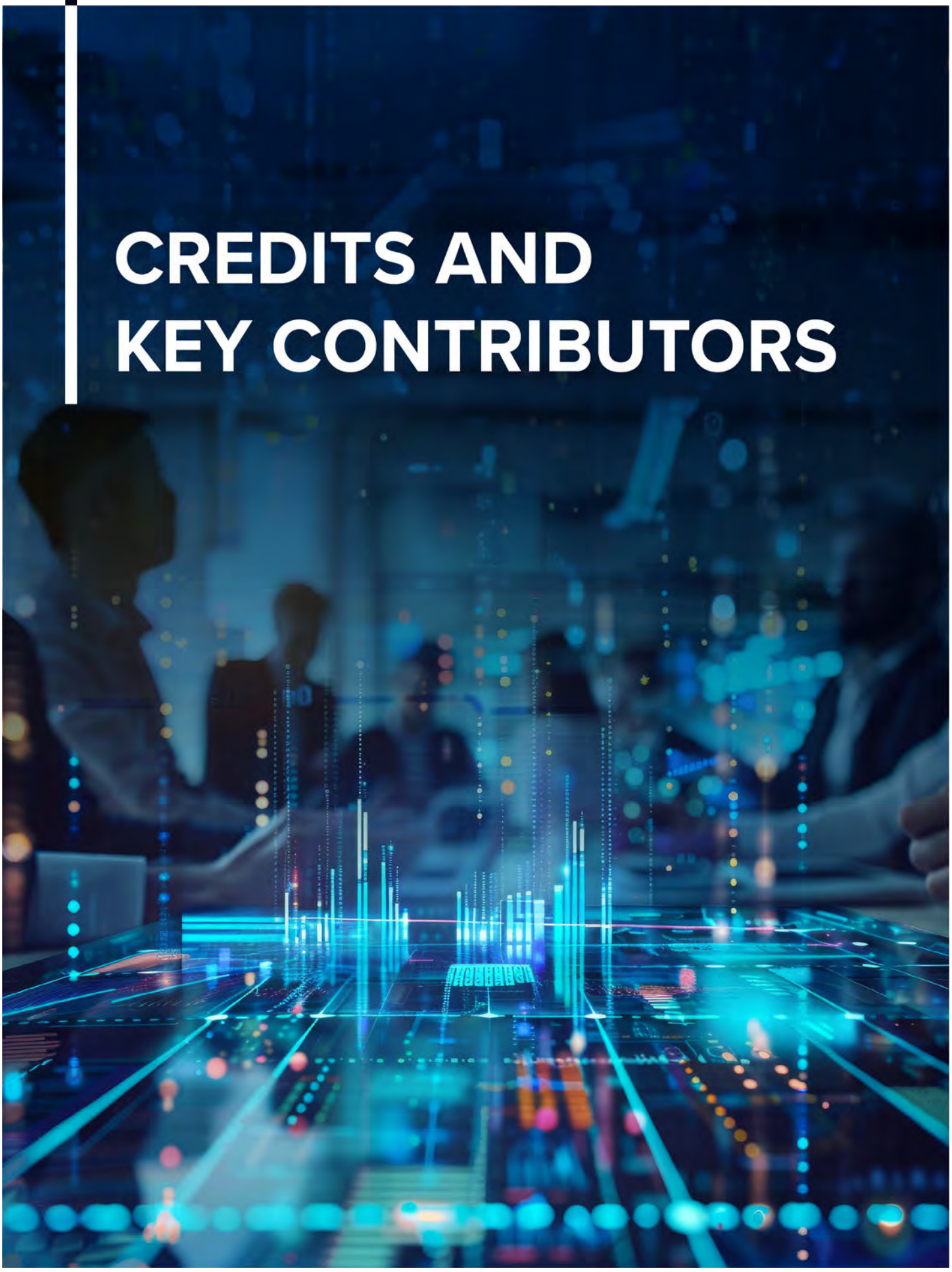
20+
Associated partners

45K+
Patents analyzed globally filed over 5 years

CONTRIBUTING PARTNERS

Associated Partners

CREDITS AND KEY CONTRIBUTORS



Authors:

Josey V George
Chief Editor
General Manager, CRS-GROUP

Core Research, Content and Editorial Team

Moumila Das
Sub-Editor, Senior Consultant, CRS-GROUP

Sayan Sarkar
Practice Consultant, CRS-GROUP

Karthikeyan S
Technical Lead, CRS-GROUP

Aditya Singh
Assistant Manager, Growth Office

Content & Research Inputs

Avneesh Mishra
Principal Consultant, Lab45

Parag Arora
Principal Consultant, Lab45

Bijal Vasant
Senior Manager, Wipro Ventures

Harimohan Rajamohanan
Solution Architect, CRS-GROUP

Concept, Design & Review Team

Dan Seyer
Entity Leader, Growth Office

Prateek Tripathi
Head of Marketing, Growth Office

Sarah Mabry
Design Manager, CRS-GROUP

Sangeeta Thomas
Content Head - Technology Services, Wipro

References:

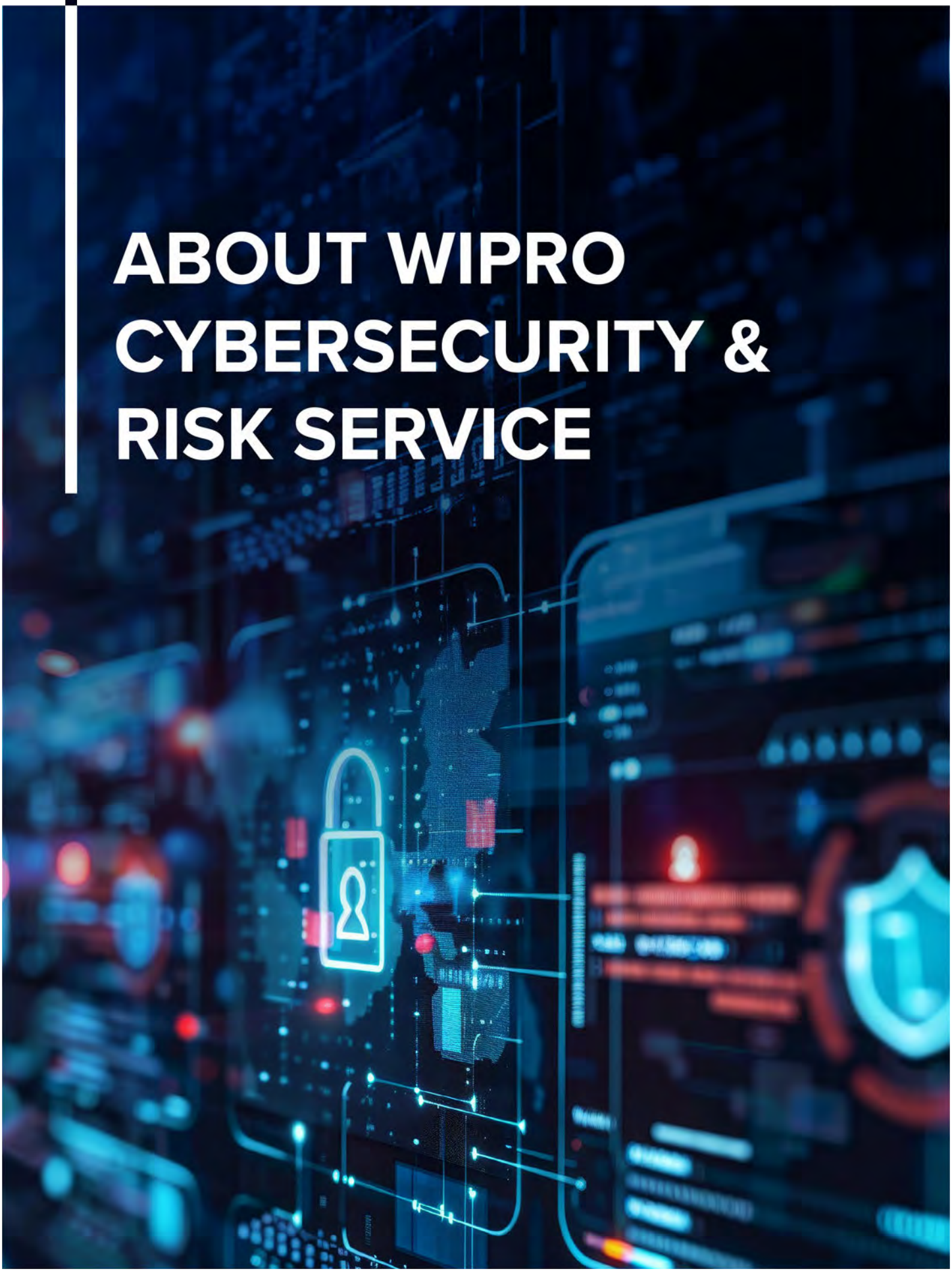
AI Incident Database. (n.d.). Incidents. Retrieved November 20, 2024,
incidentdatabase.ai/apps/incidents/

Center for Strategic and International Studies (2024). Strategic Technologies Program: Significant Cyber Incidents.
csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Council on Foreign Relations (2024, Sep 18). Cyber Operations Tracker.
cfr.org/cyber-operations/

PitchBook. Our Global Data: Deals. Retrieved August 15, 2024,
pitchbook.com/platform-data/deals

ABOUT WIPRO CYBERSECURITY & RISK SERVICE



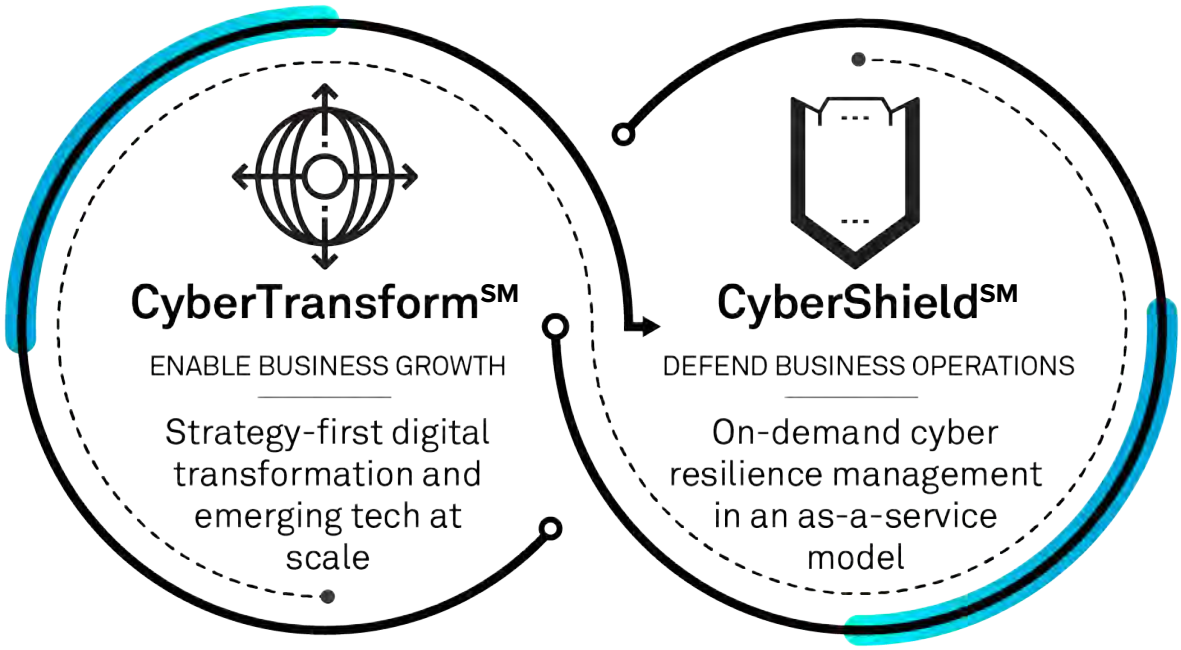
About Wipro

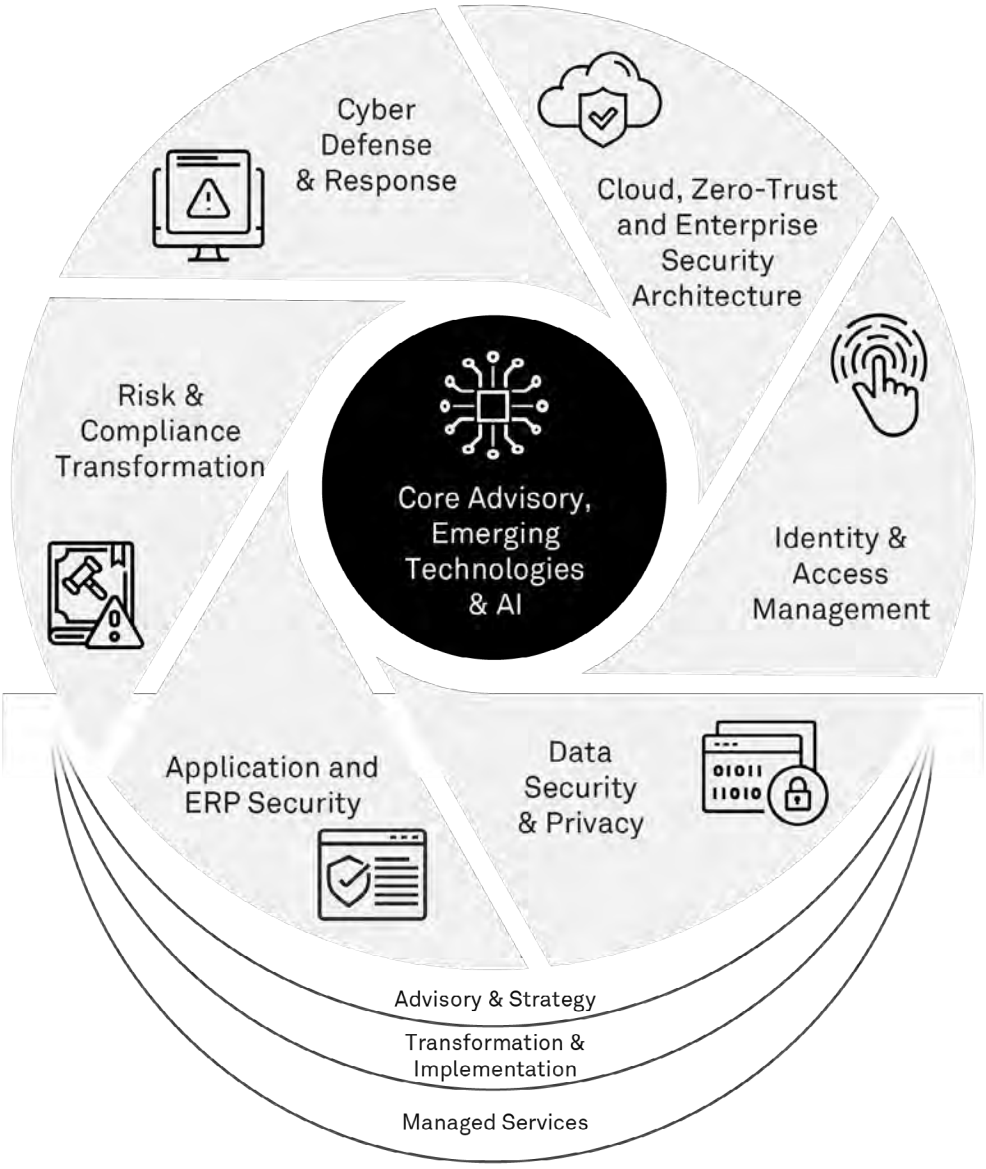
Wipro is a leading cybersecurity consulting firm and the trusted cybersecurity transformation and risk services partner to global enterprises. We secure the modern enterprise by enabling digital transformations that drive operational growth, defend business operations and build future-proof cyber resilience at scale using a strategy-first, business-aligned approach.

Wipro CyberTransform℠ is our suite of modern advisory and implementation services that strengthen security, enhance cyber resilience and enable business growth. Wipro CyberShield℠ Managed Services defend business operations with on-demand cyber resilience management in an as-as-service model.

Recent acquisitions and key investments have enabled us to expand our advisory practice. Wipro Cybersecurity Advisory Services — an integral part of CyberTransform — include plan, build, run capabilities that assess and strengthen cybersecurity posture to safeguard brand reputation, business processes and regulatory compliance with cost-optimized security controls.

Our System Integration and Managed Security Services — part of our CyberShield offerings — enhance cyber resilience across clouds, networks, perimeters, endpoints, identities, data and apps.





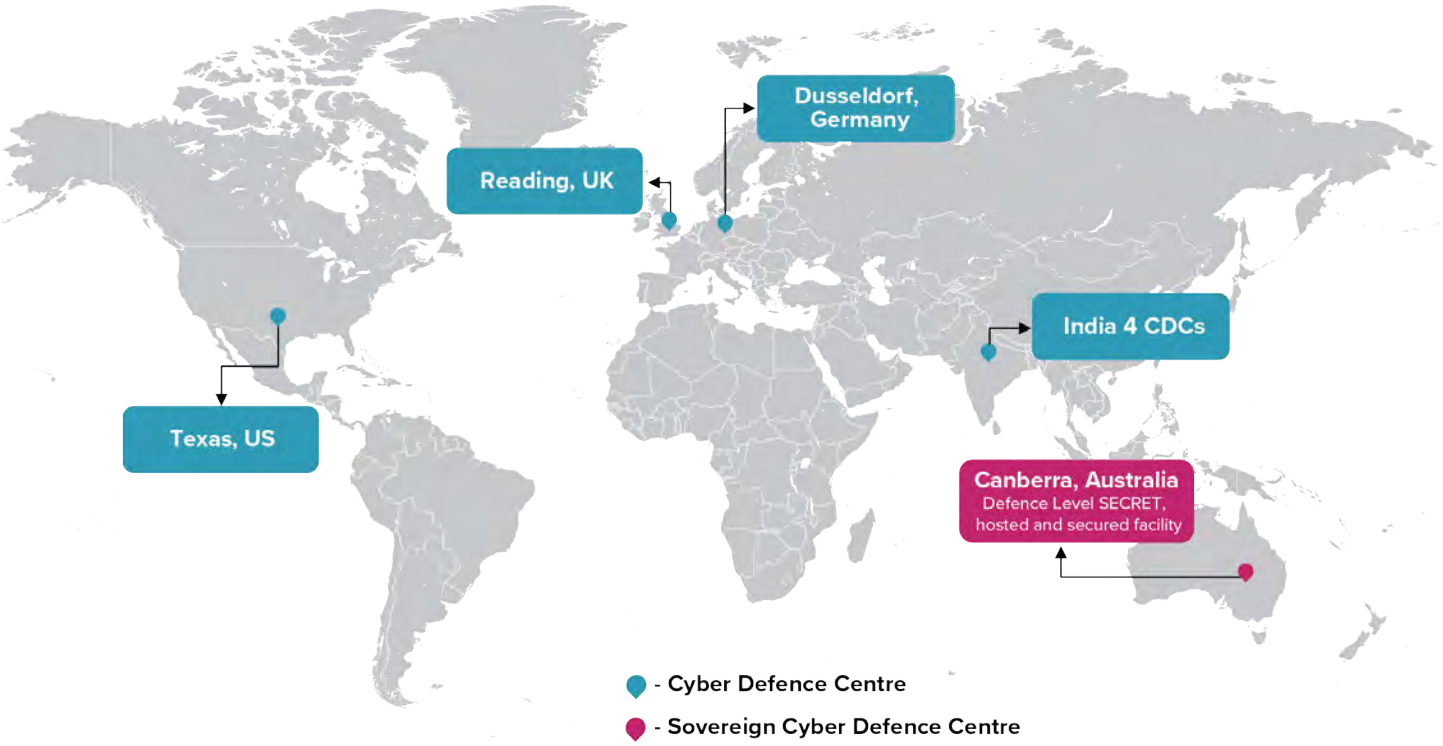
Wipro's strategic advisory and managed services capabilities are overseen by 9,000+ expert Cybersecurists who bring a deep understanding of the evolving risk and compliance challenges facing CXOs in today's environment of continuous disruption.

Our holistic, end-to-end cybersecurity services are delivered across six integrated practice areas:

- **Emerging Technologies and A**I — Leveraging emerging technologies for faster GTM, cost reduction, transparent scalability and automation capabilities.
- **Risk and Compliance Transformation** — Helping organizations implement proactive risk management and continuous regulatory compliance.
- **Cloud, Zero-Trust and Enterprise Security Architecture** — Securing the edge-to-cloud journey against evolving cyber threats with a Zero-Trust approach.
- **Identity and Access Management** — Managing digital identities with next-gen IAM solutions that enable secure, personalized and frictionless user experiences.
- **Data Security and Privacy** — Offering advisory, transformation and managed services for data protection and OT/IoT security to enhance productivity.
- **Cyber Defense and Response** — Providing real-time monitoring, detection and mitigation of cyber threats.

Cyber Defense Centers

Wipro Cybersecurists deliver managed and hosted services out of Cyber Defense Centers strategically located around the globe, ensuring we are always close to our 600+ customers.



Contact us

Americas 1

Rangana Guha

Head of Americas 1

- Healthcare and Medical Devices
- Consumer Goods and Lifesciences
- Retail, Transportation and Services
- Communications, Media and Information Services
- Technology Products and Platforms
- Latin America (LATAM)

Americas 2

Mark Vanston

Head of Americas 2

- Banking, Financial Services
- Security, Investment Banking and Insurance
- Hi-Tech
- Energy, Natural Resources and Utilities (ENU)
- Manufacturing
- Canada

Europe

Hitesh Bansal

Head of UK and Ireland

Viv. Eberhardt

Head of Continental Europe

APMEA

Bharat Shetty

APMEA leader for India, Middle East, Australia and New Zealand, Southeast Asia, Japan, Africa

Previous editions of State of Cybersecurity Report

SOCR 2023:
wipro.com/cybersecurity/state-of-cybersecurity-report-2023/

SOCR 2020:
wipro.com/content/dam/nexus/en/service-lines/applications/latest-thinking/state-of-cyber-security-report-2020.pdf

SOCR 2019:
wipro.com/content/dam/nexus/en/service-lines/applications/latest-thinking/state-of-cyber-security-report-2019.pdf

SOCR 2018:
wipro.com/content/dam/nexus/en/service-lines/applications/latest-thinking/state-of-cyber-security-report-2018.pdf

SOCR 2017:
wipro.com/content/dam/nexus/en/landing-page/state-of-cybersecurity-report-2018/pdf/state-of-cybersecurity-report-2017.pdf

Ambitions Realized.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs.

Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With over 230,000 employees and business partners across 65 countries, we deliver on the promise of helping our clients, colleagues, and communities thrive in an ever-changing world.

For additional information, visit us at **www.wipro.com**

GEO/AGENCY CODE/VALIDITY