

# STATE OF CYBERSECURITY REPORT

CYBER RESILIENCE IN AN AGE  
OF CONTINUOUS DISRUPTION

#SOCR

2023

Spotlight  
on AI

PAGE 8

# TABLE OF CONTENTS

A NOTE FROM TONY BUFFOMANTE .....	3
<b>EXECUTIVE SUMMARY .....</b>	<b>4</b>
The Big Picture.....	5
Spotlight on AI: Risk and Compliance.....	8
Insights.....	10
Attacks are on the rise .....	11
The modern enterprise embraces cybersecurity.....	13
How are enterprises investing in 2023 .....	15
Cloud-first mindset gaining momentum.....	17
Collaboration is critical .....	18
A look into the future .....	19
Security Trends by Geography .....	21
Americas .....	22
Europe .....	23
Asia Pacific • Middle East • Africa .....	24
Security Trends by Sector .....	25
Banking, Financial Services and Insurance .....	26
Communications.....	27
Consumer .....	28
Energy, Natural Resources and Utilities .....	29
Healthcare .....	30
Manufacturing.....	31
Technology .....	32
<b>SECTION I: State of Attacks, Breaches and Laws .....</b>	<b>33</b>
<b>SECTION II: State of Cyber Capabilities .....</b>	<b>46</b>
<b>SECTION III: State of Collaboration .....</b>	<b>67</b>
<b>SECTION IV: Future of Cybersecurity .....</b>	<b>75</b>
ASSOCIATED PARTNERS .....	87
ABOUT WIPRO .....	88
AUTHORS AND REFERENCES .....	91

# A Note from Tony Buffomante



**TONY  
BUFFOMANTE**

SVP & Global Head –  
Cybersecurity & Risk Services

Wipro Ltd.

@TonyBuffomante

[www.linkedin.com/in/  
buffomante](https://www.linkedin.com/in/buffomante)

**“The best response to continuous disruption is continuous innovation.”**

Over the past three years, major technological, geopolitical and economic disruptions have forced organizations to change their approach to cybersecurity threats and risk management. The pandemic exposed the enterprise to new risks due to a sharp increase in remote work and disruptions to the supply chain. Nation-state attacks disproportionately impacted the private sector. We've also seen a rapid acceleration of advanced technologies for phishing and ransomware. Shocks to the global economy have put pressure on cybersecurity budgets, pushing security professionals to do more with less.

Today we find ourselves in an age of continuous disruption. It's the new normal for cybersecurity and challenges the modern enterprise to rethink how the C-suite prepares and reacts. This report answers four key questions:

1. What is the state of cyberattacks, breaches and regulatory laws?
2. What is the state of enterprise capabilities for addressing threats?
3. How well are enterprises collaborating with key internal and external stakeholders?
4. Which technologies are likely to impact enterprise cybersecurity in the near future?

The best response to continuous disruption is continuous innovation. Wipro has transformed to help our clients meet these evolving challenges. We deliver on the promise of reducing costs and gaining efficiencies through managed services — our foundational expert skillset — and growing innovative strategic consulting services through targeted acquisitions of regional and industry-specific strategy consulting firms.

# EXECUTIVE SUMMARY



# The Big Picture

We've entered an age of continuous disruption, and because of this, the responsibilities of the typical CISO and others holding senior risk and security roles, are rapidly evolving. The 2023 State of Cybersecurity Report (SOCR) offers a perspective and framework to help enterprises achieve cyber resilience. Our extensive research uncovered a wealth of actionable insights within four main topic areas:

- State of Attacks, Breaches and Laws
- State of Cyber Capabilities
- State of Collaboration
- Future of Cybersecurity

## **Wipro's cybersecurity outlook for 2023 and beyond**

Global enterprises have been leveraging innovative technology to modernize business operations and grow at scale. The primary driver of this effort has been cloud adoption which provides the means to deliver almost unlimited scalability.

We're arguably reaching the tail end of the digital transformation journey now that a majority of businesses have transitioned at least some workloads to the public or private cloud. As cloud footprints continue to expand, logical boundaries are becoming fuzzy. Cloud security loopholes such as misconfigurations, blind spots, shadow IT and lack of visibility create challenges for CXOs. A resilient cloud must strategically align with the organization's business objectives. This requires building a secure cloud architecture, adopting standards and best practices for cloud security governance and using automation to enhance risk and compliance visibility.

Security leaders have been working hard to solve these issues. But CISOs can't afford to take a breath. An even more disruptive technology is rolling out at a dizzying pace. The enterprise IT, security and risk challenges surrounding Artificial Intelligence (AI) are orders of magnitude greater than those produced by cloud adoption.

## **AI adoption in the business environment**

Businesses are focused on efficiently growing at scale, and many organizations are rapidly adopting generative AI tools to accelerate their growth objectives. AI is being embedded across the enterprise — in new and existing products and software — to create improved customer experiences, more intelligent software and broad operational efficiencies. In this early phase, companies are primarily using AI to automate repetitive tasks and uncover relevant patterns and correlations. Our research revealed that 79% of companies

are prioritizing security orchestration and automation. But the seemingly unlimited capabilities of generative AI and large language models are evolving so quickly that it's all too easy to put risk management on the back burner. Managing the risk, security and compliance of generative AI is a formidable challenge for CISOs.

The enterprise threat landscape from edge to cloud is becoming more porous. It includes millions of distributed endpoints, poorly protected remote sites and home offices, IoT/IIoT/OT devices, shadow clouds next to legitimate clouds, mobile devices that are never backed up by IT and scores of global partners with greater levels of access privileges.

In this unstable environment, hacking has become a multi-billion-dollar well-funded industry. Bad actors have the same advanced technology tools as the businesses they target. This is fueling an increase in the sophistication and sheer numbers of attacks and is cutting down the end-to-end life cycle of attacks — in many cases, to a matter of hours. It is driving — arguably forcing — businesses to adopt AI systems to fortify defenses and simultaneously accelerate growth.

AI, along with its machine learning (ML) component, has the potential to sharply change the cybersecurity landscape. It can grow and learn. It can accelerate defense reactions fast enough to keep ahead of the bad actors by recognizing attacks that don't necessarily match previously seen patterns.

But like all tools, AI is only as good as the people using it. To avoid the kinks in the AI cybersecurity armor, a proper deployment is truly a partnership. You need the right people to write the code, the right people to test it and, critically, the right people to oversee the AI effort on an ongoing basis. To deploy cost-effective AI governance, enterprises must design a risk-based AI framework that includes constant monitoring and oversight to prevent it from creating security holes and backdoors that could allow data leakage to cyber thieves and business competitors. To better understand the risk and compliance challenges posed by AI, along with some best practices on how to solve them, please see the **Spotlight on AI Risk and Compliance** section on [page 8](#).

## Balancing agile risk strategies with cost optimization and business priorities

These technology sea changes, coupled with global economic uncertainty, changing regulatory compliance requirements and market dynamics, are challenging security leaders to reduce costs without increasing risks and to optimize the performance of existing cybersecurity investments.

Cybersecurity financial management best practices are evolving to support increasing levels of operational speed, agility, flexibility and security. However, more than two-thirds of organizations are spending less than 10% of the IT budget on security. Enterprises need to assess current cybersecurity spending against the maturity of the organization to identify cyber cost optimization opportunities using four key strategies:

- **Cybersecurity operating model** enhancing risk-based collaboration and accountability with governance and control frameworks.
- **Tools rationalization** assessing security technology investments with a market view on where expansion or consolidation is warranted.
- **Process optimization** using automation and integration to allocate available resources more effectively and adequately fund prioritized risk and compliance processes.
- **Intelligent automation** adopting generative AI and machine learning across all processes to automate and orchestrate cyber hunting, containment, response and remediation.

The reality is security professionals must learn to do more with less. We believe, and share with our clients, that the way to do this, leveraging the framework above, is to view security as an investment that can help win new business, increase market share and boost revenue.

An agile operating model can quickly reallocate the security budget to ensure resources are aligned with strategic business priorities. This includes encouraging leaders in all departments to consider cybersecurity investments with a focus on multi-year cost optimization rather than pure cost reduction. This agility allows an enterprise to efficiently dial its security spend up and down for more effective risk management.

## Expanding cybersecurity expertise in the boardroom

One critical change enterprises are embracing is adding experienced cybersecurity talent to the board. Security concerns, and linking these to the enterprise risk tolerance, is now on the agenda at nearly every board meeting. Having directors with cybersecurity experience in the room enables the board to understand security data and improve the quality of critical security briefings.

Security and risk management can no longer be considered just a cost center. They must factor into every element of operations, including marketing, manufacturing, distribution, supply chain, web operations and selecting global partners. Cybersecurity expertise in the boardroom ensures that a company makes strategic decisions that align with long-term business objectives.

## Simulating attacks and responses to improve cyber resilience

Other aspects that a modern cybersecurity strategy must address are the impacts — direct and indirect — attacks have on the business. For example, the steady drumbeat of breach notifications could desensitize some customers and partners to the significant risks of working with a breached company. But if a breach, whether via ransomware or a DDoS attack, causes the company's website to go down for an extended period, that could result in a significant revenue impact.

Our report found that many CIOs lack confidence in the ability of their enterprises to recover quickly from an attack. The term "quickly" means different things to different CIOs, but the fact is that many of them do not have a good grasp of what will happen after an attack.

One way to improve the understanding of and response to attacks is to run regular cyberattack simulation exercises. Simulations can train employees to respond effectively in different scenarios to minimize damages and help the organization discover blind spots in their systems that threat actors may use as breach access points. It's encouraging to note that just 4% of survey respondents had not conducted any sort of incident response exercise in the past two years. However, among the organizations that have conducted simulation exercises, only 27% led board members in the process. While no business can perfectly protect itself from every attack, every business can map out what is likely to happen, communication protocols, and how it can quickly recover.

In addition to testing operational crisis readiness based on predefined scenarios, organizations are starting to continuously test their defenses through automated penetration testing. Automated attack simulations use the same AI tools and processes employed by bad actors in an effort to continuously reduce the attack surface without waiting for the next planned simulation exercise.

# Spotlight on AI: Risk and Compliance

As Artificial Intelligence (AI) and machine learning (ML) transition from the early adoption phase to the mainstream, the supporting technology will become more powerful, take on more roles and disrupt the risk and compliance landscape of virtually every organization.

Enterprises are exploring how AI can help implement greater operational efficiencies by automating simple, repetitive tasks and enhancing complex communications.

But the challenges are evolving and growing in complexity at an alarming rate. Key challenges include:

- **Disruption** — Millions of jobs may be eliminated by generative AI unless intended use guidelines and policies are established and enforced
- **Data protection and privacy** — AI running across organizations to grow the business has little oversight on the potential exposure of personal data and the overall impacts on privacy and consumer protection
- **Legal and compliance** — The US and the EU are introducing AI-related laws and regulations and designing blueprints for an AI Bill of Rights, including how the incorrect or unethical use of AI can subject organizations to compliance penalties
- **Reputational risk** — While AI is a growth driver, poor implementation and usage inexperience can lead to consumer dissatisfaction and reputational brand damage
- **Cybersecurity** — Hackers can use AI to increase the volume and sophistication of attacks and steal confidential data sets and AI models to sell on the dark web.

Because there are so many unknowns surrounding the risks of AI, there is a tendency to simply say, “You can’t use it until we fix it.”

## AI risk management framework

Organizations need to establish a framework incorporating rules and controls around how the technology will be adopted. This includes defining the types of prompts that can and cannot be fed into AI models and how to leverage what comes out.

Wipro utilizes the NIST AI RMF Core in conjunction with the OECD Framework to classify and provide outcomes and actions that enable dialogue, understanding and activities to manage AI risks and responsibly develop trustworthy AI systems. Trustworthy AI is safe, secure, resilient, explainable and interpretable, privacy-enhanced, fair, valid, reliable, accountable and transparent.

The NIST AI RMF Core is composed of four functions:

- **Govern** — A culture of risk management is cultivated and present
- **Map** — Context is recognized and related risks are identified
- **Measure** — Identified risks are assessed, analyzed or tracked
- **Manage** — Risks are prioritized and acted on based on project impact

## AI/ML risk governance action steps

There is no one answer to the question of how to approach AI/ML governance with cybersecurity and privacy in mind. Following are seven recommended actions organizations can take to become more digitally resilient with their AI-enabled technologies.

- Define intended use and user guidelines
- Clarify code ownership
- Establish intellectual property rights
- Address security policies and confidentiality measures
- Focus on identity security
- Revamp security offerings
- Ensure compliance with legal and regulatory requirements

These rules of engagement help security leaders to have informed conversations with stakeholders that have a vested interest in using AI systems. Once a governance process is established, classification of the systems can be put in place and risks may be documented. Only then can the organization build cybersecurity controls and protection mechanisms directly into the AI system and data model and provide a foundational infrastructure. It is a multi-step journey in the wake of an ever-expanding attack surface introduced by AI systems.



# INSIGHTS



# ATTACKS ARE ON THE RISE

Nation-state attacks are targeting public and private sectors

82%

of all nation-state attacks are focused on espionage

## Top Targets

39%

Private Sector

34%

Government

23%

Civil Society

Private sector espionage attacks include stealing IP secrets, research, corporate secrets and competitive spying.

81%

Email phishing



79%

Ransomware attacks

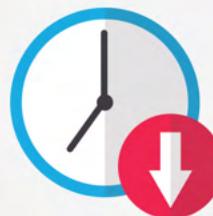
Top threats remain the same, tactics are evolving

Advanced PII theft is increasing



Breaches involving PII records increased by  
**13%**





## 65%

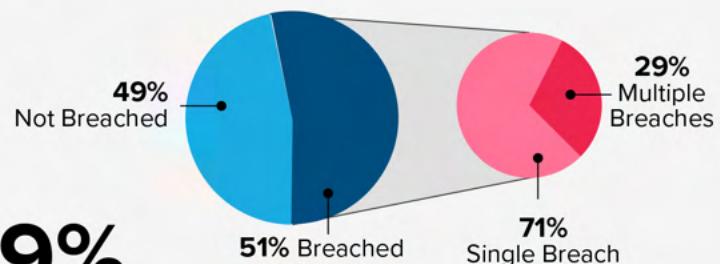
of organizations faced more than six days of downtime after a ransomware attack

## System restoration time is still a challenge

## Repeat breaches are a growing concern

## 29%

of breached organizations experienced repeated incursions within three years



## 70%

of the 23 countries analyzed have strengthened breach notification laws

## Breach notification laws are being strengthened globally

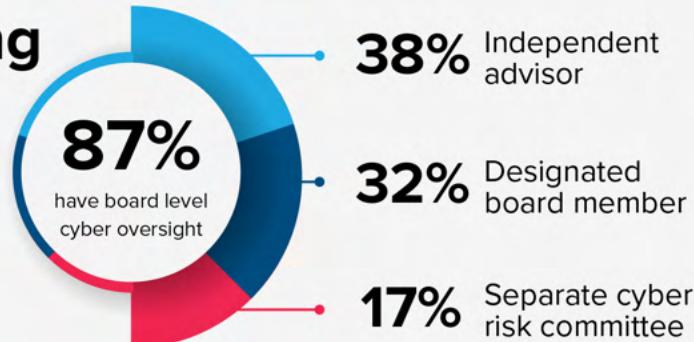


### State of Attacks, Breaches and Laws

Read more on page 33

# THE MODERN ENTERPRISE EMBRACES CYBERSECURITY

**Board cyber reporting systems must be enhanced to keep pace with demands**



**41%** Quarterly

**27%** Monthly

**68%**

of organizations report cyber risk to the board at least once every quarter

**Risk reporting to the board is getting more frequent**

**Increasing demands on systems to supply real-time reporting**



Cyber risk management must be aligned to business objectives



Reports must be relevant and succinct enough for board digestion





**75%**

Brand  
reputation



**42%**

Consumer  
trust



**42%**

Revenue Loss  
Due to Downtime

## Damage to the organization from cyber threats

## Attack recovery confidence is low

Only **9%**  
of CIOs are confident  
that they can recover quickly  
from attacks



Reporting to CEO



Reporting to CIO



## The number of CISOs reporting to the CEO grew by 11% since 2020



### State of Cyber Capabilities

Read more on page 46

# HOW ARE ENTERPRISES INVESTING IN 2023

## Security allocations in IT budgets

**32%**

of surveyed organizations are spending greater than 10% of their IT budget for security



**61%**

of organizations are focusing on regional compliance

**Compliance is being prioritized**

**Identity is the new cybersecurity perimeter**

**57%**

of organizations listed OpEx reduction leveraging IAM-as-a-Service as a priority





Tackling unknown attacks



Asset visibility



Team skills

## Top priorities for Security Operation Centers

## Top barriers to business transformation



**63%**

Lack of appropriate cyber talent



**50%**

Lack of time to execute

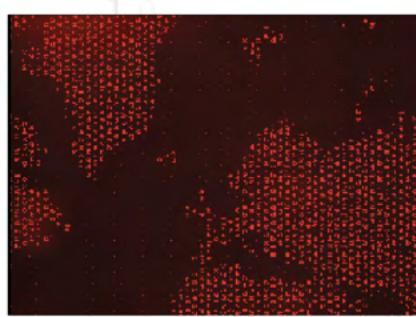
### TOP 3

- Technical Aptitude
- Certifications
- Relevant Experience

### BOTTOM 3

- Intellect
- Interpersonal Skills
- Agility

## CISO priorities for cyber talent



**State of Cyber Capabilities**  
Read more on page 46

# CLOUD-FIRST MINDSET GAINING MOMENTUM

Hosting risks are coming down and more organizations are thinking cloud-first



Declining cloud hosting risks



**79%**

Security  
orchestration  
& automation



**71%**

Zero Trust  
networks



**67%**

Third party risks/  
supply chain  
security

**Top security  
investment  
priorities**

**Cloud footprints  
continue to expand**

“ Logical boundaries are becoming very fuzzy. Cloud security loopholes such as misconfigurations, blind spots, shadow IT and lack of visibility are creating worrying challenges for CXOs. ”

# COLLABORATION IS CRITICAL

## Top barriers to threat intelligence sharing



Only  
**27%**  
of cyber simulation exercises involve boards



**Most incident response exercises exclude board members**

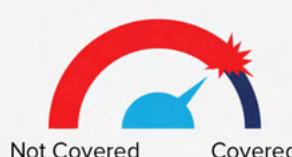
**Third-party risk reporting needs to be better managed**



**35%**

of organizations said their third-party suppliers reported a security breach

**69%**  
of organizations report that reputational risk is not covered



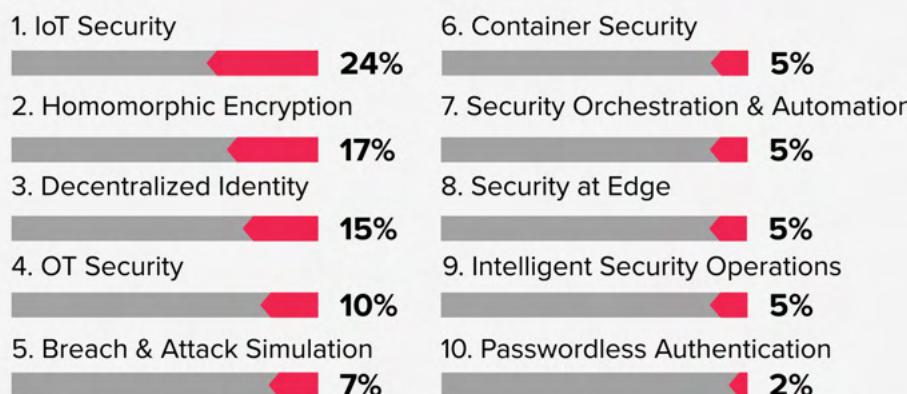
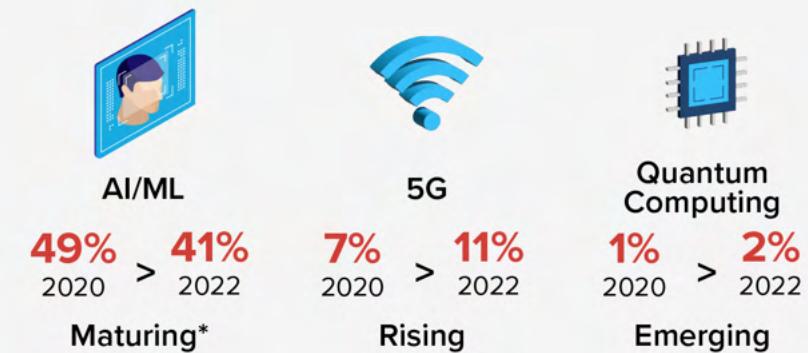
**Cyber insurance does not cover all risks**



**State of Collaboration**  
Read more on page 67

# A LOOK INTO THE FUTURE

## Cyber technology patent trends



## Top domains for new cyber patents

Global dominance in new technology patents is in the early stage

#1  
China

- |              |             |
|--------------|-------------|
| 2. USA       | 7. Canada   |
| 3. EU        | 8. Japan    |
| 4. Korea     | 9. Taiwan   |
| 5. India     | 10. Germany |
| 6. Australia |             |



Future of Cybersecurity  
Read more on page 75

# SECURITY TRENDS GEOGRAPHY & SECTOR

# Security Trends by Geography

We analyzed responses from the State of Cybersecurity Report 2023 research across three geographical clusters:

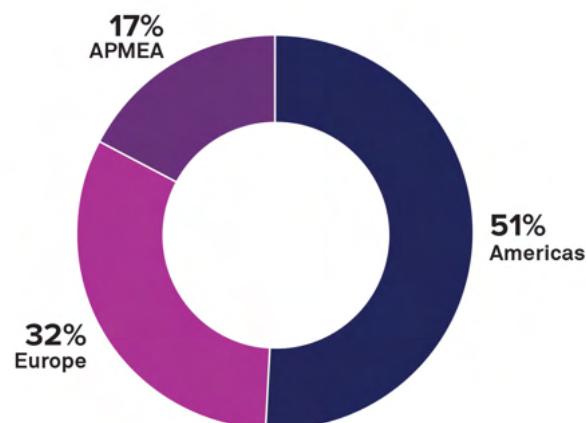
## GEOGRAPHIES:

Americas, Europe, APMEA (Asia Pacific, Middle East and Africa)

Responses were further analyzed to produce 10 critical trends:

- Cadence of cyber risk reporting
- Board's cyber expertise
- CISO reporting
- Top cyber risks
- Confidence in cyber controls
- Recent data breach
- Third-party security breach
- Downtime due to ransomware attacks
- Percentage of annual IT budget allocated for security
- Investment priorities

Figure 1: Response Distribution by Geography



# AMERICAS

## Cyber Risk Reporting to the Board

40% of the organizations report quarterly and 27% report monthly

## Board's Cyber Expertise

85% of the boards have established some form of cybersecurity oversight\*

## CISO Reporting

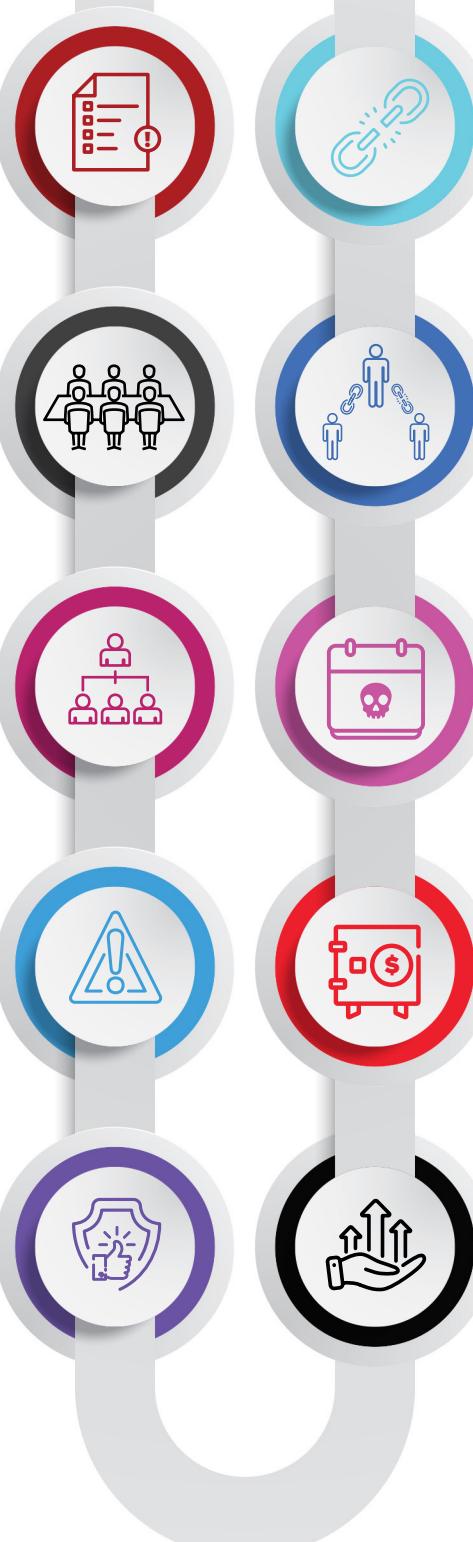
55% CISOs report to CIO and 25% report to CEO

## Top 2 Cyber Risks

87% view ransomware attacks as their top risk  
82% view email phishing as their top risk

## Confidence in Cyber Control

37% are highly confident about protecting their systems from an attack, however only 11% are confident in recovering quickly from a cyberattack



## Recent Data Breaches

46% of the organizations have experienced at least one breach in the last 3 years

## 3rd Party Security Breaches

34% said their 3rd party suppliers reported a security breach last year

## Downtime Due to Ransomware Attacks

33% of organizations that experienced ransomware attack in the last 3 years, faced a downtime of 11 to 30 days

## Security Budget

27% of organizations allocate more than 12% of their IT budget for security

## Investment Priorities

84% picked Security Orchestration and Automation as a continued investment priority  
75% picked both Zero Trust Networks & Third-Party Risk/Supply Chain Security as their top priority

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# EUROPE

## Cyber Risk Reporting to the Board

**37%** of the organizations report quarterly and  
**28%** report monthly

### Investment Priorities

**73%** picked Security Orchestration and Automation as their top priority  
**72%** picked Zero Trust Networks as their top priority

### Security Budget

**13%** of organizations allocate more than **12%** of their IT budget for security

### Downtime Due to Ransomware Attacks

**28%** of organizations that experienced a ransomware attack in the last 3 years, faced a downtime of 11 to 30 days

### 3rd Party Security Breaches

**36%** said their 3rd party suppliers reported a security breach last year

### Board's Cyber Expertise

**85%** of the boards have established some form of cybersecurity oversight\*

### CISO Reporting

**51%** CISOs report to the CIO and **24%** report to the CEO

### Top 2 Cyber Risks

**78%** view email phishing as their top risk  
**72%** view ransomware attacks as their top risk

### Confidence in Cyber Control

**23%** are highly confident about protecting their systems from an attack, however only **8%** are confident in recovering quickly from a cyberattack

### Recent Data Breaches

**56%** of the organizations have experienced at least one breach in the last 3 years

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# ASIA PACIFIC • MIDDLE EAST AFRICA

## Cyber Risk Reporting to the Board

**54%** of the organizations report quarterly and **24%** report monthly

## Board's Cyber Expertise

**97%** of the boards have established some form of cybersecurity oversight\*

## CISO Reporting

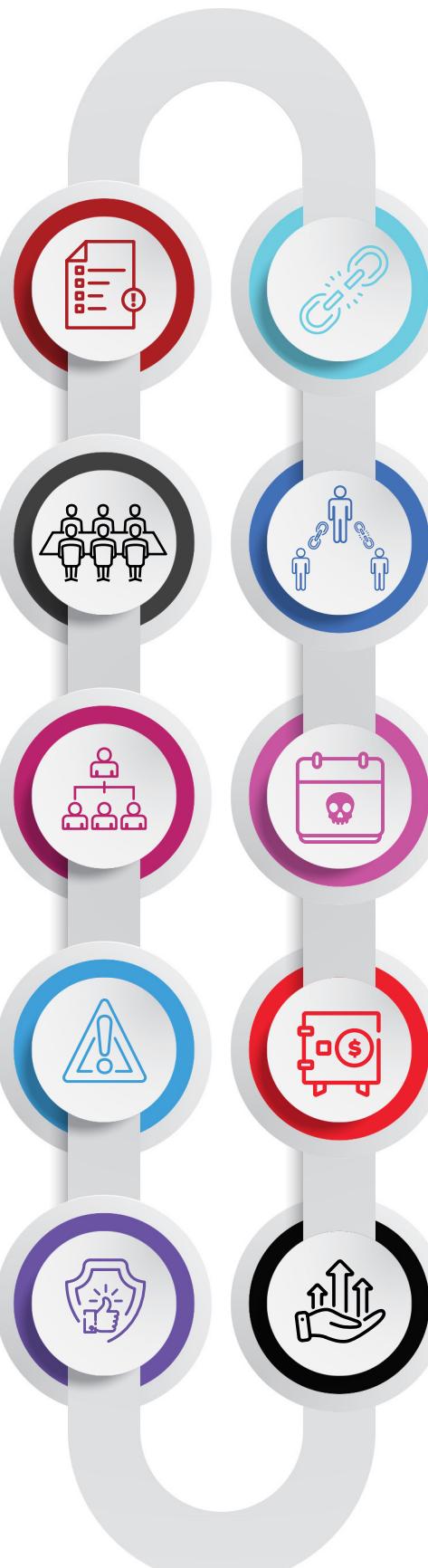
**58%** CISOs report to the CIO and **25%** report to the CEO

## Top 2 Cyber Risks

**83%** view email phishing as their top risk  
**68%** view ransomware attacks as their top risk

## Confidence in Cyber Control

**36%** are highly confident about protecting their systems from an attack, however only **5%** are confident in recovering quickly from a cyberattack



## Recent Data Breaches

**59%** of the organizations have experienced at least one breach in the last 3 years

## 3rd Party Security Breaches

**37%** said their 3rd party suppliers reported a security breach last year

## Downtime Due to Ransomware Attacks

**44%** of organizations that experienced a ransomware attack in the last three years faced downtime of 11 to 30 days

## Security Budget

**14%** of organizations allocate more than **12%** of their IT budget for security

## Investment Priorities

**75%** picked Security Orchestration and Automation as their top priority  
**64%** picked DevSecOps as their top priority

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# Security Trends by Sector

We analyzed responses from the State of Cybersecurity Report 2023 research across seven industry sectors:

## SECTORS:

**BFSI:** Banking, Financial Services, Insurance

**Communications:** Telecommunications

**Consumer:** Consumer Goods, Retail, Distribution, Travel & Hospitality, Transportation, Media, Education, Public services

**ENU:** Energy, Natural Resources, Utilities

**Healthcare:** Life Sciences, Medical Devices

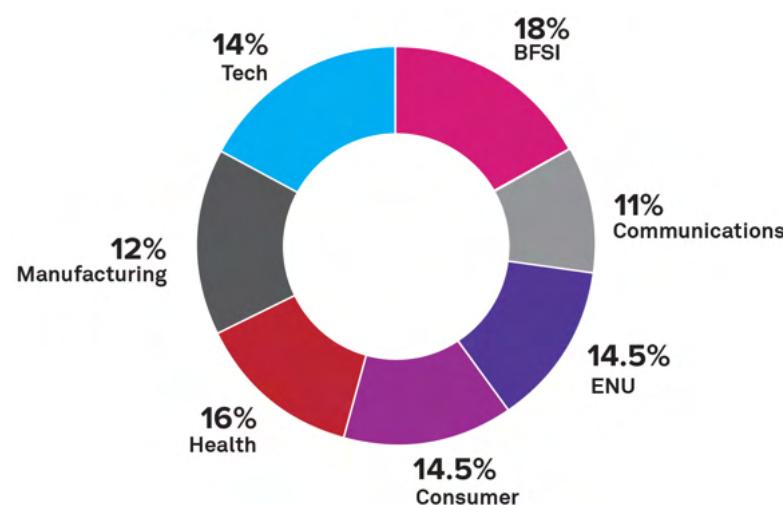
**Manufacturing:** Industrial Process Manufacturing, Automobile

**Technology:** Tech Products and Platforms, Semiconductors, Network Equipment Providers

These sector-specific responses were further analyzed to produce 10 critical trends:

- Cadence of cyber risk reporting
- Board cyber expertise
- CISO reporting
- Top cyber risks
- Confidence in cyber controls
- Recent data breach
- Third-party security breach
- Downtime due to ransomware attacks
- Percentage of annual IT budget allocated for security
- Investment priorities

Figure 2: Response Distribution by Sector



# BANKING, FINANCIAL SERVICES AND INSURANCE

## Cyber Risk Reporting to the Board

**54%** of the organizations report monthly and  
**40%** report quarterly

### Investment Priorities

**71%** said Security Orchestration and Automation continued to be their top priority  
**59%** said Third-Party Risk and DevSecOps is their top priority

### Security Budget

**43%** of organizations allocate more than **12%** of their IT budget for security

### Downtime Due to Ransomware Attacks

**28%** of organizations that experienced a ransomware attack in the last three years faced downtime of 11 to 30 days

### 3rd Party Security Breaches

**47%** said their 3rd party suppliers reported a security breach last year

### Board's Cyber Expertise

**95%** of the boards have established some form of cybersecurity oversight\*

### CISO Reporting

**52%** CISOs report to the CIO and **19%** report to the CRO

### Top 2 Cyber Risks

**79%** view email phishing as their top risk  
**76%** view ransomware attacks as their top risk

### Confidence in Cyber Control

**54%** are highly confident about protecting their systems from an attack, however only **10%** are highly confident in recovering quickly from a cyberattack

### Recent Data Breaches

**59%** of the organizations have experienced at least one breach in the last 3 years

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# COMMUNICATIONS

## Cyber Risk Reporting to the Board

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

## Board's Cyber Expertise

**97%** of the boards have established some form of cybersecurity oversight\*

## CISO Reporting

**62%** CISOs report to the CIO and **21%** report to the CEO

## Top 2 Cyber Risks

**84%** view email phishing as their top risk  
**84%** view ransomware attacks as their top risk

## Confidence in Cyber Control

**62%** are highly confident about protecting their systems from an attack, however only **16%** are highly confident in recovering quickly from a cyberattack

## Recent Data Breaches

**62%** of the organizations have experienced at least one breach in the last 3 years

## 3rd Party Security Breaches

**46%** said their 3rd party suppliers reported a security breach last year

## Downtime Due to Ransomware Attacks

**52%** of organizations that experienced a ransomware attack in the last three years faced downtime of 11 to 30 days

## Security Budget

**43%** of organizations allocate more than **12%** of their IT budget for security

## Investment Priorities

**81%** said Security Orchestration and Automation is their top priority  
**81%** said Zero Trust Networks is their top priority

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# CONSUMER

## Cyber Risk Reporting to the Board

36% of the organizations report quarterly and  
28% report semi-annually

### Investment Priorities

78% chose Security Orchestration and Automation as their top priority  
78% said Zero Trust Networks is their top priority

### Security Budget

10% of organizations allocate more than 8% of their IT budget for security

### Downtime Due to Ransomware Attacks

19% of organizations that experienced a ransomware attack in the last three years faced downtime of 11 to 30 days

### 3rd Party Security Breaches

35% said their 3rd party suppliers reported a security breach last year

### Board's Cyber Expertise

68% of the boards have established some form of cybersecurity oversight\*

### CISO Reporting

50% CISOs report to the CIO and 26% report to the CEO

### Top 2 Cyber Risks

82% view email phishing as their top risk  
78% view ransomware attacks as their top risk

### Confidence in Cyber Control

Only 14% are highly confident about protecting their systems from an attack, however 70% are not confident in recovering quickly from a cyberattack

### Recent Data Breaches

55% of the organizations have experienced at least one breach in the last 3 years

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# ENERGY, NATURAL RESOURCES AND UTILITIES

## Cyber Risk Reporting to the Board

**34%** of the organizations report quarterly and **28%** report semi-annually

## Board's Cyber Expertise

**87%** of the boards have established some form of cybersecurity oversight\*

## CISO Reporting

**58%** CISOs report to the CIO and **32%** report to the CEO

## Top 2 Cyber Risks

**82%** view email phishing as their top risk  
**74%** view ransomware attacks as their top risk

## Confidence in Cyber Control

Only **6%** are highly confident about protecting their systems from an attack however confidence in quick recovery from a cyberattack is very low across all respondents



## Recent Data Breaches

**34%** of the organizations have experienced at least one breach in the last 3 years

## 3rd Party Security Breaches

**20%** said their 3rd party suppliers reported a security breach last year

## Downtime Due to Ransomware Attacks

**31%** of organizations that experienced a ransomware attack in the last three years faced downtime of 11 to 30 days

## Security Budget

**30%** of organizations allocate around **6%** or more of their IT budget for security

## Investment Priorities

**78%** said Security Orchestration and Automation continued to be their top priority  
**72%** said Zero Trust Networks Security is their top priority

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# HEALTHCARE

## Cyber Risk Reporting to the Board

51% of the organizations report quarterly and  
23% report semi-annually

### Investment Priorities

78% said Security Orchestration and Automation continued to be their top priority

71% said Zero Trust Networks Security is their top priority

### Security Budget

28% of organizations allocate more than 8% of their IT budget for security

### Downtime Due to Ransomware Attacks

40% of organizations that experienced a ransomware attack in the last three years faced downtime of 11 to 30 days

### 3rd Party Security Breaches

38% said their 3rd party suppliers reported a security breach last year

### Board's Cyber Expertise

94.5% of the boards have established some form of cybersecurity oversight\*

### CISO Reporting

55% CISOs report to the CIO and 25% report to the CEO

### Top 2 Cyber Risks

84% view email phishing as their top risk

75% view ransomware attacks as their top risk

### Confidence in Cyber Control

20% are highly confident about protecting their systems from an attack, however only 11% are highly confident in recovering quickly from a cyberattack

### Recent Data Breaches

62% of the organizations have experienced at least one breach in the last 3 years

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# MANUFACTURING

## Cyber Risk Reporting to the Board

**36%** of the organizations report quarterly and **26%** report annually

## Board's Cyber Expertise

**69%** of the boards have established some form of cybersecurity oversight\*

## CISO Reporting

**45%** CISOs report to the CIO and **29%** report to the CEO

## Top 2 Cyber Risks

**81%** view ransomware attacks as their top risk  
**74%** view email phishing as their top risk

## Confidence in Cyber Control

**17%** are highly confident about protecting their systems from an attack, however only **7%** are confident in recovering quickly from a cyberattack



## Recent Data Breaches

**38%** of the organizations have experienced at least one breach in the last 3 years

## 3rd Party Security Breaches

**26%** said their 3rd party suppliers reported a security breach last year

## Downtime Due to Ransomware Attacks

**31%** of organizations that experienced a ransomware attack in the last three years faced downtime of 11 to 30 days

## Security Budget

**17%** of organizations allocate more than **8%** of their IT budget for security

## Investment Priorities

**76%** said Security Orchestration and Automation is their top priority  
**71%** said Third-Party Risk/Supply Chain Security is their top priority

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

# TECHNOLOGY

## Cyber Risk Reporting to the Board

**54%** of the organizations report monthly and  
**38%** report quarterly

### Investment Priorities

**90%** picked Security Orchestration and Automation as their top priority  
**81%** picked Zero Trust Networks as their top priority

### Security Budget

**52%** of organizations allocate more than **12%** of their IT budget for security

### Downtime Due to Ransomware Attacks

**36%** of organizations that experienced a ransomware attack in the last three years faced downtime of 11 to 30 days

### 3rd Party Security Breaches

**31%** said their 3rd party suppliers reported a security breach last year

### Board's Cyber Expertise

**96%** of the boards have established some form of cybersecurity oversight\*

### CISO Reporting

**59%** CISOs report to the CIO and **27%** report to the CEO

### Top 2 Cyber Risks

**90%** view ransomware attacks as their top risk  
**83%** view email phishing as their top risk

### Confidence in Cyber Control

**56%** are highly confident about protecting their systems from an attack, however only **21%** are highly confident in recovering quickly from a cyberattack

### Recent Data Breaches

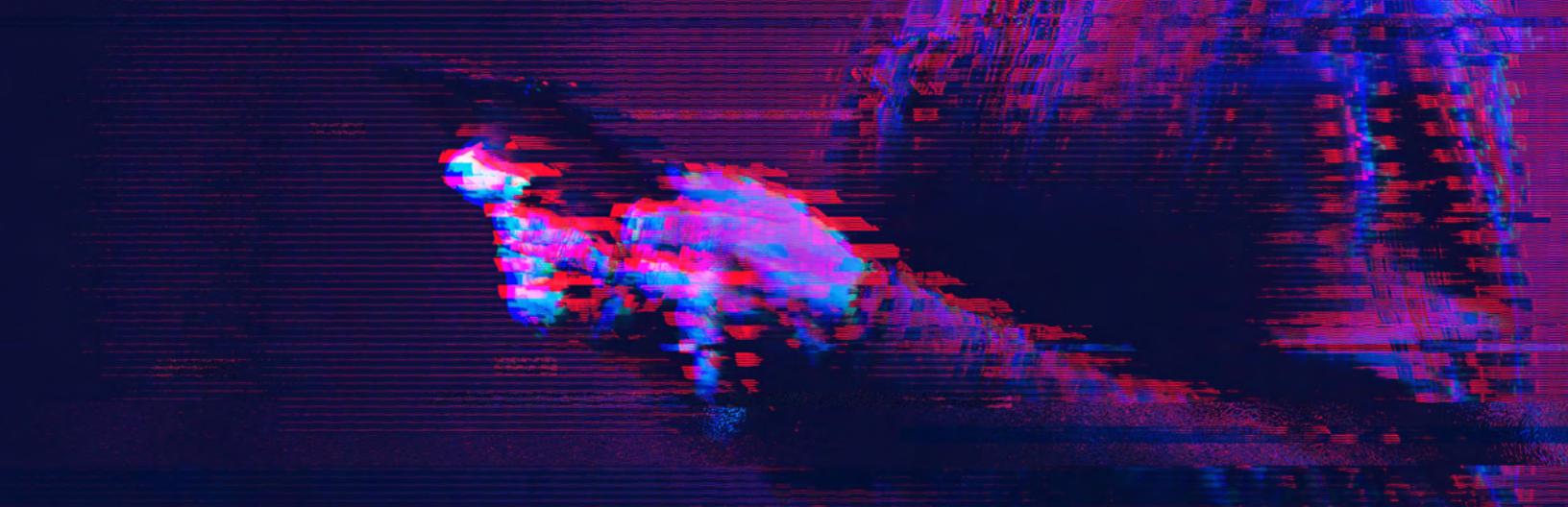
**48%** of the organizations have experienced at least one breach in the last 3 years

\*Through independent cyber advisors or designated board members or a defined cyber risk committee

SECTION I

# STATE OF **ATTACKS** BREACHES & LAWS





We identified six top cyber challenges that organizations face today:

- Nation-state cyber warfare
- Global non-state cyber risks
- Breaches – the data and the targets
- Time to recover
- Repeat breaches
- Cybersecurity regulatory change

## Nation-State Cyber Warfare

From 2018 to 2022, 39% of nation-state attacks have targeted the private sector, exposing organizations to all manner of threats, including espionage, digital lockdowns and damage to critical infrastructure. It is not the first time in recent history that cyberspace has served as a “second battlefield.” But it’s becoming an increasingly frequent phenomenon.

To provide a macro view of the situation, we carried out a secondary data analysis on 1,100+ nation-state attacks tracked by the Council on Foreign Relations from 2018 to 2022. We analyzed the intent of the attacks, which countries were behind the attacks, and which countries were targeted.

### GLOBAL INSIGHT



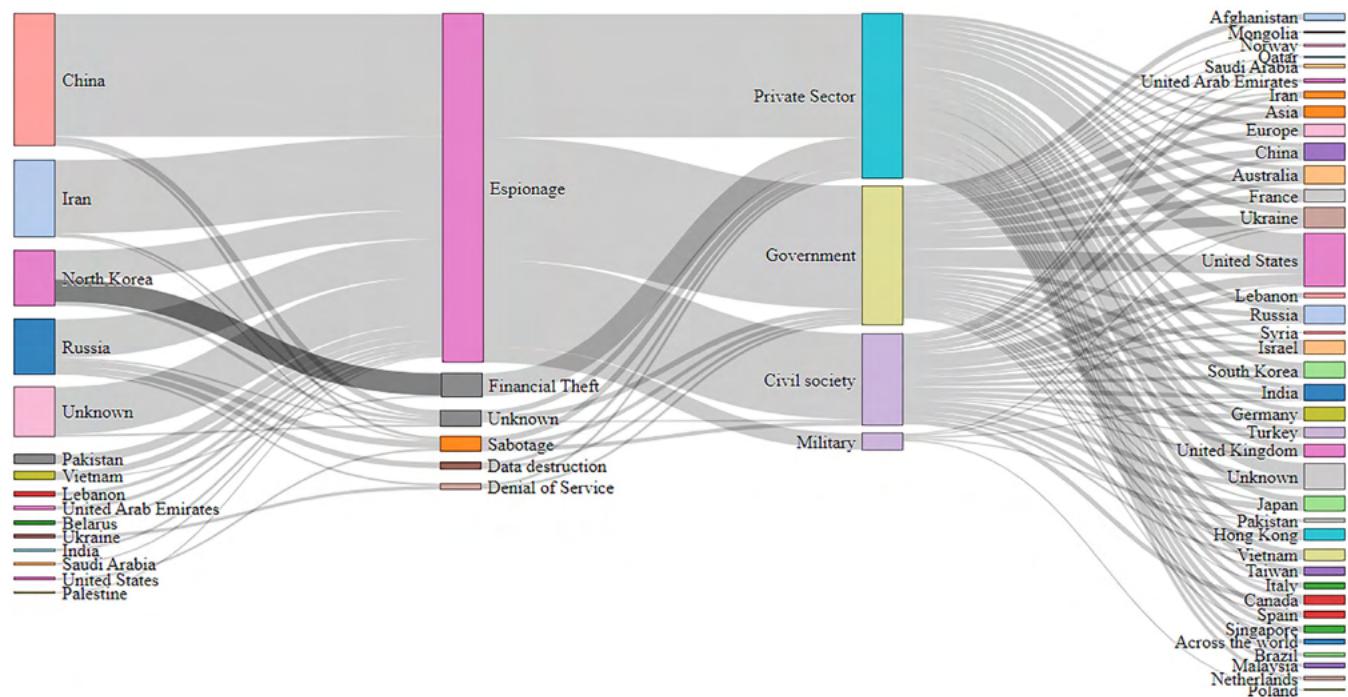
**82%**

of all nation state attacks focused on **espionage**

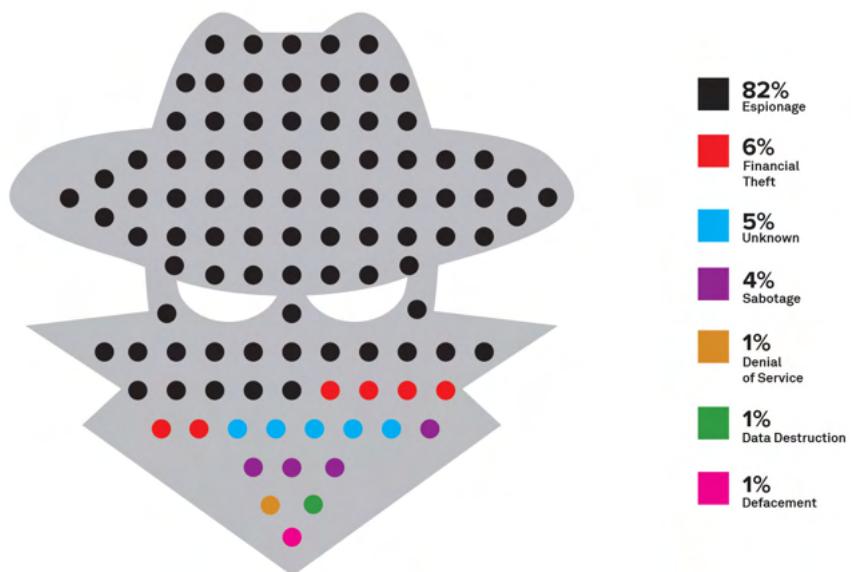
**39%**

of nation-state attacks targeted the private sector

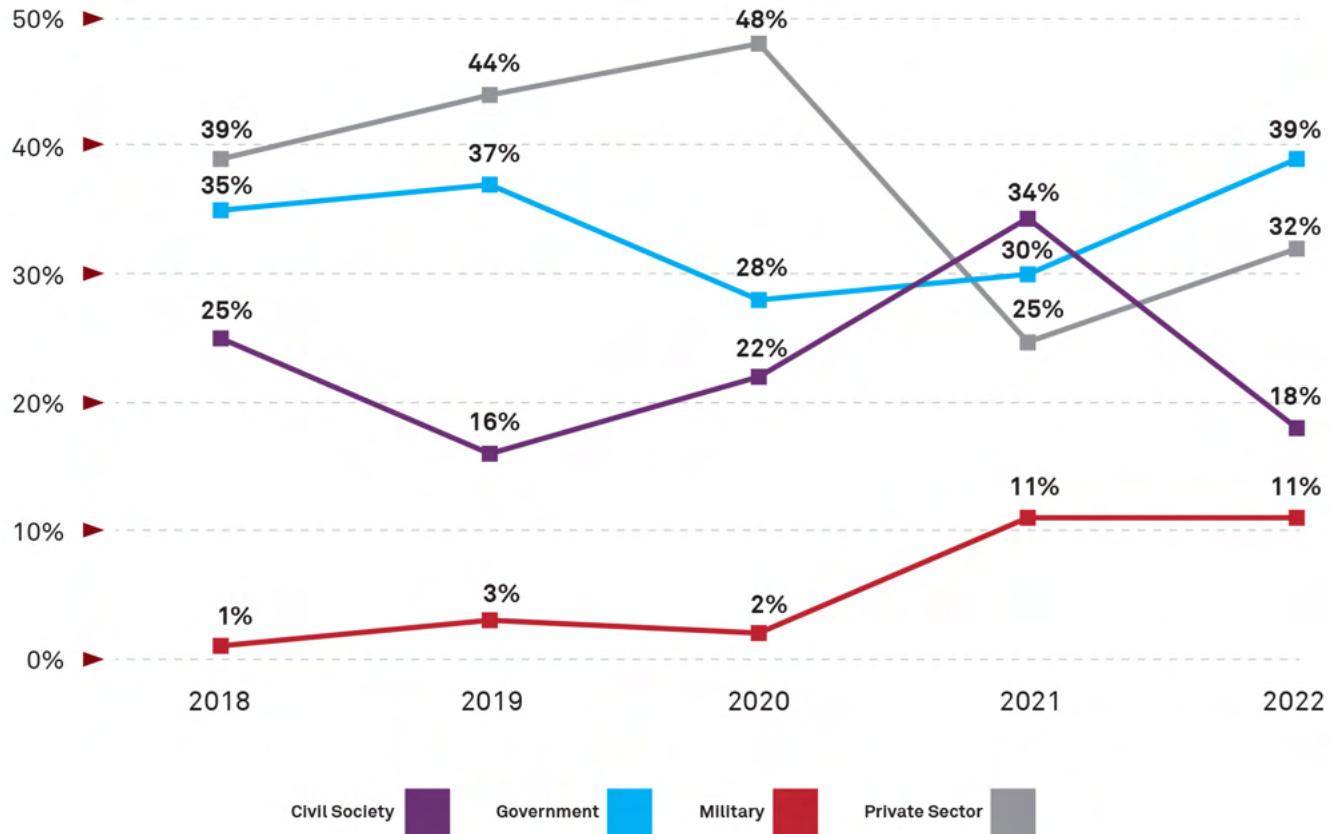
**Figure 3: Nation State Attack Analysis**



**Figure 4: Nation State Attack Type Distribution**



**Figure 5: Nation State Attack Trends by Target Category**



### A quick summary of the data:

- The vast majority (82%) of attacks were espionage-related.
- The main aggressors are China, Iran, North Korea, and Russia.
- Many countries were victims, but the US was the biggest target, followed by countries that border Russia.

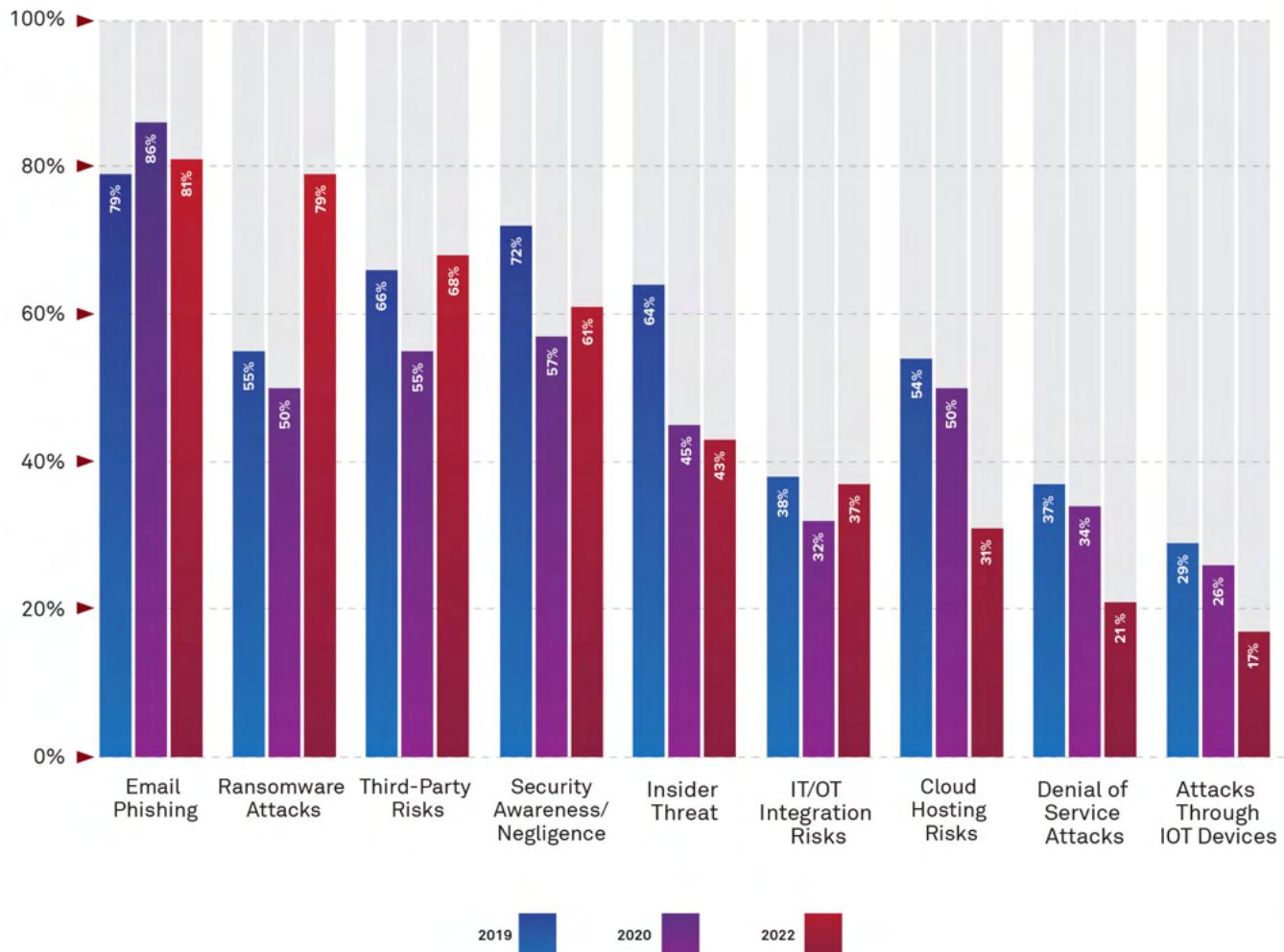
That the US was the top target country should be of concern to businesses that operate there. At the same time, it is worth noting that the most aggressive nation-states have hostile relations with the US. Businesses in the crossfire of hostilities should be mindful of the geopolitical implications of nation-state attacks.

## Global Non-State Cyber Risks

Organizations are facing more exposure to technologically sophisticated attacks from non-state actors. The top three threats are email phishing (81%), ransomware (79%) and third-party risks (68%).

o

Figure 6: Trends in Top Cyber Risks



### Email phishing and ransomware are top threats

With the expansion of email phishing templates available to a growing population of threat actors, phishing attacks flourished throughout the pandemic. We are seeing more targeted attacks on IT administrators, R&D, and senior executives using social platforms to gather specific insights.

In addition to the rise of nation-state attacks, organizations are facing increasing exposure to sophisticated attacks from non-state actors. The top three threats in this year's report are email phishing (81%), ransomware attacks (79%), and third-party risks (68%). A few notes on our findings:

## **81% Phishing—**

### **brace for generative AI-enabled “deep phishing”**

With the expansion of email phishing templates available to a growing population of threat actors, phishing attacks flourished throughout the pandemic. Now we are seeing more targeted attacks on IT administrators, R&D and senior executives who use social platforms. The growing use of outsourced SaaS IT for HR services with new corporate domains has also created additional phishing exposures. Omni-channel “deep phishing” attacks leveraging generative AI will make the detection of fakes even more challenging. Additional AI insights can be found in section 4—The Future of Cybersecurity.

## **79% Ransomware—**

### **extortion tactics evolve to intimidate executives**

Ransomware threat actors have changed their modus operandi from digital lockdowns to multivariate extortion tactics. In addition to locking down systems through encryption, extortion tactics now include threatening senior executives with the release of their stolen data on the dark web.

## **Operational Technology (OT) risks –**

### **visible increase in attacks on plants**

Recently reported intrusions into pipeline systems, water treatment plants, electrical grids and industrial plants have heightened the concern about risks to OT environments. An example of this threat is in Ukraine, where there have been attacks on electrical and nuclear plants. Other OT-related attacks include those on an oil plant in Italy, a power plant in India and public PLC systems of water plants across the globe. While the growth in digital industrial operations allows for seamless data exchange, the lack of visibility into real-time threats and changes within legacy OT environments has increased cyber risk.

## **68% Third-party risks—**

### **leverage of generative AI on the rise**

Global supply chains have linked various third parties – outsourcing partners, distributors, suppliers, captives and affiliates — with varying degrees of cybersecurity hygiene and maturity. This has increased the number of cyberattacks through third parties.

## **Offensive generative AI risks**

Advancements in generative AI will turbocharge all manner of attacks. While generative AI has enormous potential to be applied defensively in security management, its use for offensive purposes will be propelled by the ubiquity of the technology. Use cases for generative AI in offensive cyberattacks include:

- Generative-AI enabled social engineering
- GAN-forcing password attacks by way of brute-force
- Malware code engineering
- Exploit development leveraging generative AI
- Synthetic data generation for data poisoning attacks

## Breaches – the Data and the Targets

The three sectors that experienced the most breaches were technology (35%), consumer (29%) and health care (17%).

### GLOBAL INSIGHT

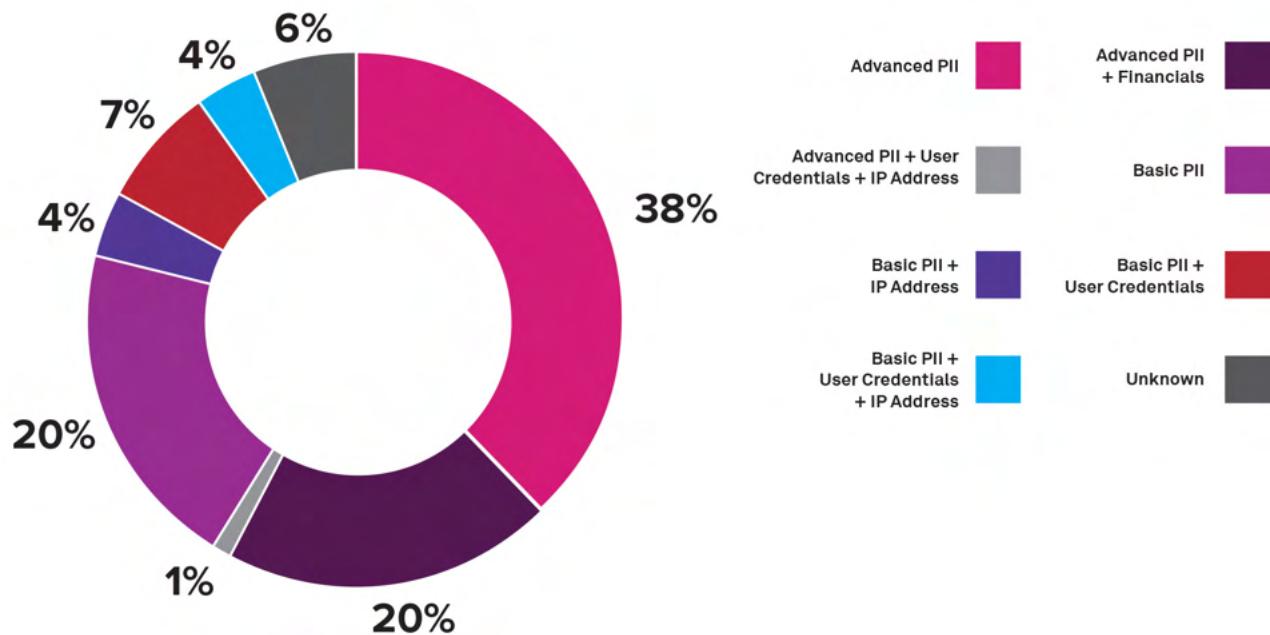
**38%** of all data breaches involved advanced PII records, which is a **13%** increase compared to 2020

Attackers have many different motivations and goals, but not all breaches and data are created equal. Nation-states may desire military secrets. Business competitors or terrorists may focus on sabotaging operations. Some attacks may be personal and motivated by profit, often targeting PII – personal identifiable information. There are different types of PII with distinct levels of economic value. To dig deeper into the kind of PII data threat actors seek, we researched the top 85 publicly-reported major data breaches of 2021 and 2022 and classified them into seven broad categories:

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

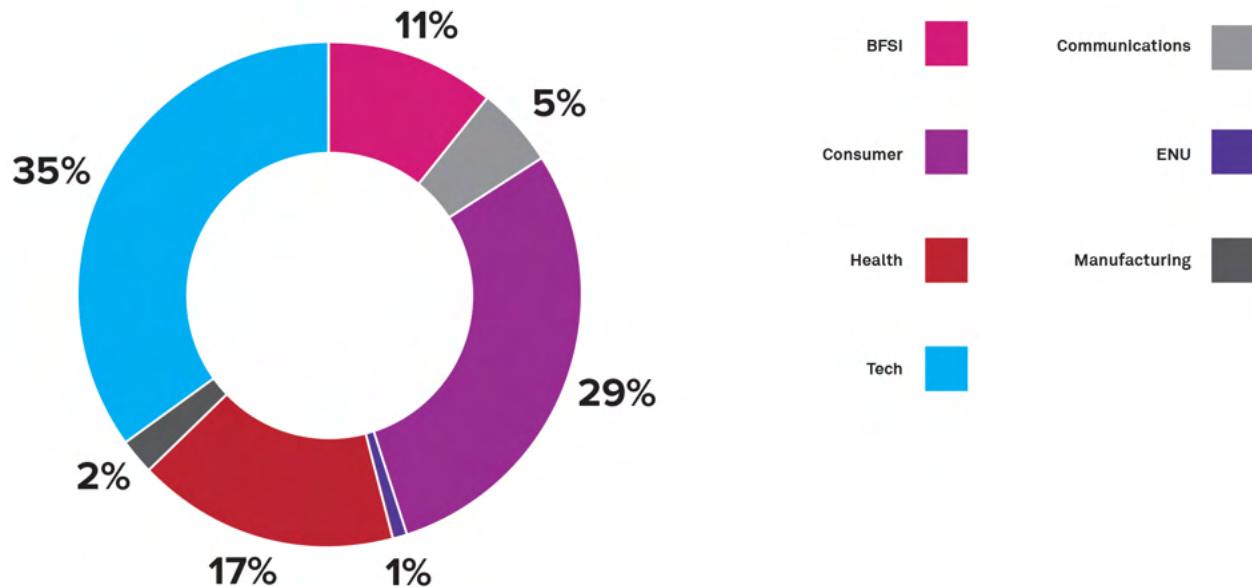
○

Figure 7: Classification of Compromised Data Across Top Breaches Worldwide

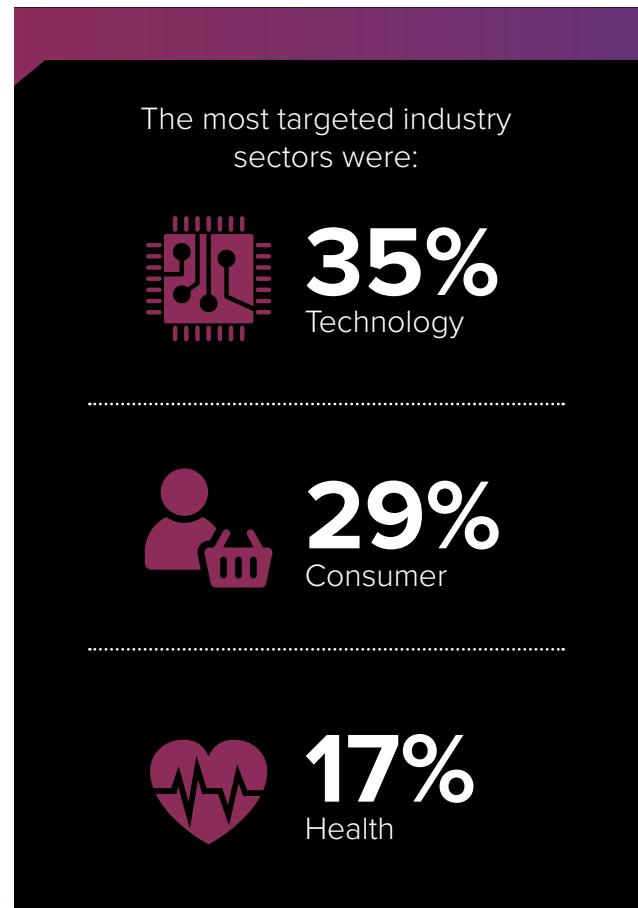


As shown in Figure 7, 38% of all data breaches included advanced PII, a sharp increase from 25% in 2020. Breaches involving advanced PII + financials increased slightly to 20% in 2022 from 17% in 2020. Breaches involving basic PII almost tripled from 8% in 2020 to 20% in 2022.

Figure 8: Distribution of Top Breaches Across Industry Sectors



As for which industries are the most targeted, technology, consumer, and health sectors were the hardest hit with 35%, 29%, and 17% of all attacks, respectively. This stands to reason because attackers are motivated by profit and these three sectors contain perhaps the richest trove of advanced PII data and are therefore the most lucrative. Again, attackers are motivated by profit. To understand an industry's exposure to threats, all one needs to do is follow the money.



## Time to Recover

Beyond the loss of sensitive data, breaches and ransomware attacks also expose enterprises to disruption of systems and business operations. Organizations have begun to evolve their ransomware recovery strategies around a minimum viable business service capability with reliable immutability and retention locking. These organizations are looking at frameworks such as Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to improve recovery time for breaches resulting from phishing and ransomware.

### GLOBAL INSIGHT

65% of the organizations took **6 days or more** to recover from ransomware attacks

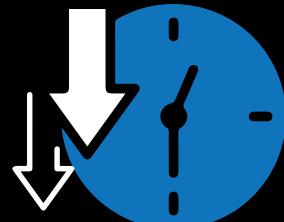
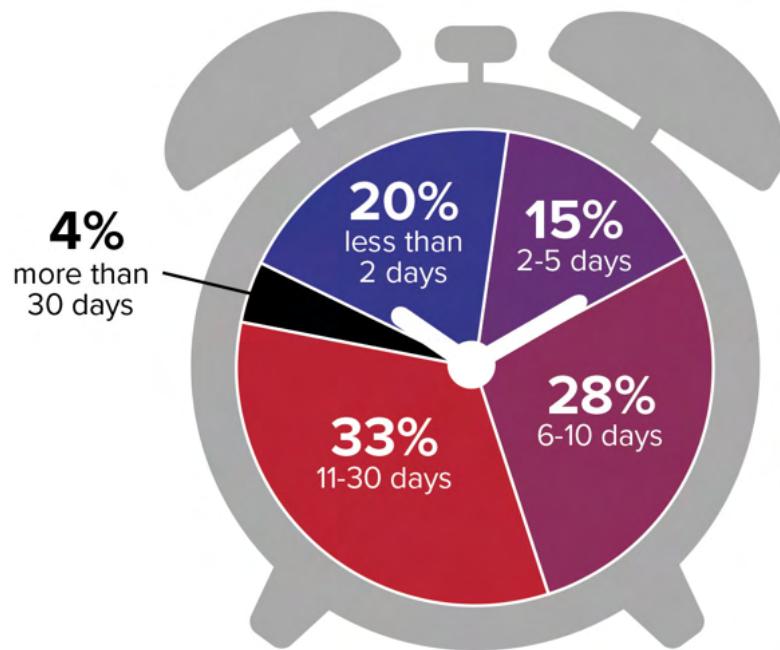


Figure 9: Downtime Due to Ransomware Attack



## Repeat Breaches

Almost one-third (29%) of all breached organizations (51% of surveyed organizations) experienced a repeat incursion within three years of the first breach. However, in many instances, the second breach did not directly correlate with the previous one. In some cases, it's the work of a new threat actor, spurred into action after learning about the original breach. This illustrates one unfortunate effect of breach publicity and the way it continues to bring harm to the enterprise. In addition, many breaches go undetected for

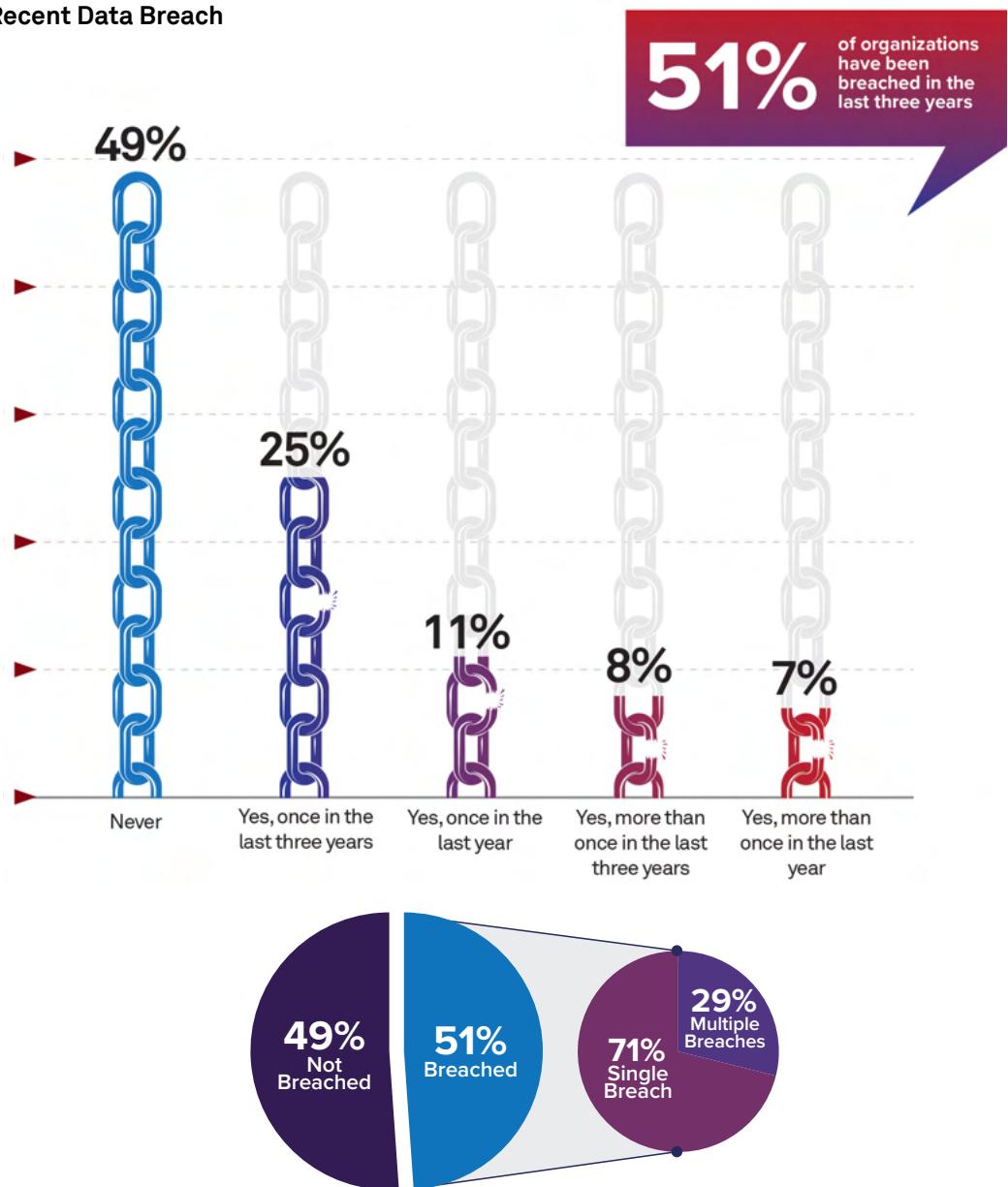
### GLOBAL INSIGHT

**29%**

of breached organizations experienced repeated incursions within 3 years

extended periods, and some are never discovered. This means organizational visibility into repeat breaches often may be obscured.

Figure 10: Recent Data Breach



## Cybersecurity Regulations

The pace of modernizing data protection laws is growing in both depth and scope. To understand the effectiveness of these regulations, we studied the data privacy laws of 23 countries (Australia, Brazil, Canada, China, Dubai, Finland, France, Germany, India, Ireland, Italy, Japan, Mexico, Norway, Poland, Russia, South Africa, Singapore, Spain, Sweden, Switzerland, UK and the U.S.) based on breach notification and cross-border data transfer clauses.

Figure 11 lists the parameters used to evaluate these clauses. For each country, a score was assigned to each parameter based on a subjective analysis of the stringency of their regulations. A weighted average helped us develop a country-specific score for data breach notifications and restrictions on overseas data transfers. We have plotted two heatmaps using these scores for breach

notification (Figure 12) and overseas data transfer (Figure 13). Out of the 23 countries analyzed, 16 countries (70%) demonstrated greater stringency in breach notification laws, while 17 countries (74%) demonstrated stringency in international data transfers. The upshot? The exposure stemming from regulatory risk is becoming even more vast and complex.

**Figure 11 : Analyzed parameters related to breach notification and data-transfer**

Focus Areas of Analysis	Parameters
Data breach notification requirements	<ul style="list-style-type: none"><li>Mandatory notification to authorities</li><li>Breach categorization</li><li>Mandatory notification to affected parties</li><li>Financial penalty if notifications are not made</li></ul>
Overseas data transfer restrictions	<ul style="list-style-type: none"><li>Consent of data subjects</li><li>Whether outside jurisdiction provides adequate protection</li><li>Binding corporate rules (BCRs)</li><li>Standard contractual clauses (SCCs)</li><li>Permission of data protection authority</li></ul>

o

Figure 12: Heat map of country-specific regulations relating to breach notifications

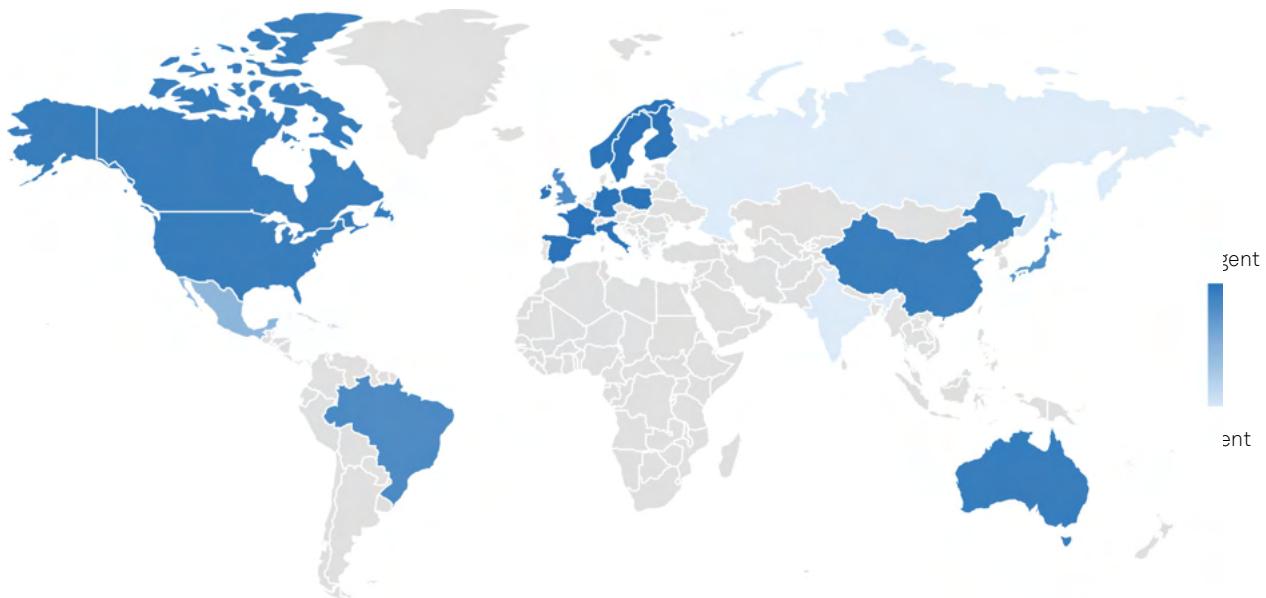
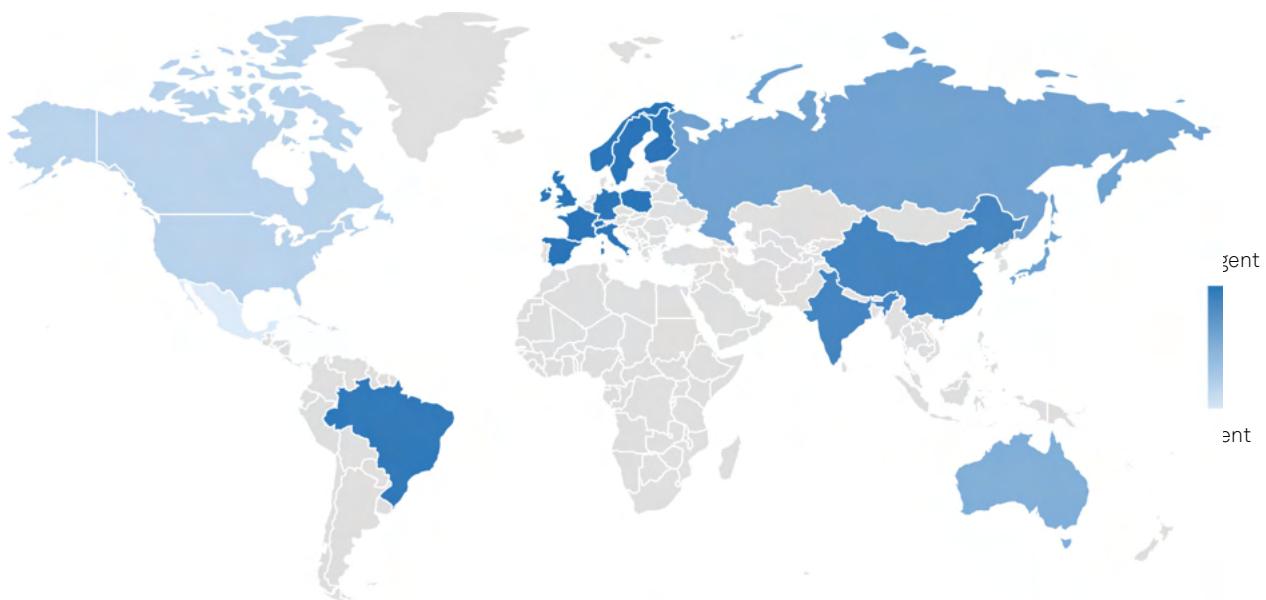


Figure 13: Heat map of country-specific regulations relating to international data transfers



#### GLOBAL INSIGHT

**70%** of analyzed countries have instigated more resilient breach notification clauses

**74%** of analyzed countries have instigated more resilient clauses on overseas data transfers

#### REGIONAL INSIGHT

**Argentina, India, Canada and the USA** are a few countries that have proposed changes to their data protection regulations through tabled bills

**FEW RECENTLY PASSED / PROPOSED**

# **REGULATORY CHANGES:**

- **Argentina's Proposed New Personal Data Protection Law**  
A new bill, DPA Resolution 119/2022, has been introduced for public consultation to replace old legislation and is modeled on the provisions of GDPR.
- **India introduces Digital Personal Data Protection Bill scrapping the old Personal Data Protection Bill**  
After public consultation, the revised data protection bill will undergo revisions before it is tabled in Parliament. The bill aims to balance the rights of individual privacy and lawful processing.
- **Canada introduces C-27, The Digital Charter Implementation Act**  
The omnibus bill is intended to strengthen existing privacy regimes and covers the development of responsible AI.
- **Indonesia's House of Representatives passed the Personal Data Protection Bill**  
The law established the rights of citizens and processing responsibilities like other data protection legislation. The law differs from other counterparts in extraterritorial scope and application.
- **America introduced a landmark federal regulation – the American Data Privacy and Protection Act**  
If passed, the bill aims to enable foundational privacy rights and bring meaningful enforcement. Conflicts with existing state laws remain to be resolved.  
**US State Privacy Legislation**  
California: California Consumer Privacy Act (effective 1 Jan 2020), CPRA eff 1 Jan 2023  
Colorado: Colorado Privacy Act (effective 1 July 2023)  
Connecticut: Connecticut Personal Data Privacy and Online Monitoring Act (effective 1 July 2023)  
Utah: Utah Consumer Privacy Act (effective 31 Dec. 2023)  
Virginia: Virginia Consumer Data Protection Act (effective 1 Jan. 2023)
- **China's Personal Information Protection Law (PIPL)**  
Since the last SOCR, China passed the Personal Information Protection Law (PIPL). Though other data security laws were in force prior to PIPL – namely the Data Security Law (DSL) and Cybersecurity Law (CSL) – PIPL is China's first comprehensive law designed to regulate and protect personal information. With the rollout of DSL and PIPL, China's laws on data security and personal information have aligned much more closely with international benchmarks. Many of PIPL's elements strongly resemble GDPR. But if you have already adopted GDPR rules, you still need to analyze the gap between GDPR and PIPL requirements. Still, adjusting to the PIPL shouldn't be too challenging.

## SECTION II

# STATE OF CYBER CAPABILITIES

This section explores the evolving trends in enterprise security governance and the management of risks through cyber capabilities in areas including the board's role, organizational design and budgeting during austerity and technical practices for the future. Damage to the brand in the aftermath of an attack continues to be a focus of attention within the C-suite. Despite austerity headwinds, security budgets have experienced a relative increase within the overall IT budget. Investments in emerging areas include assessing and mitigating risks related to generative AI. Heavy fines relating to disputes emanating from privacy regimes have plagued the industry and are driving more focus on privacy by design. We also look at the historical organizational design for security and its positioning for the future.

## Board Alignment for Cyber Governance

To allay investor concerns about the survivability of their investments, enterprise boards are focusing more on their fiduciary responsibilities directly related to cybersecurity and regulatory compliance. One way boards can achieve this is to place greater emphasis on seating directors with cybersecurity expertise. This expertise will help boards address cybersecurity decisions in a much more sophisticated and nuanced fashion. For example, a discussion of enterprise risk tolerance may sound very different if some board members have extensive security experience. This will bring more rigor within enterprises on how strategies are set and executed and how expectations and outcomes get communicated.

Governments are forcing businesses to prioritize cybersecurity risk governance, mitigation strategies, and incident reporting and response, with the help of local regulators, CERTs, and quasi-government agencies. Regulatory changes have helped to evolve the fiduciary responsibility of boards to ensure that appropriate risk management strategies are in place. In the U.S., the SEC is routinely creating new regulations, such as the proposed SEC Release No. 33-11038, which will eventually compel organizations to declare the cybersecurity expertise of board directors.

Figure 14: Board alignment to oversee cyber risks



Some 87% of organizations surveyed have a mechanism for cybersecurity board oversight. Currently, 38% of organizations surveyed have an independent board-appointed advisor. Only 32% have a designated board member with cyber risk experience and just 17% of boards have formed a cybersecurity subcommittee. As new regulations encourage boards to instigate more cyber risk governance accountability, we expect the percentage of boards with a designated board expert and/or the percentage of boards with a designated subcommittee to grow in the coming years. Well-sourced and coordinated board expertise will make business alignment, budgeting and communications more effective — both internally across the enterprise and externally with regulators.

*The percentage of boards with a designated cybersecurity expert, and the percentage of boards with a designated cyber subcommittee will continue to grow.*

## Cybersecurity Oversight by Boards

Our research also revealed how frequently enterprise management reports cyber risk to their boards. It is important to note that all the organizations surveyed have a board reporting mechanism in place but the reporting happens at varying intervals. As shown in Figure 15, 68% of executive teams report quarterly or monthly, 17% of organizations report every six months and 10% report annually. As the reporting frequency increases, the systems and processes that contribute to the quality of the reporting will need significant enhancement to ensure that what's being reported is relevant and succinct enough for board digestion.

The SOCR primary research indicates that 87% of the organizations have some mechanism for cybersecurity oversight through the board. The break-up of the 87% not only gives an indication of the status quo but also suggests a possible evolutionary path on how those numbers might look a few years from now. Currently 38% of organizations surveyed have an independent advisor appointed by the board to oversee cyber risks. Only 32% have a designated board member with cyber risk experience and the number falls to 17% for boards that have constituted a sub-committee on cybersecurity. It can be reasonably concluded that the last two figures will continue to grow at the expense of the former as new regulations force boards to take more accountability for cyber risk governance. This is good news for the security and risk leadership within enterprises, as tasks to communicate and secure alignment on strategies and budgets to support those efforts will become easier when boards have the right level of expertise.

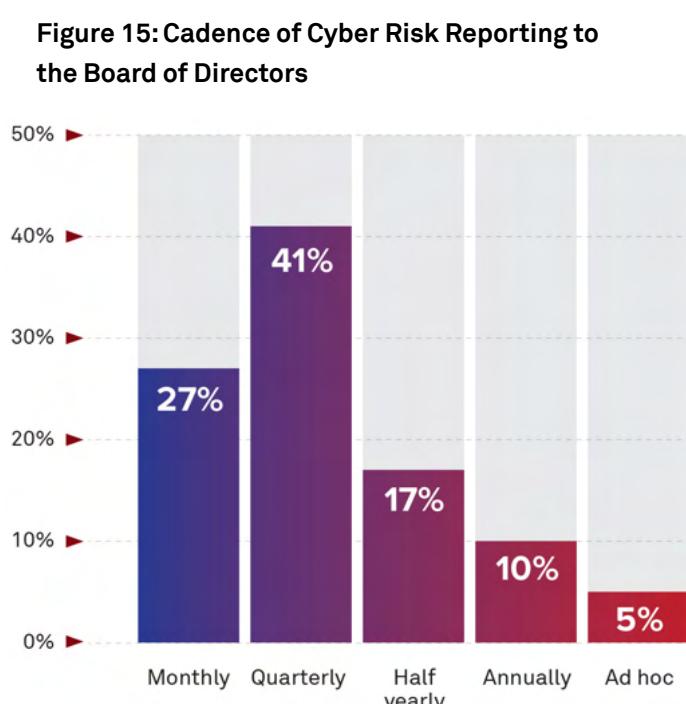
*The percentage of boards with a designated member having cybersecurity expertise or boards with a sub-committee on cybersecurity is expected to grow quickly in the coming years.*

## Cyber Risk Reporting to Boards

In the previous section, we saw how changing regulations on cyber disclosures will bring more attention within the board on cybersecurity with the right kind of experience to monitor the risks.

The frequency that a board receives cyber risk reports is also an important consideration. About 41% of surveyed organizations report cyber risk to the board every quarter, 27% report every month, 17% report semi-annually and 10% report cyber risks annually. Just 5% of organizations report cyber risk on an ad hoc basis. The most important point to note here is that all the organizations surveyed have a reporting mechanism present at different intervals during each year.

*As the frequency of cyber risk reporting to Boards increase, the systems and processes that bring timely and quality insight will need significant enhancement.*



### GLOBAL INSIGHT



of the organizations report cyber risk to executive management every quarter

### VERTICAL INSIGHT



of surveyed organizations in Communications sector report cyber risk to executive management every quarter

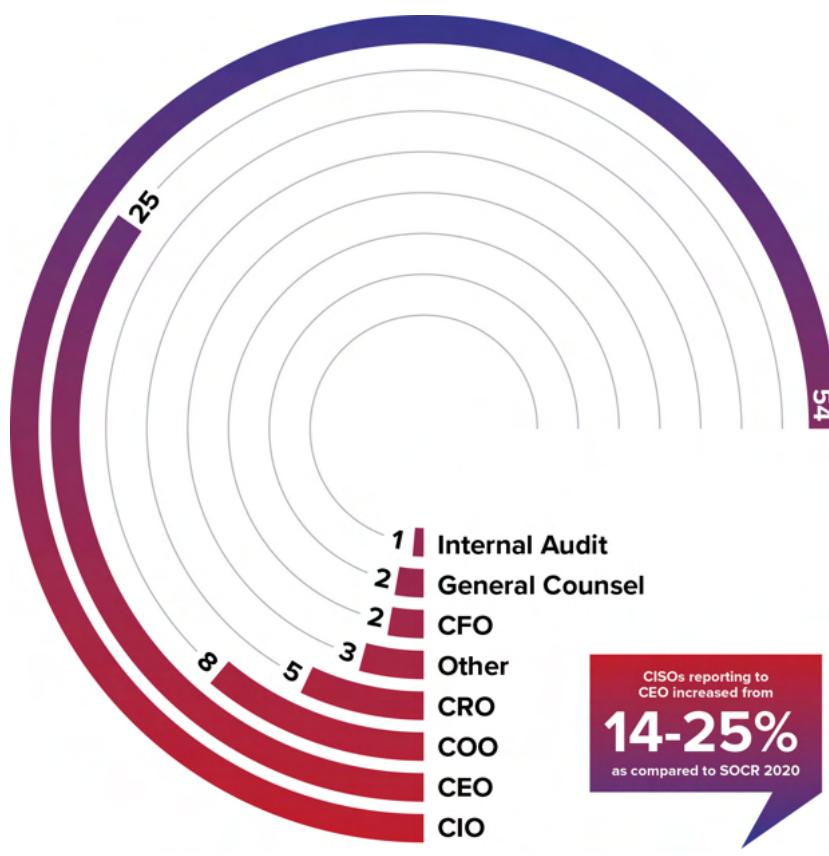
## CISO Reporting Should Align for Board Oversight

For the last decade and a half, CISOs have been largely reporting to CIOs, and this model has worked reasonably well as a fit-for-purpose approach. Infrastructure, applications, and more recently cloud ecosystems have progressively been built and managed by the IT organization. In this model, security usually gets bolted on, and while that is not the most effective approach, it's had its benefits. But for this model to work cohesively, the security structure has to be organized for the most part under the CIO.

The primary research explored the CISO reporting point: about 54% of the organizations highlighted that it was under the CIO. Interestingly, about 25% of organizations also had direct reporting to the CEO or indirect supervisory review cadences. About 20% of the reporting was spread across other C-level reporting such as the COO, CRO, CFO and CLO.



Figure 16: CISO Reporting



*Looking at the scale of change within organizations, taking cybersecurity out of the IT organization to a business aligned structure will drive multiple benefits.*

As modern enterprises continue their digital transformation journeys, organizational design strategies to manage cyber risk will undergo major revisions. Both the health of the business and the safety of its people are at stake. We've noted the importance of adding cyber expertise to the board. Properly positioning risk management responsibilities below the board level is also important. IT may not be the best fit for governing risk

mitigation strategies when they are already under pressure to deliver cutting-edge technology and keep up with IT market demands. Moving cybersecurity into a business-aligned management structure will drive multiple benefits, including better board accountability, the ability to spread risk-mitigating behavior across the organization, and the opportunity to advocate for necessary cybersecurity budgets.

#### GLOBAL INSIGHT

**54%**

of surveyed organizations' CISOs report to the CIO

**25%**

of surveyed organizations' CISOs report to the CEO

#### VERTICAL INSIGHT

**62%**

of the CISOs in Communications sector reports to CIO

**32%**

of the CISOs in ENU sector reports to CEO

### Consequences of Cyber Attacks

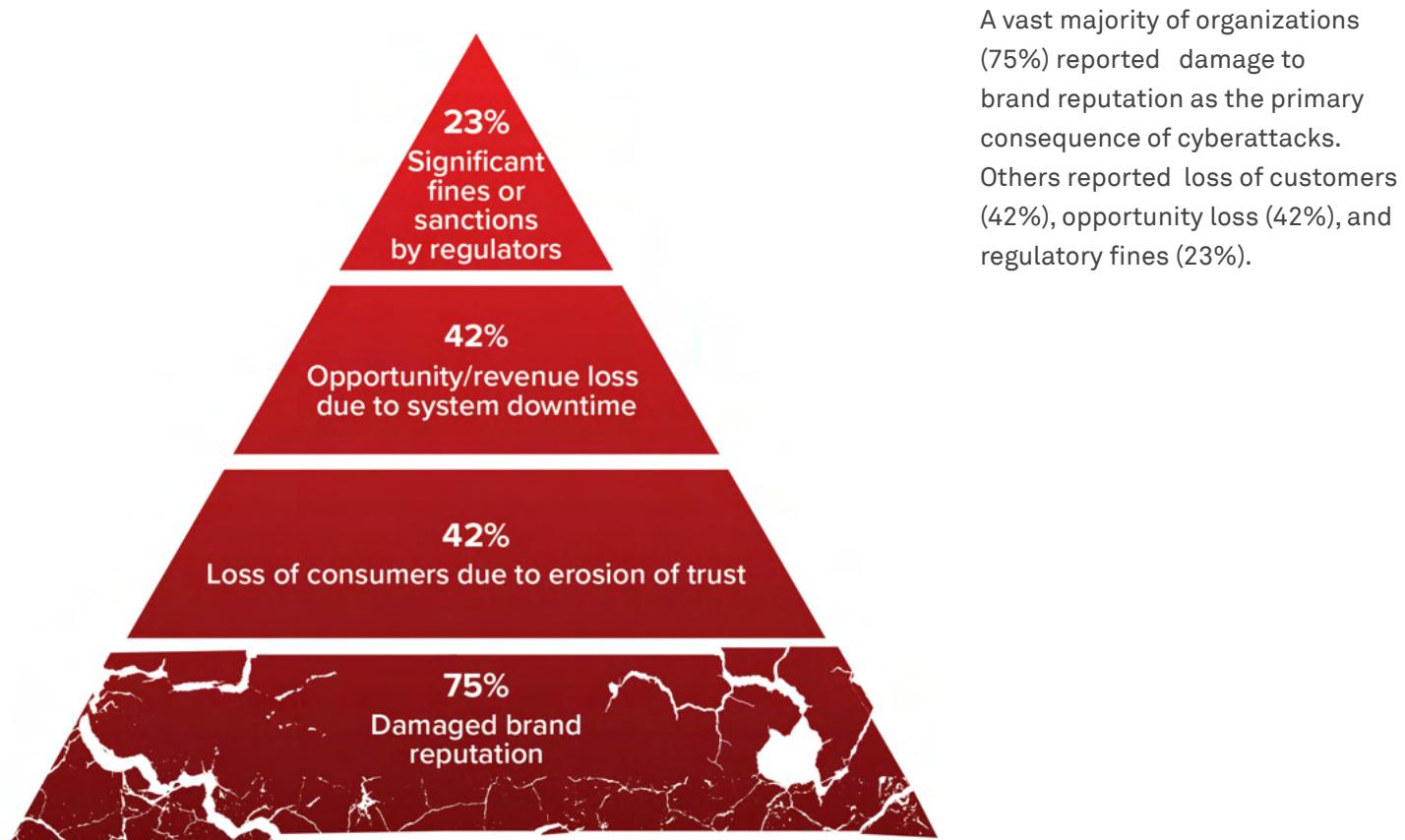
Cyber attacks in today's hyper-digital world can have serious business consequences for organizations, with both direct and indirect economic costs that go beyond what enterprises have experienced in the past. Cyber attack direct costs include regulatory fines and incident management expenses. Publicly-traded companies can suffer loss of short-term market capitalization due to share price dips. Organizations also suffer indirect economic costs after a publicly significant cyber incident, including brand damage, loss of consumer confidence and operational disruptions.

#### GLOBAL INSIGHT



**75%** of organizations highlighted damaged brand reputation as the key impact of cyberattacks

**Figure 17: Cyberattack Consequences**

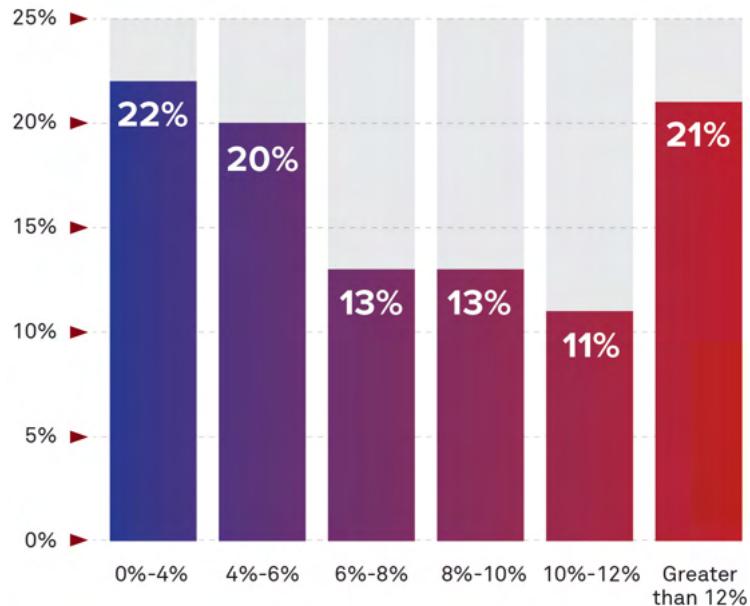


## Security Budgets & Investments

### Relative expansion despite austerity

Some 32% of organizations surveyed spent more than 10% of their annual IT budget on security, and 22% spent less than 4%. Due to the current financial headwinds, overall IT spending available at many organizations will come under pressure. CISOs will need to focus on advocating security capabilities that could help create and expand new revenue streams in areas like consumer identity.

Figure 18: Range of Percentage of Annual IT Budget allocated for Security



Businesses are investing in the following key capabilities:

- 79% identified security orchestration and automation—an important set of technologies that can help streamline costs and efficiently scale an enterprise's defenses.
- 71% called out Zero Trust networks—the emerging standard for authentication in highly networked environments.
- 67% are investing in third-party risk management and supply chain security in response to the new multi-party risk in digital transformations.
- 46% of the organizations globally have indicated OT/IoT security as priority area, however the percentage of focus on OT security spend is higher for ENU (56%) and Manufacturing (71%) sectors.

To manage costs, many organizations have invested in automation. Although automation may help to avoid simple repetitive tasks, generative AI could soon improve detection processes in the expanding cloud environment attack surfaces. CISOs are concerned about the security risks related to the increased use of generative AI. One step organizations are taking in 2023 is restricting access to public AI systems.

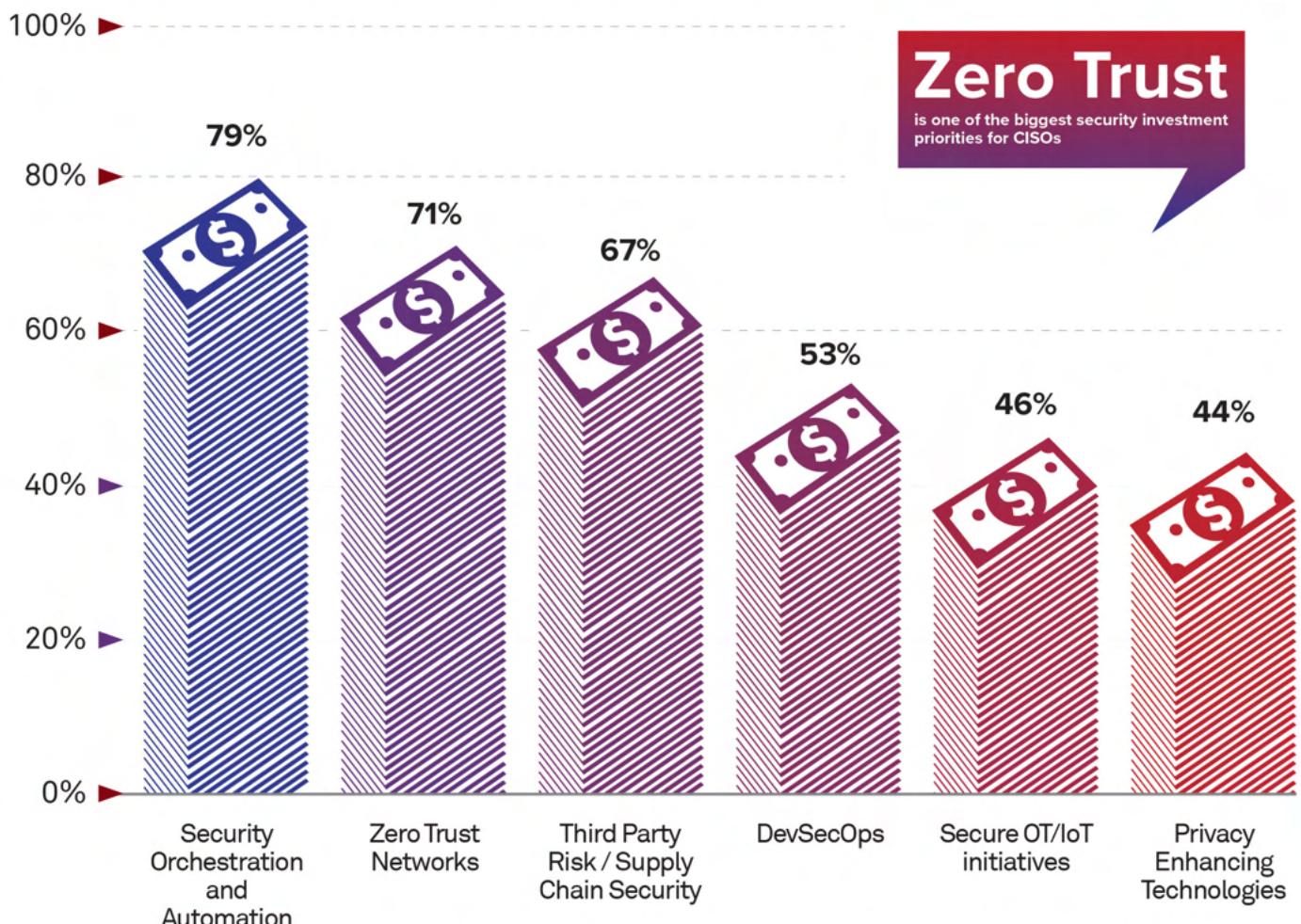
#### GLOBAL INSIGHT

**32%**

of organizations spend **greater than 10%** of their overall IT budget on **security**



Figure 19: Security investment priorities



*Although automation may help to avoid simple repetitive tasks, generative AI could soon improve detection processes in the expanding cloud environment attack surfaces.*

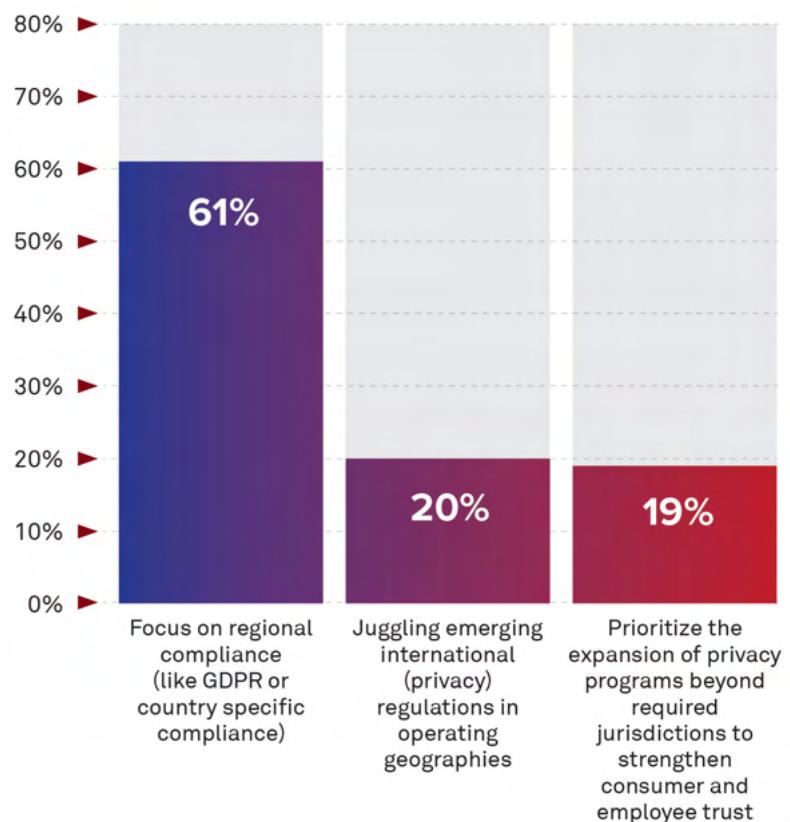
## Privacy Priorities in the Era of Record Fines

Over the last decade, data privacy has been a primary focus area for organizations due to more stringent state, country, regional and international privacy rules. Recent heavy fines on leading technology firms have put the spotlight back on the core principles of privacy and its intersection with data residency and cross-border data transfers.

As the global regulatory landscape continues to change, 61% of organizations have prioritized regional (state/country/continent) compliances, with 20% of organizations focused on international regimes. Only 19% of the remaining organizations are planning to have privacy programs focused on enhancing customer trust as opposed to meeting regulatory compliance. Data privacy is another area where AI might play a role, as AI models can be trained to assess the privacy risks of advanced PII data.

**Figure 20: Data privacy priorities**

As the global regulatory landscape continues to change, 61% of organizations have prioritized regional (state/country/continent) compliances, with 20% of organizations focused on international regimes. Only 19% of the remaining organizations are planning to have privacy programs focused on enhancing customer trust as opposed to meeting regulatory compliance. Data privacy is another area where AI might play a role, as AI models can be trained to assess the privacy risks of advanced PII data.



## Data Security Controls

Quantum computing could assist bad actors in executing sophisticated attacks on the enterprise and other digital spaces.

With the adoption of IoT and Cloud technologies and with data heavy use cases, the so-called 3 Vs of data – volume, velocity and variety – have seen a massive uptick. Businesses need to derive value from data while meeting the organization's obligations to comply with increasingly stringent privacy regulations. Security teams have been tasked with developing effective strategies for meeting these two objectives and mitigating the threat of losing intellectual property (IP) and non-public information (NPI).

Progress in quantum computing is the next frontier for security teams, representing both good and bad use cases. Quantum computing could assist bad actors in executing sophisticated attacks on core assets across enterprises, including digital currencies and blockchain apps.

Our research also explored which post-implementation data security controls provided the most value. Privileged Access Management topped the list with a score of 8.72 out of 10, followed by Automated Data Discovery & Classification (8.54), Encryption of PII/NPI (7.09) and DLP (6.93).

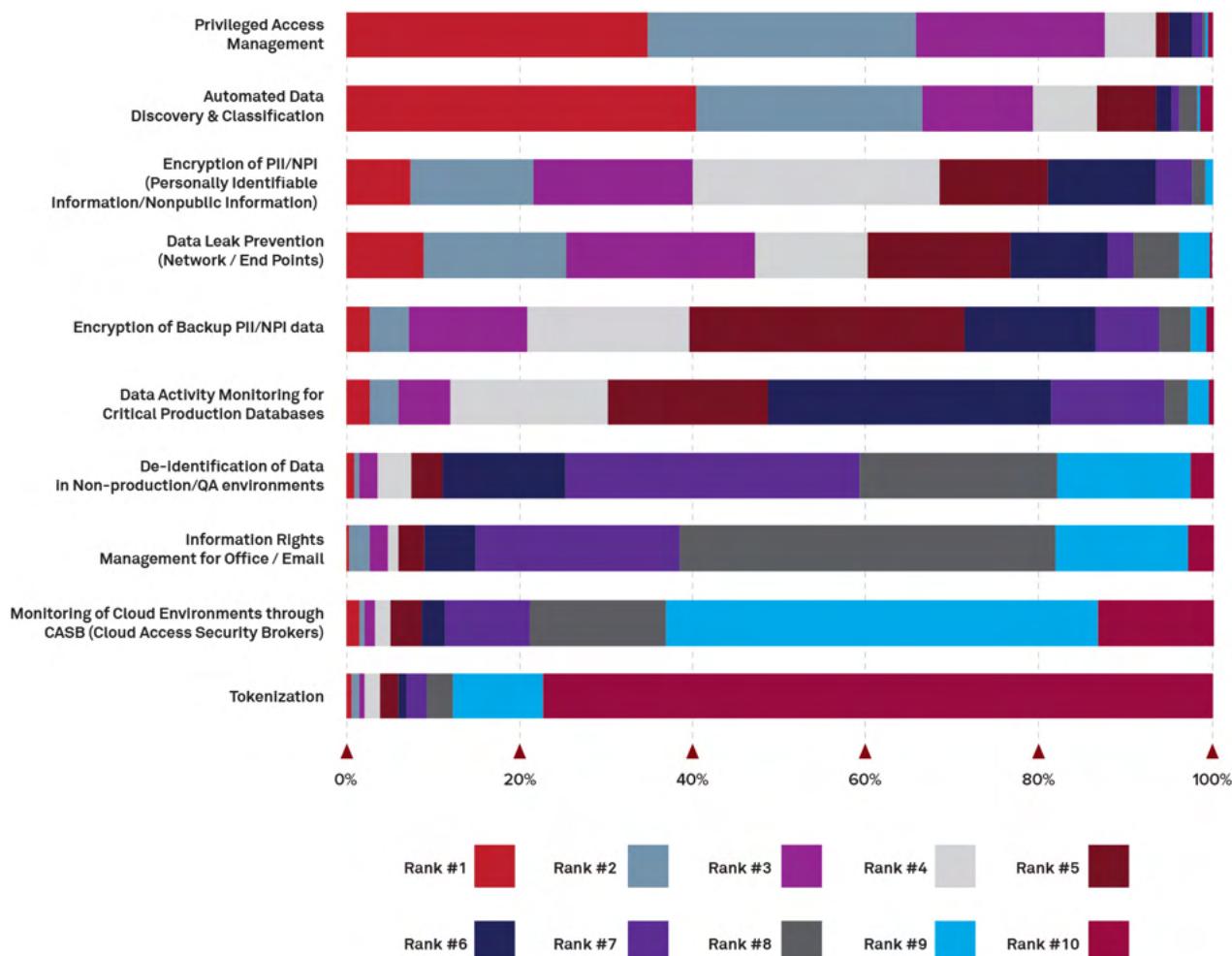
### GLOBAL INSIGHT

Privileged Access Management  
with a score of

**8.72/10**

was rated as the top  
data security control

**Figure 21:Top Data security controls**



DATA SECURITY CONTROLS	SCORE
Privileged Access Management	8.72
Automated Data Discovery & Classification	8.54
Encryption of PII/NPI (Non Public Information) Data Across the Databases	7.09
Data Leak Prevention (Network/End Points)	6.93
Encryption of PII/NPI Data	6.18
Data Activity Monitoring for Critical Production Databases	5.71
De-identification of Data in Non-production/QA Environments	3.88
Information Rights Management for Office/Email	3.54
Monitoring of Cloud Environments through CASB (Cloud Access Security Brokers)	2.76
Tokenization	1.65

## Future SOC Evolution

The Security Operations Center (SOC) of an enterprise keeps an eye on the enterprise's digital frontiers, analyzing layers of defensive controls put in place to block cyber intrusions. However, since it is impossible to build foolproof defenses, it is vital that suitable monitoring is in place to respond to attacks that break through. Many SOCs today are distributed using a "follow the sun" model with collaborative teams across geographies using a shared technology stack in an outsourced model.

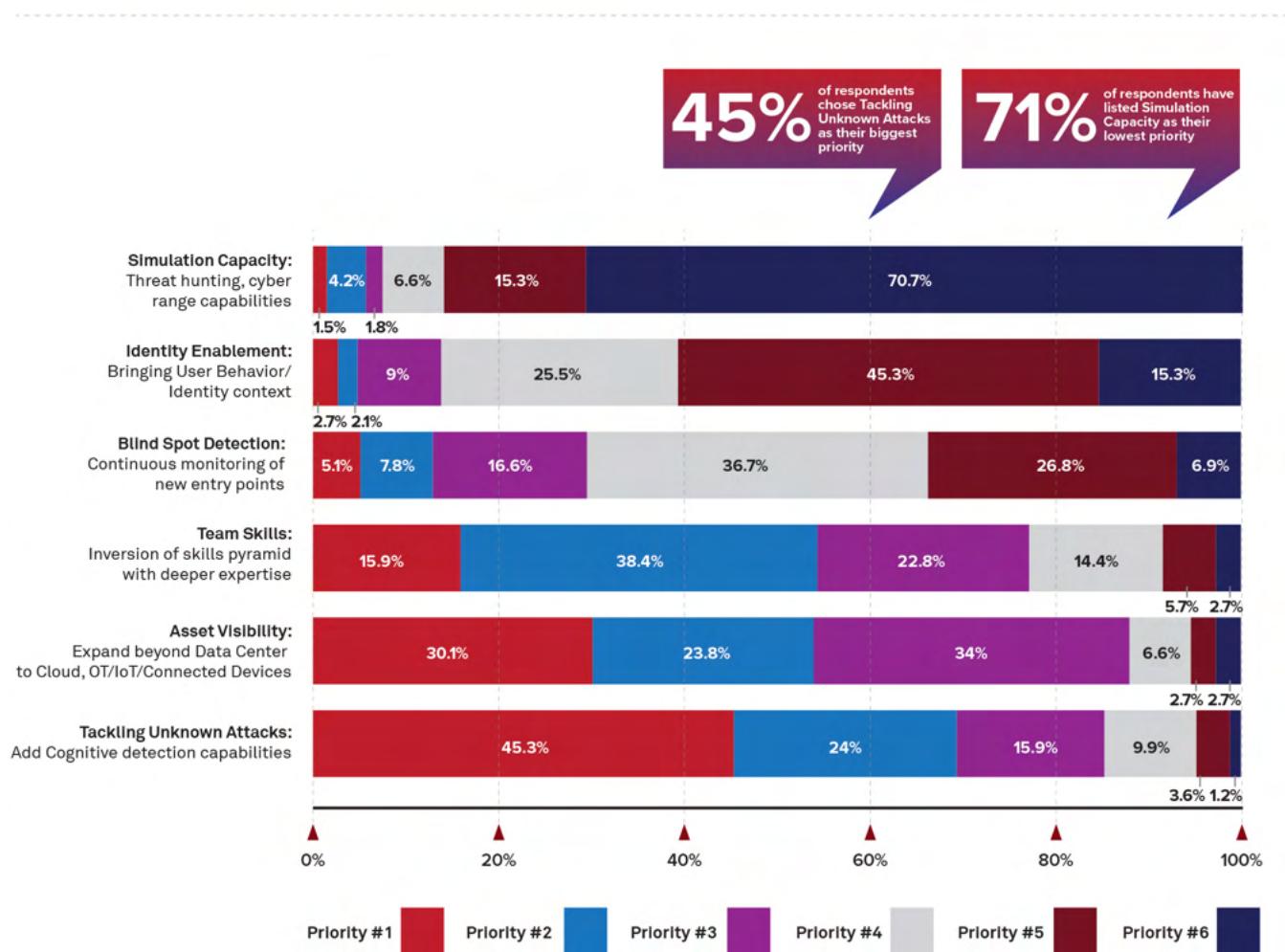
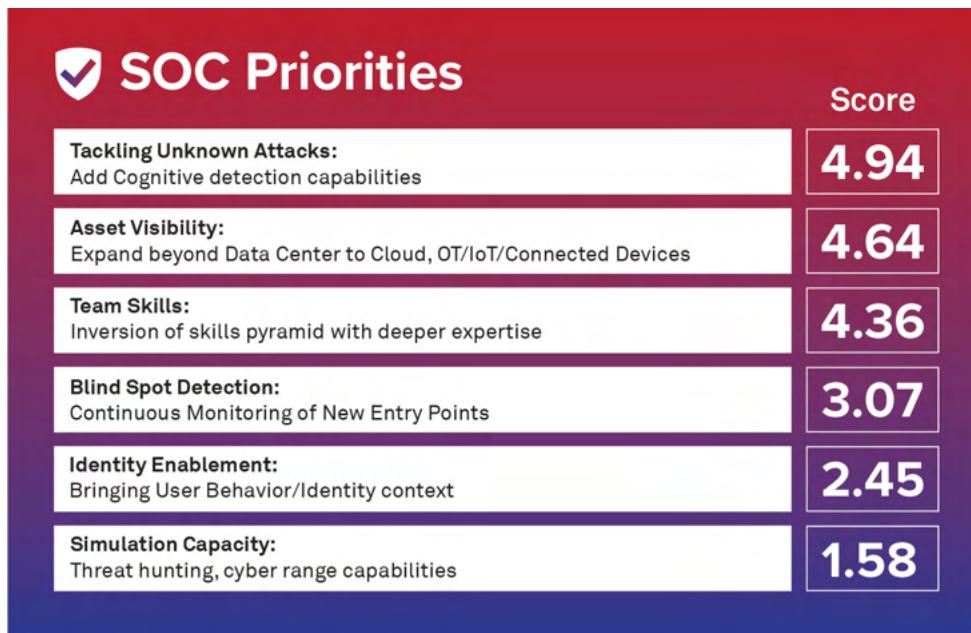
Within its SOC, an enterprise needs the right blend of security operations, full stack engineering, contextual threat intelligence, noiseless detection, threat hunting and incident response.

### GLOBAL INSIGHT



of organizations highlighted Tackling Unknown attacks through additional cognitive detection capabilities as a priority for their SOCs

Figure 22: Top Priorities for the Future SOC



## Addressing OT Security Risks

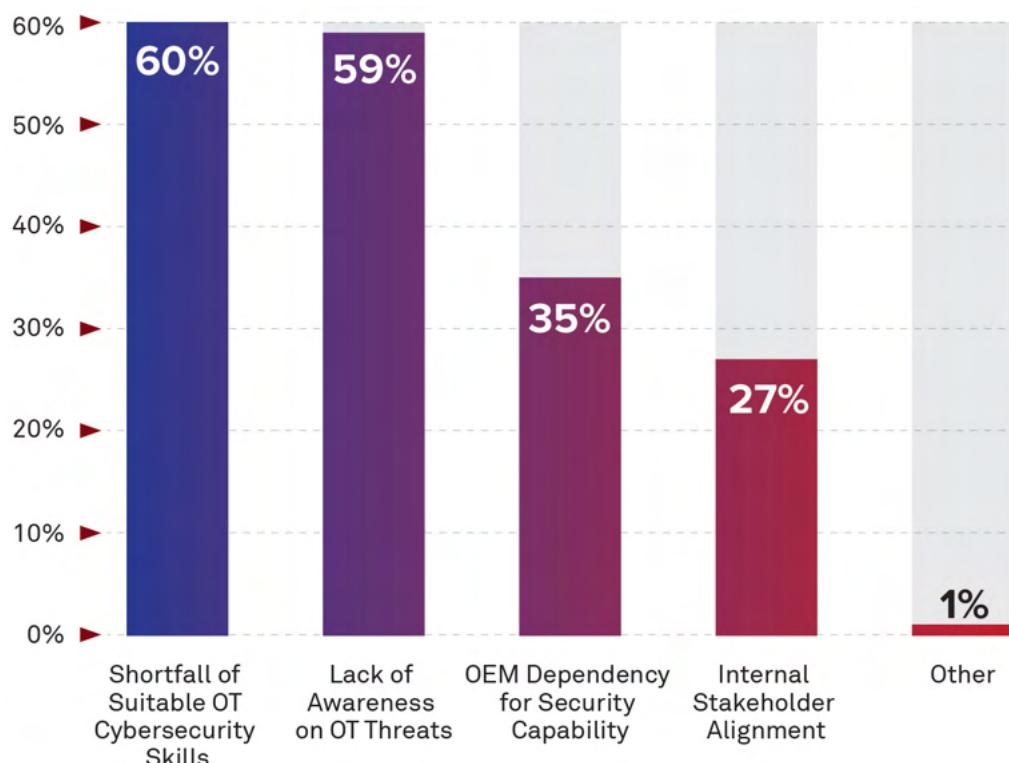
For decades, Operational Technology-heavy industries have kept their critical infrastructure segregated physically and organizationally in the hands of domain operators. With the advent of digitization, the need to connect these systems with regular IT environments has grown to meet the demand for real-time data. But this has created a tech feedback loop. Connecting the OT environments to the IT environment breaks the conventional air gap and expands the attack surface of critical infrastructure providers making them targets for nation-state bad actors. Successful OT security implementations depend on good partnerships between OT and IT teams that leverage industry best practices.

Successful OT security implementations depend on good partnerships between OT and IT teams that leverage industry best practices.

Of the surveyed organizations, 60% cited a “Shortfall of OT Cybersecurity skills” as a key barrier to addressing OT security risks. This is followed by 59% who listed lack of awareness of OT threats as their major barrier. Close to 35% highlighted their dependency on OEMs in the OT space for security capability.



Figure 23: Barriers to address OT Security Risks

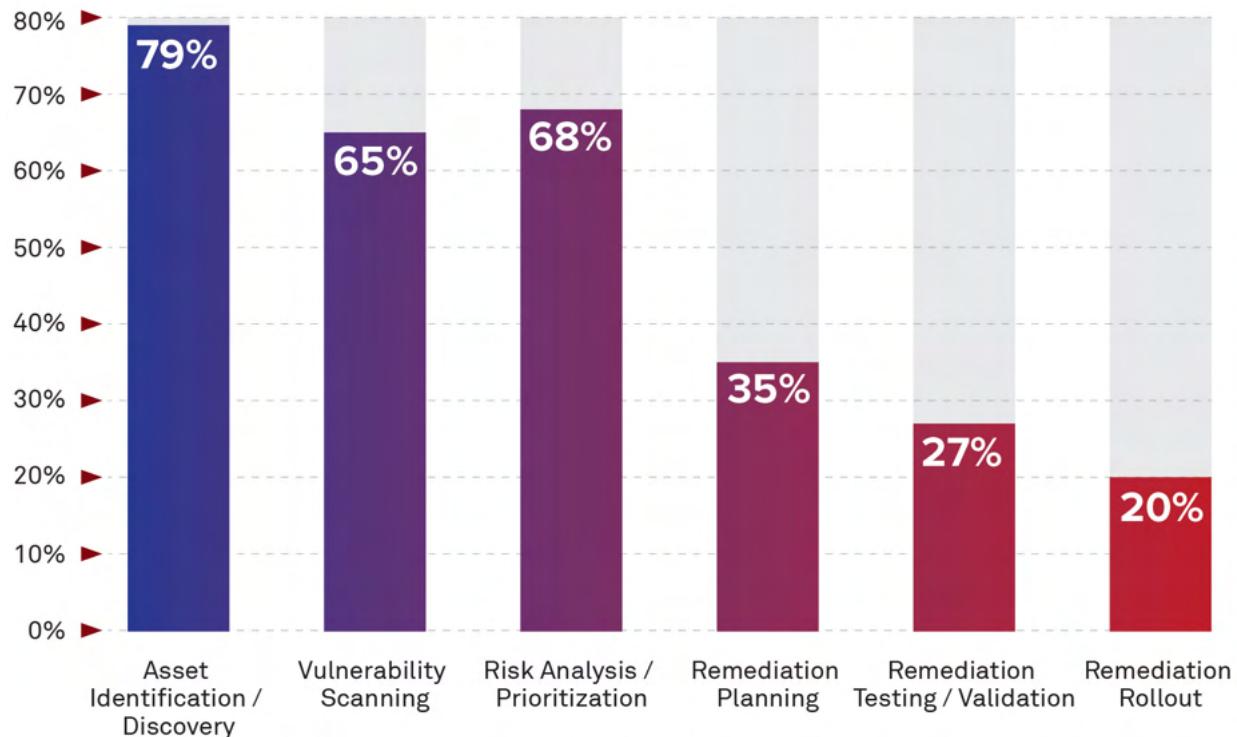


## Prioritizing Cyber Hygiene

Cyber hygiene is a foundational issue that security professionals have been grappling with for ages. Despite technological advancements, attackers continue to use timeless tactics to exploit weaknesses in software and infrastructure stemming from poor cyber hygiene. Even the tools for scanning and assessment in this space are commoditized, and many of the methods employed are standardized and outdated. This results in less-than-ideal life cycles in many organizations, with huge imbalances between vulnerability identification and post-identification remediation. Some vulnerabilities may be left aging for months, creating glaring weaknesses in the system.

o

**Figure 24: Most Challenging Phases of Vulnerability Lifecycle Management**



Despite generational technology leaps, attackers have continued to use timeless tactics for exploiting weaknesses in software and infrastructure that stem from bad cyber hygiene.

In our research, organizations identified various stages of the vulnerability management lifecycle. Asset identification and discovery topped the list at 79% but can be considered a broader problem for IT at large. Risk analysis prioritization was next at 68% followed by vulnerability scanning at 65%. Solving these top three vulnerability lifecycle management challenges enables security teams to greatly enhance their knowledge of attack paths, exploits in the wild, and the availability of patches or compensating controls to minimize risks by remediating prioritized weaknesses.

## IAM Priorities

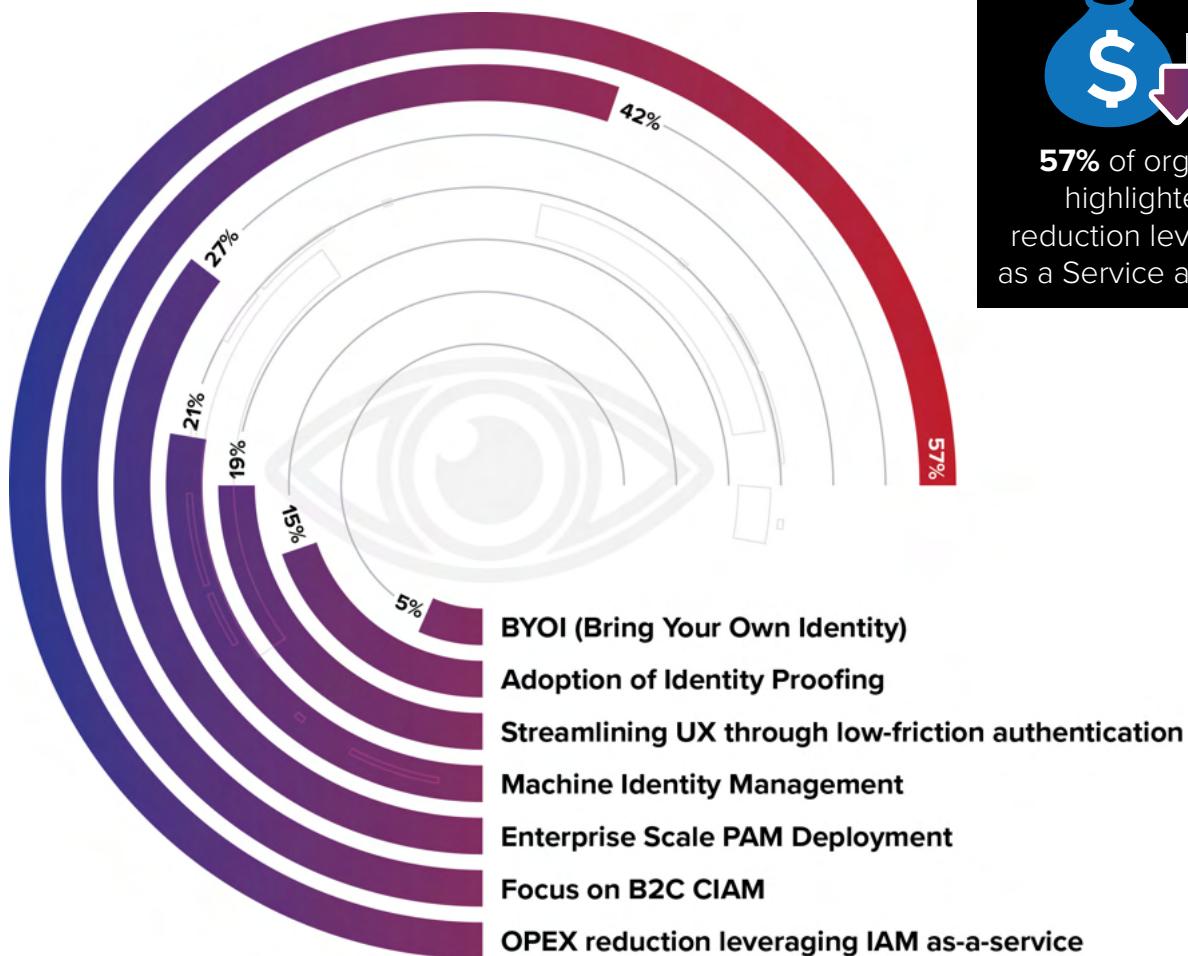
In 2023, identity is the new perimeter of cybersecurity. The digital nature of today's businesses has extended the boundaries of identity management to cut across employees, partners and suppliers. But growth in the different classes of IT assets has led to a corresponding growth of identities to sustain these environments. The emergence of non-human identities—think IoT devices—and the impending expansion in identities associated with generative AI ecosystems has made the landscape extremely complex.

Cost reductions through OpEx savings in IAM operations and a focus on digital transformation initiatives involving Customer IAM (CIAM) will help IAM strategies become more business-aligned.

According to our research, 57% of the respondents highlighted OpEx reduction leveraging IAM-as-a-Service as a key priority. Revenue generation by modernizing CIAM was cited by 42% of the surveyed organizations. OPEX reduction helps the IT and Security organizations align to any austerity pressures, while CIAM helps the business establish future revenue streams using security as a key enabler.



Figure 25: Identity Access Management priorities



## Integrating Security into Business Transformation

Security technology capabilities such as low latency connectivity, sensorial awareness, pervasive data, and large language-based cognition are driving significant transformations in the way the world does business. This is particularly relevant in verticals such as Healthcare, Manufacturing, Banking & Financial Services, Retail, Transportation, Consumer Goods and Energy & Utilities. However, many of these transformative efforts do not factor in cyber risks at the inception stage, which leads to the escalation of enterprise risk, project delays, cost overruns and a less-than-satisfying end-user experience.

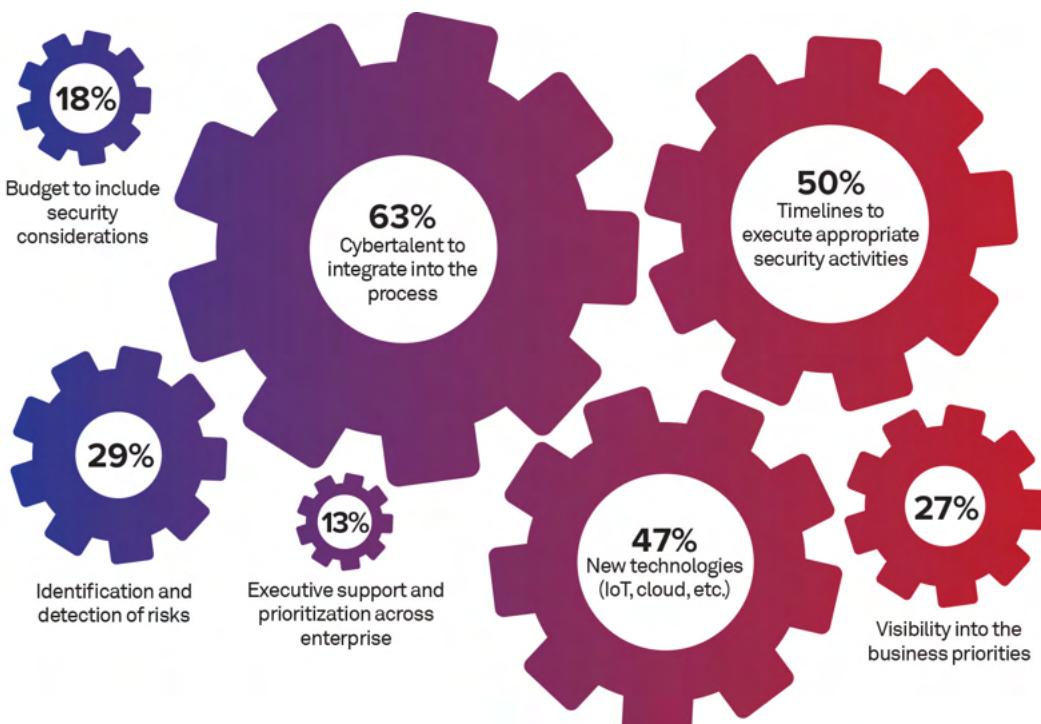
Digital transformation efforts are often accompanied by a lack of awareness of risks due to additional attack surfaces emanating from new digital assets. This sometimes results in a less-than-adequate effort to bolt on disparate security solutions for a quick fix. But successful risk management requires a strategy-first approach with business-aligned, integrated solutions. To get there, organizations must overcome common barriers.

According to our research, a majority of the respondents (63%) believe that the biggest barrier to integrating security into business transformation is the lack of proper cyber talent, followed by stricter timelines to execute appropriate security activities (50%) and the rise of new-age technologies (47%).

### GLOBAL INSIGHT

**63%** of organizations consider lack of cyber talent as the biggest barrier in integrating security into business transformation

Figure 26: Barriers to Integrating security into Business Transformation





## Characteristics of a Modern Cyber Professional

The cybersecurity talent gap has put tremendous pressure on security leadership and human resource teams to find new talent, limit security team attrition and manage operational costs. The skills required for cybersecurity management range from deep tech expertise in areas like threat hunting, to forensics, and regulatory and legal knowledge. As business technology stacks evolve, the pressure on cybersecurity teams increases to understand the latest technologies and uncover weaknesses. Cloud, IoT, AI/ML, and generative AI are just a few examples of new technologies that have required security teams to track and contain related risks. Domains such as OT Security have required cybersecurity professionals to step into previously unexplored roles and territories.

The skills required for cybersecurity management range from deep tech expertise in areas like threat hunting, to forensics, and regulatory and legal knowledge.

Because so much importance is placed on cybersecurity talent, our research employed a ranking process that prioritized the skills and characteristics CISOs were looking for when recruiting and hiring cybersecurity professionals.

Technical aptitude was the most important skill driving the hiring process, with a score of 6.3 out of 7, followed by cybersecurity certifications at 5.2. Relevant work experience in the cybersecurity field came in third at 5.1. Note that respondents chose core cybersecurity knowledge and skills over softer characteristics such as intellect, business knowledge and interpersonal skills. To overcome the challenges around gaining alignment, overcoming conflicts, and finding

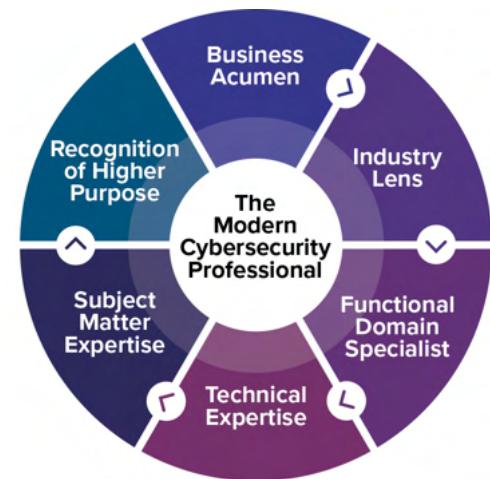
common ground, cyber professionals must have these soft skills along with their technical area of expertise, suggesting that industry professionals may need to modify their over-reliance on tech expertise when evaluating new hires.

#### GLOBAL INSIGHT

**Technical aptitude** is the topmost priority while hiring

o

**Figure 27: What CISOs Look for in modern cybersecurity professionals?**



## Confidence in Cyber Controls

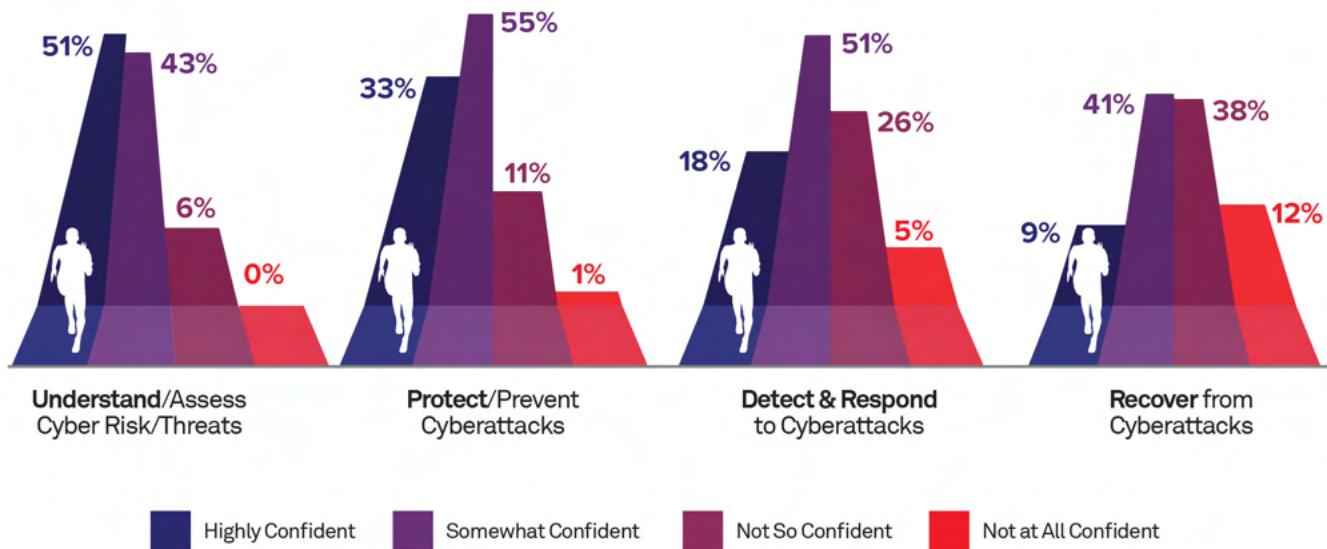
Cybersecurity is clearly at a crossroads. For more than a decade, the industry has been battling attacks that keep increasing in frequency and impact. The enterprises' understanding of cyber risk is getting better with more robust assessments and with budget increases for laying down controls that were primarily preventive in nature. Layers of detection are being added to catch attacks that cut through the defenses. But despite advances made in technologies like AI/ML, cyber hygiene continues to be less than desirable, meaning many breaches occur without the attackers needing to exponentially advance their sophistication. Now that attackers have greater access to generative AI and machine learning (ML), they are poised to raise the technical sophistication bar.

As a result, security professionals are not exactly brimming with confidence in their ability to understand cyber risks. Just 51% of the surveyed organizations are highly confident about their understanding of cyber risks. Only 18% of organizations are highly confident in their ability to detect attacks that find their way

around preventive controls. And here's the key data point: only 9% of organizations are highly confident about their preparedness to quickly recover from a significant attack.

o

**Figure 28: Confidence in cyber controls**



#### GLOBAL INSIGHT



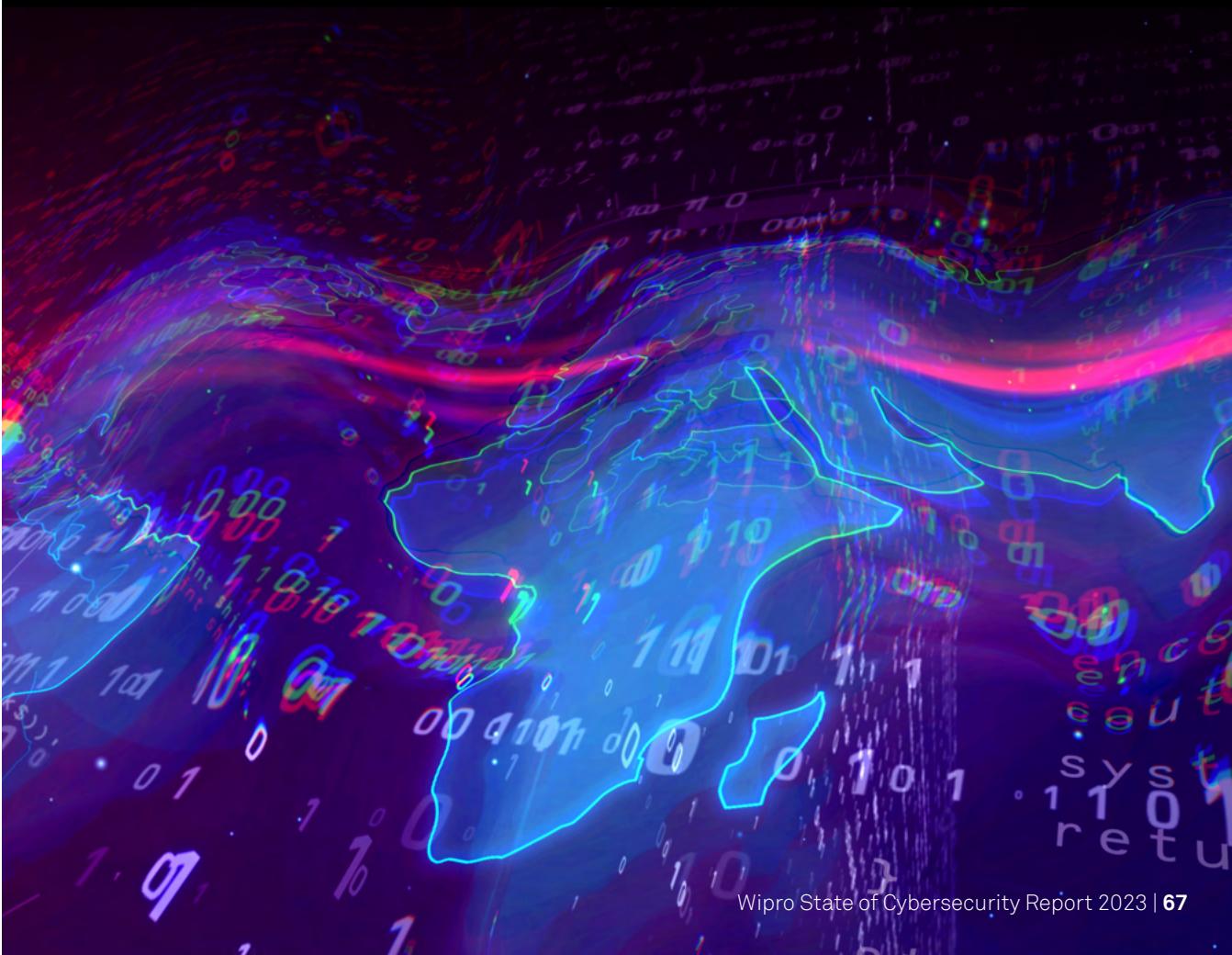
**51%** of organizations are highly confident about their understanding of cyber risks



but only **9%** are highly confident about quickly recovering from a significant attack

STATE OF

# COLLABORATION





*Organizations are exposed to risk by failing to include and manage key stakeholders —both internal and external — in the enterprise’s security ecosystem.*

This section examines the practical barriers to information sharing with stakeholders both inside and outside the so-called ‘four walls of the enterprise.’ A critical factor for cyber resilience success is collaboration among all stakeholders and the ability to manage risk from third-party suppliers.

We also look at the value of running simulation exercises as a way to prepare for inevitable attacks, and the importance of engaging the board in these exercises. Even the most robust risk management programs will sometimes fail, and that’s why cyber insurance is a critical component. But it’s important to understand the limitations of cyber insurance, which does not cover some major enterprise risks.

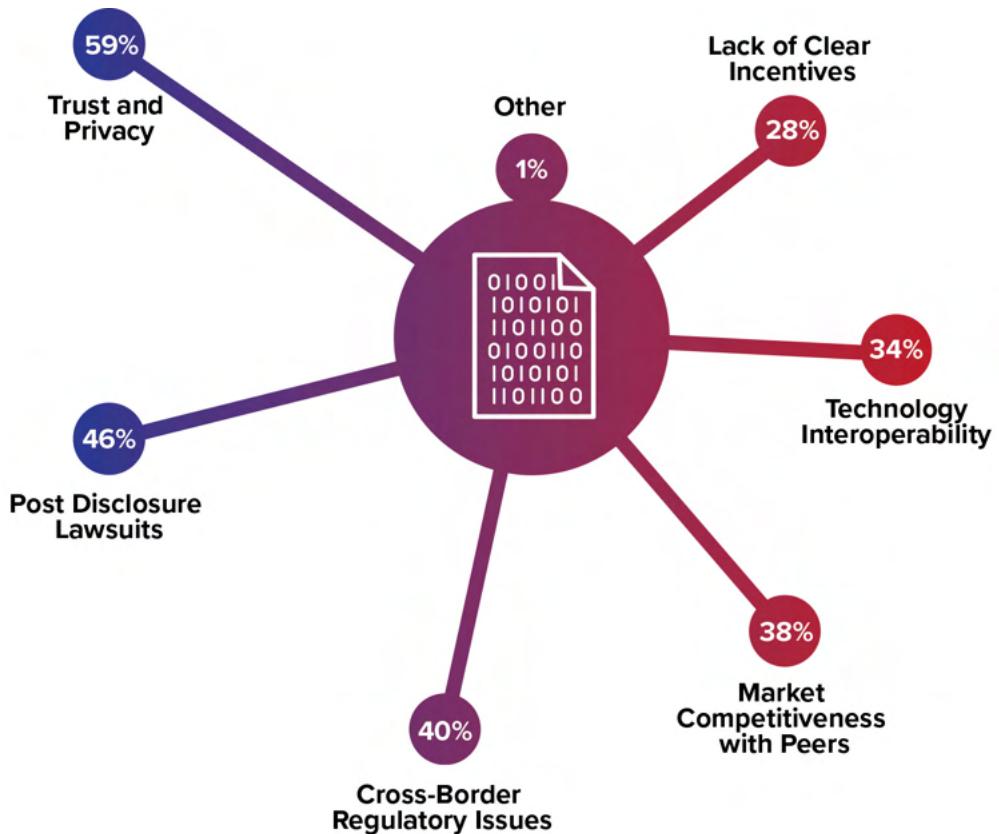
## Barriers to Threat Intelligence Sharing

*While collaboration is generally regarded positively in the cybersecurity world, there are practical and legal reasons for the enterprise to limit open information sharing.*

Organizations build threat information sharing relationships solely to prevent cyberattacks. The shared information could be details about the latest attacks, identification of potential cyber actors, strategies and tactics used by those cyber actors and the company’s response to attacks and breaches. There are many benefits to exchanging cyber threat intelligence information, including speeding up threat awareness, developing new technology for averting and responding to cyberattacks and reducing long-term cybersecurity expenditures. But while collaboration is generally regarded positively in the cybersecurity world, there are practical and legal reasons for the enterprise to limit open information sharing.

We asked our survey respondents what stops them from sharing intelligence information with external stakeholders.

Figure 29: Challenges in Threat Intel Sharing



The top three reasons were:

- Trust and privacy
- Potential lawsuits (after disclosure of an attack), and
- Cross-border regulatory issues

By far, trust and privacy is the top barrier to information sharing, with close to 59% of the respondents saying it's their biggest concern. Organizations often fear that disclosing any cyberattack might cause huge damage to their reputation and strike fear among their customers, ultimately impacting their financials. As we observed earlier in this report, damage to one's brand is the top concern of 75% of all CISOs.

#### GLOBAL INSIGHT

**59%**

organizations consider '**Trust and Privacy**' as the major challenge in sharing threat intel

## Third-Party Collaboration

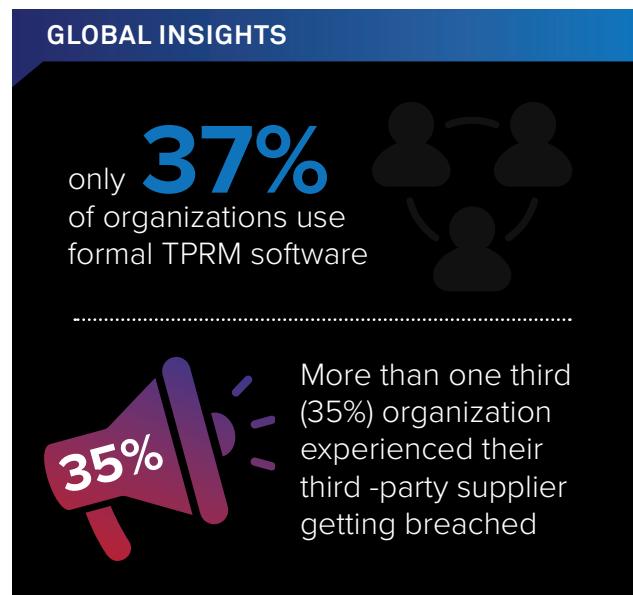
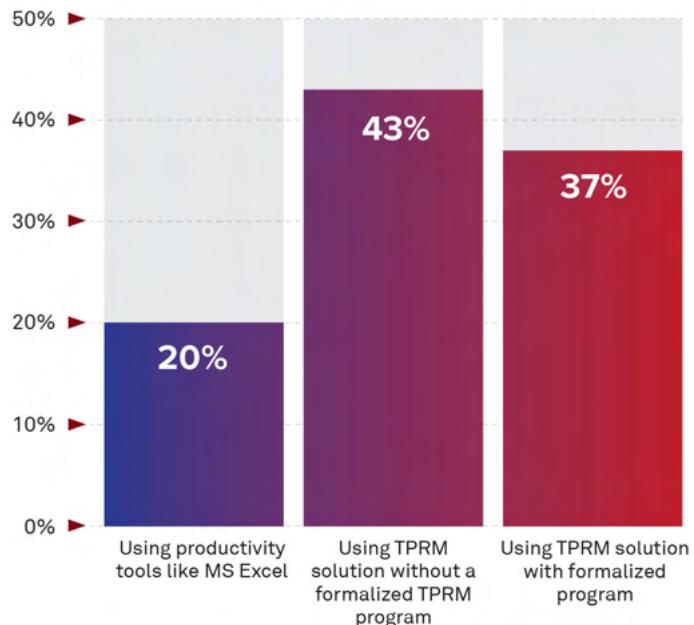
*Considering the pace that organizations are expanding physically and digitally, third-party collaboration has become a necessity—but it presents strategic, operational, technological and regulatory challenges.*

Third-party collaboration is generally favored by organizations that rely on multiple vendors and partners to provide more efficient and agile services to their stakeholders. These collaborations also help organizations expand their revenue base by serving wider geographical areas. Considering the pace that organizations are expanding physically and digitally, such third-party collaboration has become a necessity. But it presents strategic, operational, technological and regulatory challenges due to a number of risk factors across the third-party ecosystems, including:

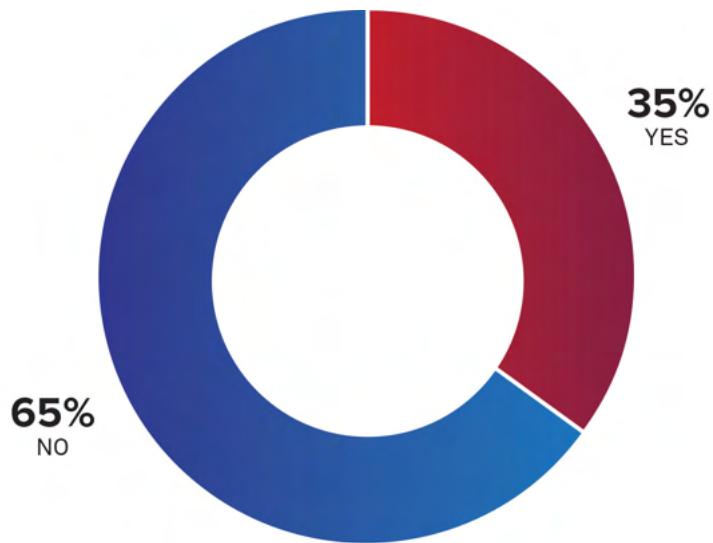
- Outdated software patches
- Non-compliance to data regulatory requirements such as the General Data Protection Regulation (GDPR).
- Fines resulting from regulatory non-compliance
- Insufficient security verifications
- Infrequent audits to check cybersecurity posture

According to our research, 35% of organizations said their third-party suppliers reported a security breach in the past year. About 37% of organizations use formal Third-Party Risk Management (TPRM) software that conducts automatic third-party screenings and risk-area decision tracking. However, 20% of survey respondents still use basic tools like Microsoft Word and Excel to keep track of third-party cyber risks. As noted in the executive summary, third-party supplier reporting needs to be better managed.

**Figure 30: Approaches to Third-Party Risk Monitoring**



**Figure 31: Organizations Whose Third-Party Suppliers Experienced Security Breaches**



## Simulation Exercises

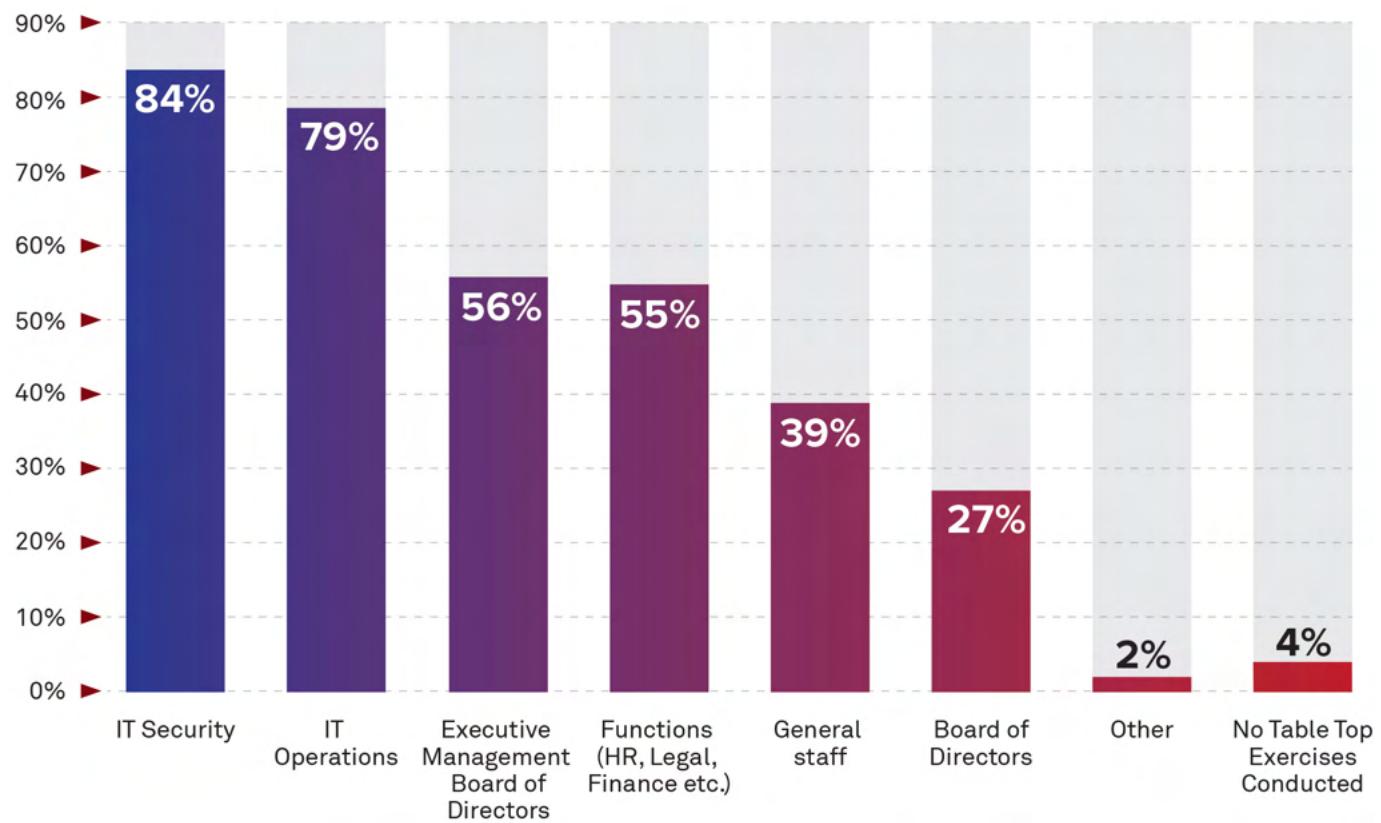
Only 4% of respondents had not conducted any sort of crisis or incident response exercises in the last two years. Only 27% of the surveyed organization witnessed participation of board members in simulation exercises.

One of the most impactful ways for an organization to diagnose its cybersecurity defenses is to conduct cyberattack simulation exercises. Simulations can train employees to respond effectively in different scenarios to minimize damages.

Well-planned and orchestrated cyberattack simulation exercises can also help organizations discover the blind spots in their systems that threat actors may use as breach access points. Simulations can also help analysts look at the organization's cybersecurity posture from the attacker's point of view, giving them greater insight into how to secure their devices, systems and networks.

In our survey, we learned that in the last two years, 84% of the respondent organizations had conducted tabletop exercises that included the IT Security team, and 79% of the organizations involved the IT operations team. This shows that major organizations are proactively developing a

Figure 32: Stakeholder Engagement in Cybersecurity Simulation Exercise



```

<ul class="menu__list">
  <li class="menu__item menu__item--home">
    <div class="menu__item-inner"><a href="/" data-metrics-action="click npr logo">Home</a></div>
  </li>
  <li class="menu__item menu__item--news menu__item--has-submenu" data-metrics-hover="toggle news drawer">
    <div class="menu__item-inner">
      <a href="/sections/news/" data-metrics-action="click news"><News</a>
      <button class="menu__toggle-submenu" data-metrics-action="toggle news drawer">Expand/collapse submenu for News</button>
    </div>

    <ul class="submenu submenu--news">
      <li class="submenu__item"><a href="/sections/national/" data-metrics-action="click national">National</a></li>
      <li class="submenu__item"><a href="/sections/world/" data-metrics-action="click world">World</a></li>
      <li class="submenu__item"><a href="/sections/politics/" data-metrics-action="click politics">Politics</a></li>
      <li class="submenu__item"><a href="/sections/business/" data-metrics-action="click business">Business</a></li>
      <li class="submenu__item"><a href="/sections/health/" data-metrics-action="click health">Health</a></li>
      <li class="submenu__item"><a href="/sections/science/" data-metrics-action="click science">Science</a></li>
      <li class="submenu__item"><a href="/sections/technology/" data-metrics-action="click technology">Technology</a></li>
      <li class="submenu__item"><a href="/sections/codeswitch/" data-metrics-action="click race & culture">Race & Culture</a></li>
    </ul>
  </li>
  <li class="menu__item menu__item--arts-life menu__item--has-submenu" data-metrics-hover="toggle arts drawer">
    <div class="menu__item-inner">
      <a href="/sections/arts/" data-metrics-action="click arts & life">Arts & Life</a>
      <button class="menu__toggle-submenu" data-metrics-action="toggle arts drawer">Expand/collapse submenu for Arts & Life</button>
    </div>

    <ul class="submenu submenu--arts-life">
      <li class="submenu__item"><a href="/books/" data-metrics-action="click books">Books</a></li>
      <li class="submenu__item"><a href="/sections/movies/" data-metrics-action="click movies">Movies</a></li>
      <li class="submenu__item"><a href="/sections/television/" data-metrics-action="click television">Television</a></li>
      <li class="submenu__item"><a href="/sections/pop-culture/" data-metrics-action="click pop culture">Pop Culture</a></li>
      <li class="submenu__item"><a href="/sections/food/" data-metrics-action="click food">Food</a></li>
      <li class="submenu__item"><a href="/sections/art-design/" data-metrics-action="click art & design">Art & Design</a></li>
      <li class="submenu__item"><a href="/sections/performing-arts/" data-metrics-action="click performing arts">Performing Arts</a></li>
    </ul>
  </li>
  <li class="menu__item menu__item--music menu__item--has-submenu" data-metrics-hover="toggle music drawer">
    <div class="menu__item-inner">
      <a href="/music/" data-metrics-action="click music">Music</a>
      <button class="menu__toggle-submenu" data-metrics-action="toggle music drawer">Expand/collapse submenu for Music</button>
    </div>
  </li>
  <li class="menu__item menu__item--tiny-desk">
    <a href="https://www.npr.org/series/tiny-desk-concerts/" data-metrics-action="click tiny desk">Tiny Desk</a>
  </li>
  <li class="menu__item menu__item--allsongs">
    <a href="https://www.npr.org/sections/allsongs/" data-metrics-action="click all songs considered">All Songs Considered</a>
  </li>
  <li class="menu__item menu__item--music-news">
    <a href="https://www.npr.org/sections/music-news/" data-metrics-action="click music news">Music News</a>
  </li>
  <li class="menu__item menu__item--music-features">
    <a href="https://www.npr.org/sections/music-features/" data-metrics-action="click music features">Music Features</a>
  </li>

```

better cybersecurity posture through simulation. We've discussed the importance of engaging the board in all aspects of cybersecurity strategic planning, and this includes board participation in simulation exercises. But almost three-quarters (73%) of surveyed organizations did not include board directors in their exercises. Board involvement is a golden opportunity for companies to improve collaboration efforts. Only 27% of the surveyed organization witnessed participation of board members in simulation exercises. This may be the one place where many organizations can improve their ability to collaborate. Although tabletop exercises are a quick way to check for cybersecurity preparedness, full-scale functional simulations can give better insight into what a cybersecurity posture looks like. A functional simulation with the collaboration of all relevant teams—including the board—will help analyze potentially negative impacts in a real-time setting, which in turn helps to optimize responses as part of an enterprise's incident response playbook.

## GLOBAL INSIGHT

**27%**

of organizations showing active board participation in cybersecurity simulation exercises

## SECTORAL INSIGHT

Top three sectors witnessing highest participation of board members in cyber simulation are:

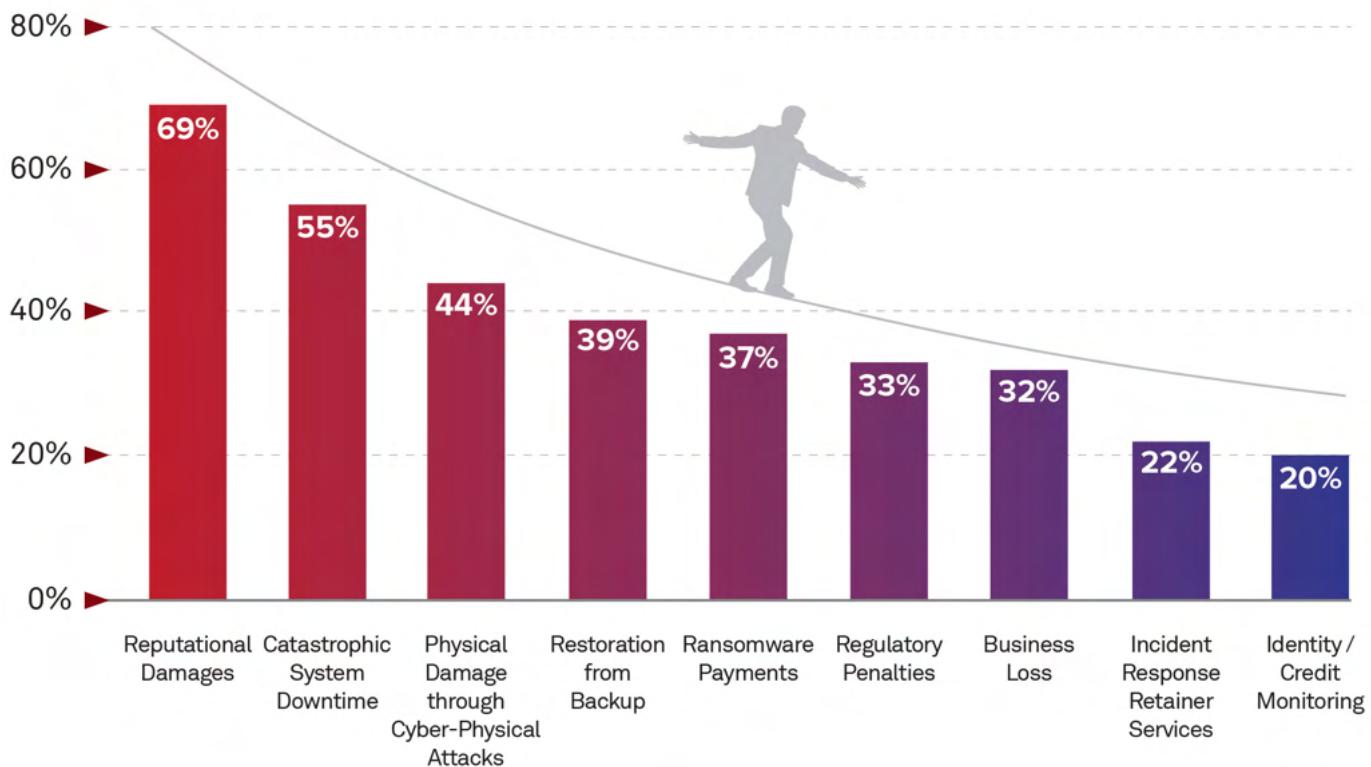
**43%**  
BFSI

.....  
**43%**  
Communications

.....  
**29%**  
Technology

- o

**Figure 33: Areas not covered by Cyber Insurance Policy**



## The Limits of Cyber Insurance

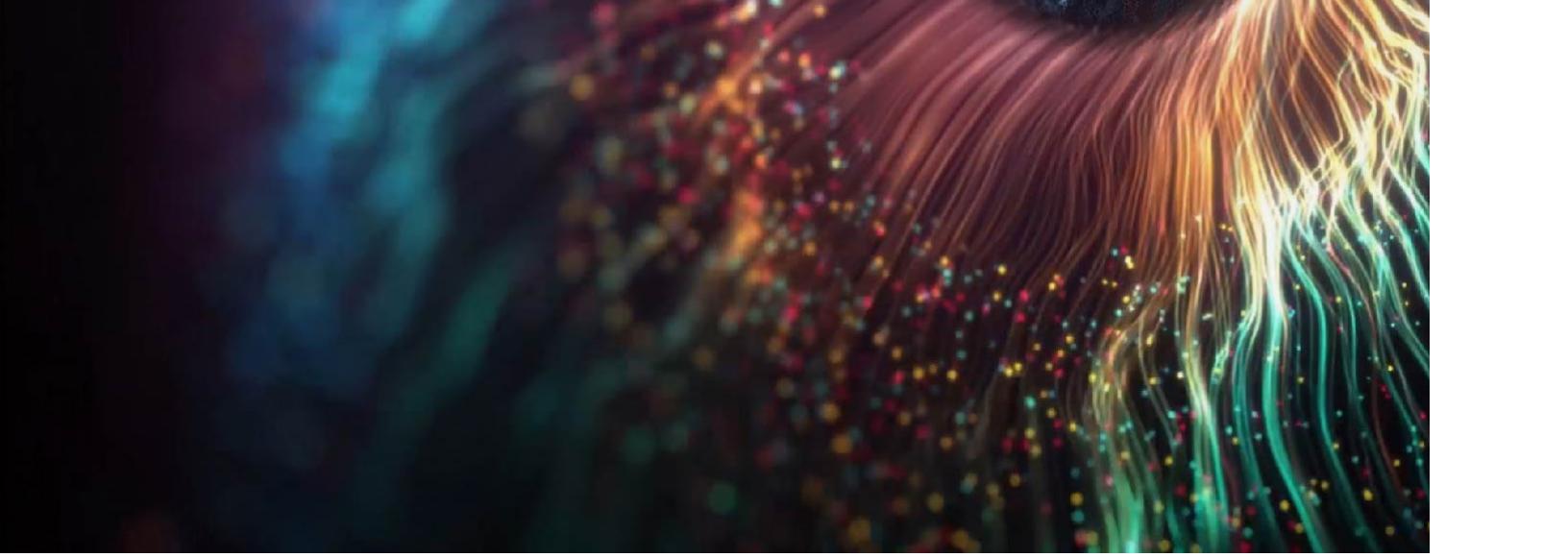
The cyber threat landscape is evolving every day, and despite an organization's efforts to implement the best cybersecurity and regulatory measures, cyberattacks and data breaches remain a very real possibility that can have catastrophic financial and reputational impacts on the enterprise. Adequate cybersecurity insurance is a necessity. But a word of caution: while cyber insurance can help organizations cover some of the financial losses that arise from cyberattacks and breaches, not all types of liability are covered, including some of the biggest exposures that organizations face today.

Figure 33 suggests that insurance companies may need to produce plans that provide more coverage at a reasonable premium. But here's the challenge for insurance companies: they have struggled to diversify risk across different domains and/or predict future risk based on past trends as a result of rapidly evolving threat scenarios. This results in higher premiums. And in most cases, the calculation of exact damages is difficult because of the nature of the attacks and the cascading damage that follows.

At the very least, organizations need to take a hard look at cyber insurance as a method of managing cyber and ask, "Are we adequately protected?" This is a conversation that CISOs might have with the CFO or head of risk management, both of whom have the expertise and tools to evaluate cyber and regulatory risk. They could become part of the collaborative team.

# FUTURE OF CYBER SECURITY





*As disruptive technologies accelerate, CISOs may need to think like futurists to stay ahead of security innovations.*

## **Introduction: The long view on patent submissions**

One way to identify future cyber technology trends is to analyze patent submissions. It's important to gain insights into how organizations are making investments and how they are protecting them with patents. Generally, it takes years for a new technology to begin maturing. Consider generative AI, which is currently experiencing unprecedented growth. Generative AI has been in R&D for many years, but is only making headlines now. We take a long view on the future of cybersecurity that is tied to the premise that patents highlight the beginning of a process designed to push technology solutions forward and eventually drive new revenue streams. As the noted futurist Ray Kurzweil has suggested, the future comes faster than one thinks. As disruptive technologies accelerate, CISOs may need to think like futurists to stay ahead of security innovations.

### **Research Scope**

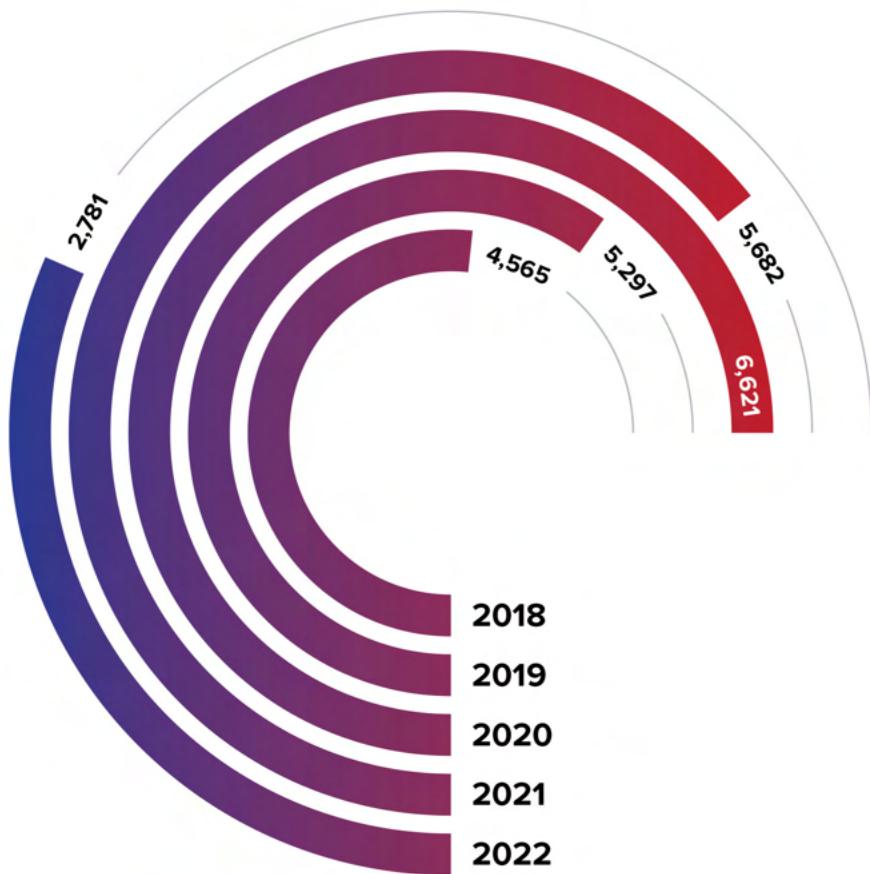
This research was conducted for nine cybersecurity practice areas like Data Security, Application Security, Network Security, Cloud Security, Endpoint security etc. across top six key emerging technologies, Artificial Intelligence (AI)

/ Machine Learning (ML), Blockchain, Internet of Things (IoT), 5G, Quantum Computing, and Digital Twin. This analysis was performed by scanning patents submitted from 2018 onwards covering all geographies. More specifically, this technology trend analysis focuses on twenty-one countries. This analysis also tries to map patent submission activities in cybersecurity patent tech radar areas.

### **Cybersecurity Patent Submission Trend**

It is observed that, since 2018, 24900+ patent families (technology inventions) have been submitted in the cross-section of relevant cybersecurity practice areas, industry domains and technologies. Every year, starting from 2018, there was an increase in number of patent submissions. This specifies that there is an increased emphasis in research, technology growth and its adoption in cybersecurity. It is worth noting that the data for 2021 and 2022 is incomplete (due to standard time lag in publication procedure at patent offices across the world) and is expected to be higher when all the patent applications submitted at different patent offices are published. Consequently, the aggregated patent submission numbers shown here for the years 2019, 2020 would be higher than the numbers reported in the previous editions of SOCR.

Figure 34: Year-Wise Cybersecurity Patent Submission Trend



## Which countries are leading the race in patent submissions?

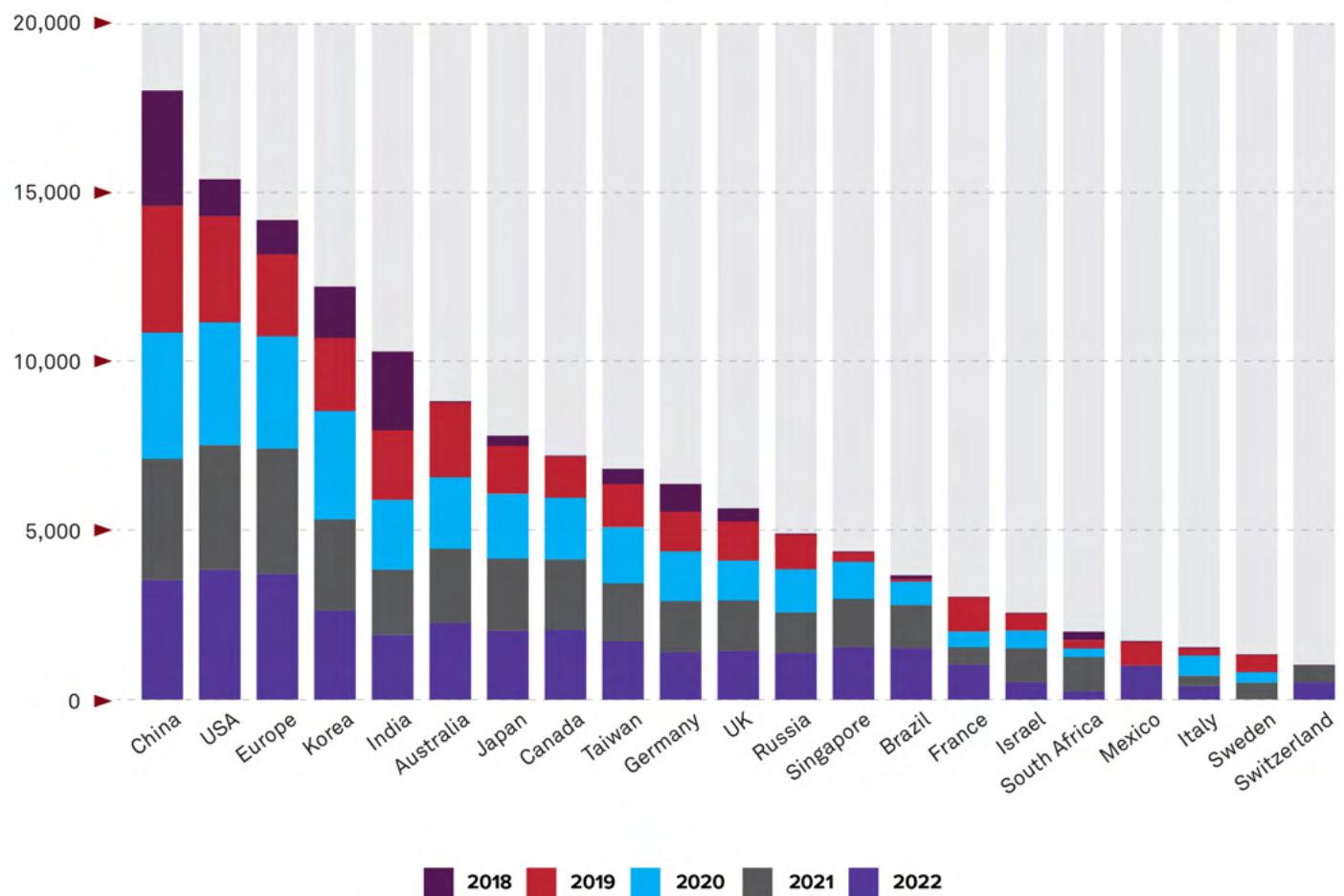
*Although China leads in overall submissions, the race for global dominance in new technology patents is still in the early stages. Any concerns regarding the geopolitical implications of China's domestic filings may be premature.*

Our data show that China today is leading in total patents filed, with more than 19,000 in 2022. The U.S. was second, with more than 4,500 patents filed. It's important to note that only 6% of the Chinese patents were submitted in the U.S. and other geographies. This suggests that Chinese patents are largely domestic and unprotected outside China.

The reality is that while China leads in overall submissions, the race for global dominance in new technology patents is still in the early stages. Any concerns regarding the geopolitical implications of China's domestic filings may be premature.

Many of the patents filed by China and the U.S. are in different technology domains. Most of the U.S. patents are related to data security, device security and network protection. Many China-filed patents pertain to cloud security, threat intelligence using AI / ML and blockchain.

**Figure 35: Geography Wise Cybersecurity Patent Count on a Logarithmic Scale**



	China	USA	Europe	Korea	India	Australia	Japan	Canada	Taiwan	Germany	UK	Russia	Singapore	Brazil	France	Israel	South Africa	Mexico	Italy	Sweden	Switzerland
2018	3264	1574	387	232	119	86	92	95	50	37	49	40	45	30	11	12	4	8	4	0	1
2019	3925	1388	363	274	114	67	100	88	61	46	51	25	35	19	18	15	2	0	1	2	1
2020	5212	1174	214	299	165	58	64	57	46	42	28	33	15	5	12	12	1	0	2	1	1
2021	4945	393	48	97	164	72	23	14	17	20	19	16	2	1	5	4	3	1	1	2	1
2022	2409	9	1	19	309	0	1	0	3	8	3	0	0	1	0	0	3	0	0	0	0

\* This table consists of Patent Data till 31st Oct 2022

## Which Industry Sectors are Most Impacted by these Patents?

*For technology organizations, AI/ML patents are leading the way. AI/ML has already been leveraged to address both practical and complex problems in the cybersecurity space.*

The three most impacted industry domains for cyber patents are:

- Consumer
- Healthcare
- Technology

### Consumer industry

Within the consumer industry domain, most patent submissions have been in media, followed by travel and hospitality. The greatest number of submissions have been related to user account security, privacy protection, and personally identifiable information (PII).

### Healthcare industry

In healthcare, most of the patent submissions have been related to the protection of PII and digital patient medical records. In the medical device subdomain, most submissions were related to intrusion/detection protection, software supply chain security, and device access management.

### Technology industry

For technology organizations, AI/ML patents are leading the way. Dominating headlines for the past two years — thanks to the meteoric rise of generative AI — AI/ML has already been leveraged to address both practical and complex problems in the cybersecurity space. The CEOs of a number of top technology companies — including hardware firms and consumer tech giants — have announced plans to integrate generative AI into every application and device. Other emerging technologies, such as 5G and quantum computing, have gained early adoption but still have great headroom to grow. These technologies offer tremendous opportunities to streamline processes and expand security capabilities, but they may also multiply enterprise risk exposures.



Figure 36: Cross-Section of Industry Domain and Emerging Technologies in Cybersecurity

S. No	Sector	Sub-Sector	Digital Twin	Quantum Computing	5G	IoT	Block-chain	AI/ML
1	BFSI	Securities and Investment Banking	24	11	63	38	120	143
		Insurance	3	5	10	22	79	248
		Banking	4	23	56	109	508	422
2	COMM	Comms	4	21	155	222	104	221
3	Consumer	Consumer Goods	7	3	15	64	119	101
		Education	2	8	2	5	2	24
		Media	14	30	205	212	235	448
		Travel & Hospitality	6	13	75	101	79	330
		Retail	6	2	26	70	169	173
		Transportation	19	10	20	37	25	102
		Public Services	2	5	30	72	137	147
		Distribution	7	10	5	8	17	76
4	ENU	Engineering & Construction	20	21	64	229	114	204
		Utilities	4	9	8	23	8	32
		Resources-Oil & Gas, Mining	2	5	7	37	30	97
5	Health	Information Services	3	2	21	66	137	92
		Medical Devices	8	6	17	37	58	170
		Healthcare	14	32	239	292	310	640
		Life Sciences	5	4	133	47	52	251
6	MFG	Industrial Product Manufacturing (IPM)	7	38	98	342	265	509
		Auto	4	5	78	243	97	308
7	TECH	Network Equipment Providers (NEP)	1	32	96	155	59	144
		Semiconductor, Computing, Storage & Peripherals	4	9	15	35	97	338
		Consumer Electronics And Peripherals	9	15	212	349	296	437

o

**Figure 37: Cybersecurity Patent Tech Radar**

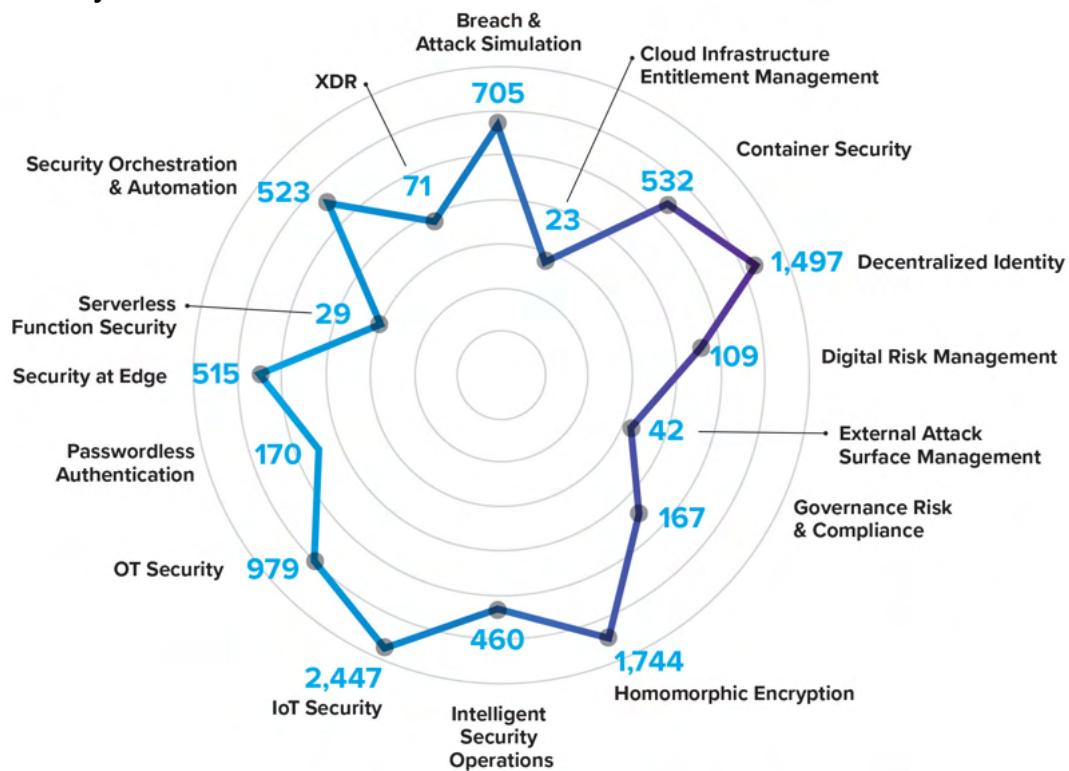


Figure 37 shows how **IoT security** led the race before 2023 with more than 2,400 technological inventions. It was followed by **homomorphic encryption** with over 1,700 patent families, and **decentralized identity** with more than 1,400 patent families in just the past few years. The adoption of homomorphic encryption, DID, OT security, and breach and attack simulation were at least partially responsible for the significant growth in patent filings. Other areas have seen relatively modest growth. Newer entrants, such as XDR, serverless and function security, external attack surface management, and cloud infrastructure entitlement management, appear to be gaining some momentum.

It is notable that IoT and decentralized identity are at the top of this analysis. It is a reminder of where the internet is going, with the recent trend of decentralization at the heart of IoT and Web3. These are technologies that are adaptive to major architectural shifts in modern IT, and CISOs should keep them on their radar.

#### SECTORAL INSIGHT

The top domains for new cyber patents over the past few years are **IoT, Homomorphic Encryption and Decentralized Identity**



## Patent Technology Trends at the Cross-Section of Cybersecurity Practice Areas

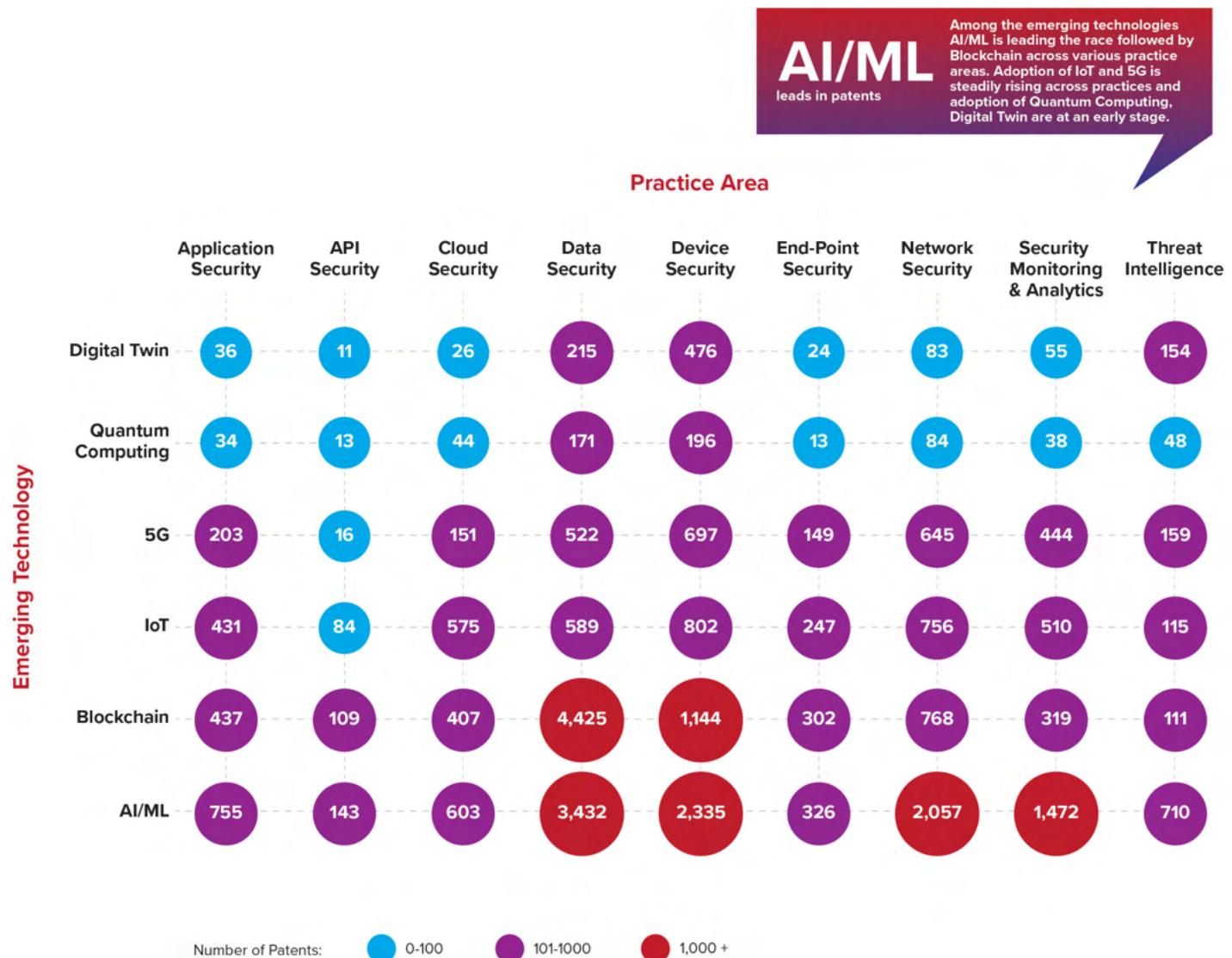
Blockchain and AI/ML – two of the most disruptive technologies to rise over the last few years – are among the emerging technologies poised for future impact. Other notable contenders include 5G and in the more distant future, quantum computing. Here's a by-the-numbers look at patent filings across four core practice areas:

- **Data security:** A deep dive into patent submissions in data security reveals that protection against unauthorized access is enabled by unique mechanisms of data encryption, tokenization, and key management across all applications and platforms.
- **Device security:** In device security practice, AI/ML leads in patent filings (2,335) followed by blockchain (1,144), IoT (802), 5G (697), digital twin (476), and quantum computing (196).
- **Network security:** In network security, AI/ML (2,057) again dominates, followed by blockchain (768), IoT (756), 5G (645), quantum computing (84), and digital twin (83).
- **Technology implementation.** AI/ML again dominates the field, followed by blockchain, IoT, and 5G. Digital twins and quantum computing appear to be gaining momentum in this practice area.

### SECTORAL INSIGHT

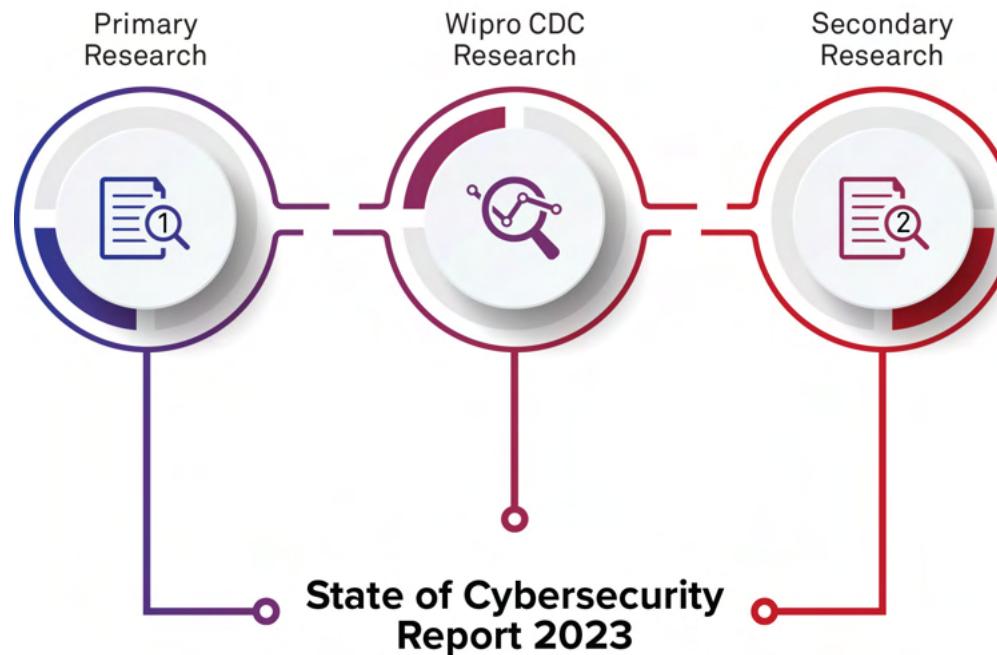
There are several emerging technologies that will impact cybersecurity in the near future including **AI/ML, 5G and Quantum Computing**

Figure 38: Patents in the Cross-Section of Cybersecurity Practice Areas and Emerging Technologies



# Methodology & Demographics

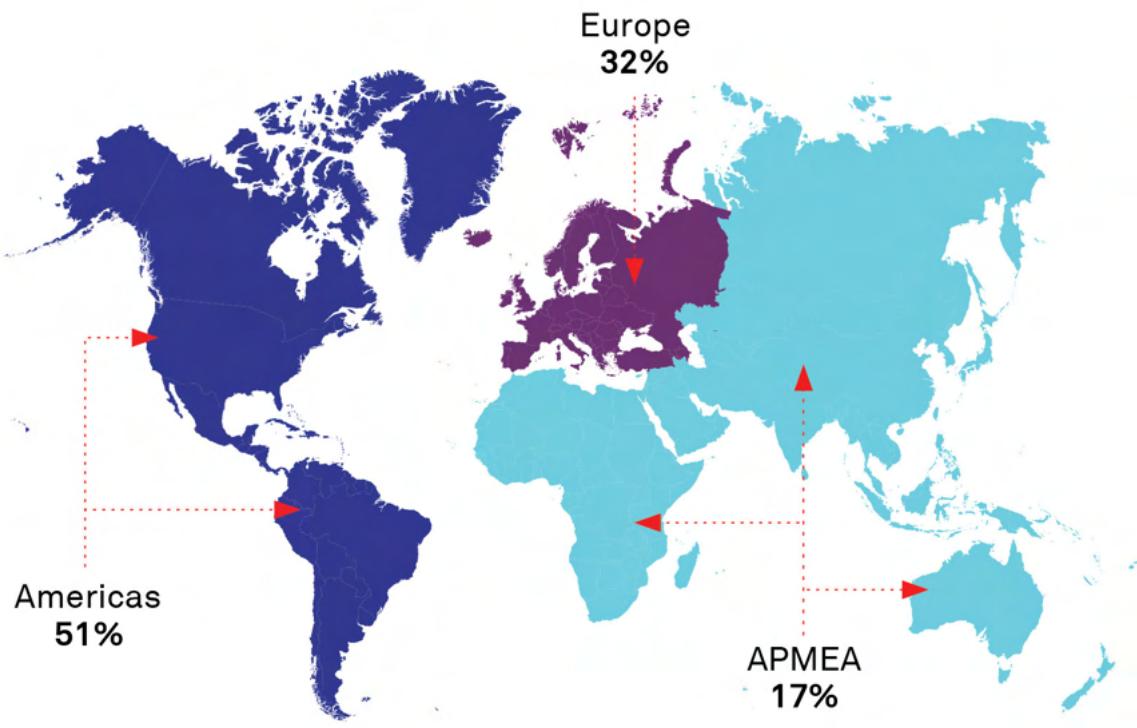
Wipro developed the State of Cybersecurity Report 2023 following a three-pronged methodology



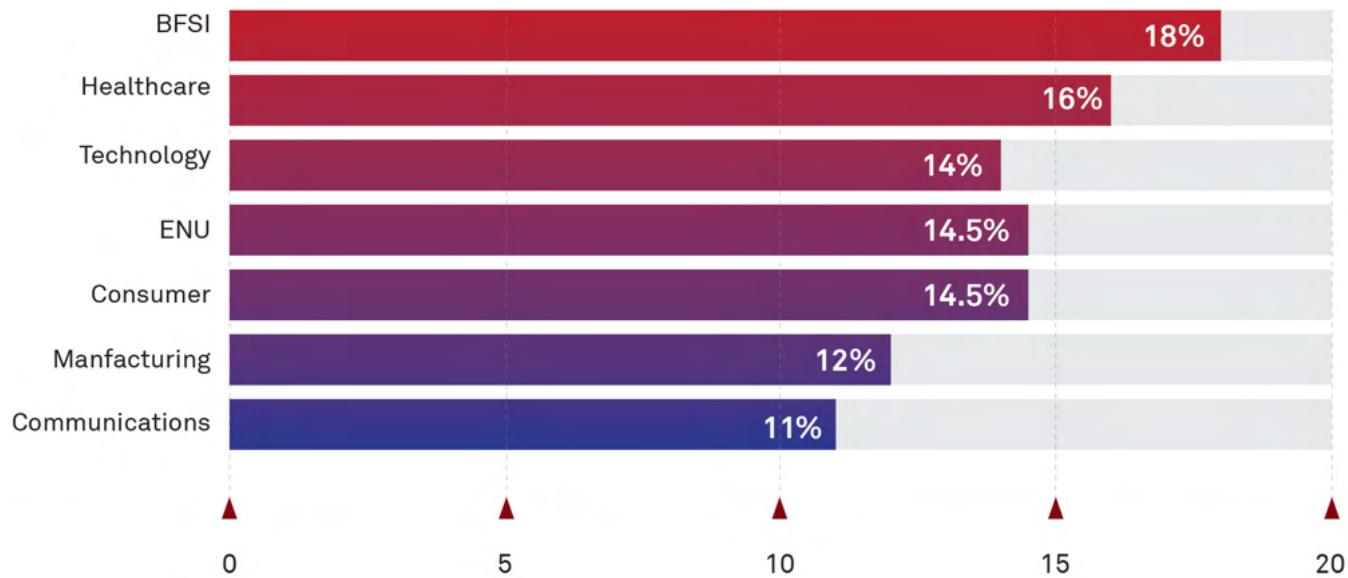
The primary research (external) involved surveying security leadership throughout US, Europe and APMEA geographies. A questionnaire with 30 questions about trends, governance, security practices, collaboration and best practices was administered over two months. The survey was anonymous, and the responses were processed at an aggregated level to arrive at insights. The CDC research was conducted on aggregated data from Wipro's CDCs across North America, Europe, India, the Middle East, and the APAC region.

The secondary research, carried out by the SOCR core team, involved various public databases and research platforms to supplement the primary research and correlate trends in the cybersecurity domain. This year, Wipro collaborated with our Ventures partners, security product partners, and academia to bring together their perspectives on the changing cybersecurity landscape.

## Respondent's Geography



## Organizations Surveyed: By Vertical



Key Statistics: Making of SOCR 2023



**345**

organizations surveyed  
across 21 countries



**24,900+**

patents filed worldwide over  
last five years are analyzed



**1,100+**

nation-state attack data  
of last 5 years analyzed



**28**

associated partners



**23**

countries data protection  
laws are analyzed



# Associated Partners



**AIShield**

Powered by Bosch



**Microsoft**

**servicenow.**



**b!nalyze**



**onetrust**

**transmit**  
security



**Upstream**



**VECTRA**  
SECURITY THAT THINKS.

**CYCOGNITO**



**VULCAN.**

**FORTINET**



**Google Cloud**

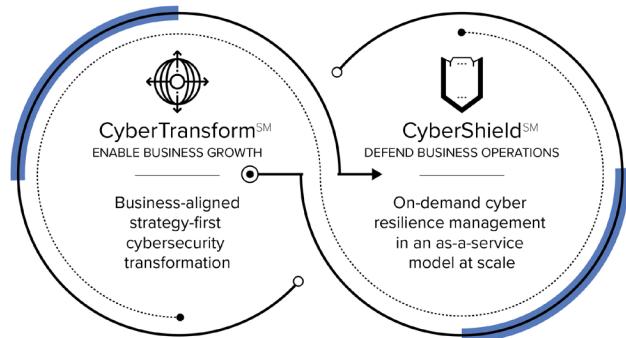


**securonix**

# About Wipro

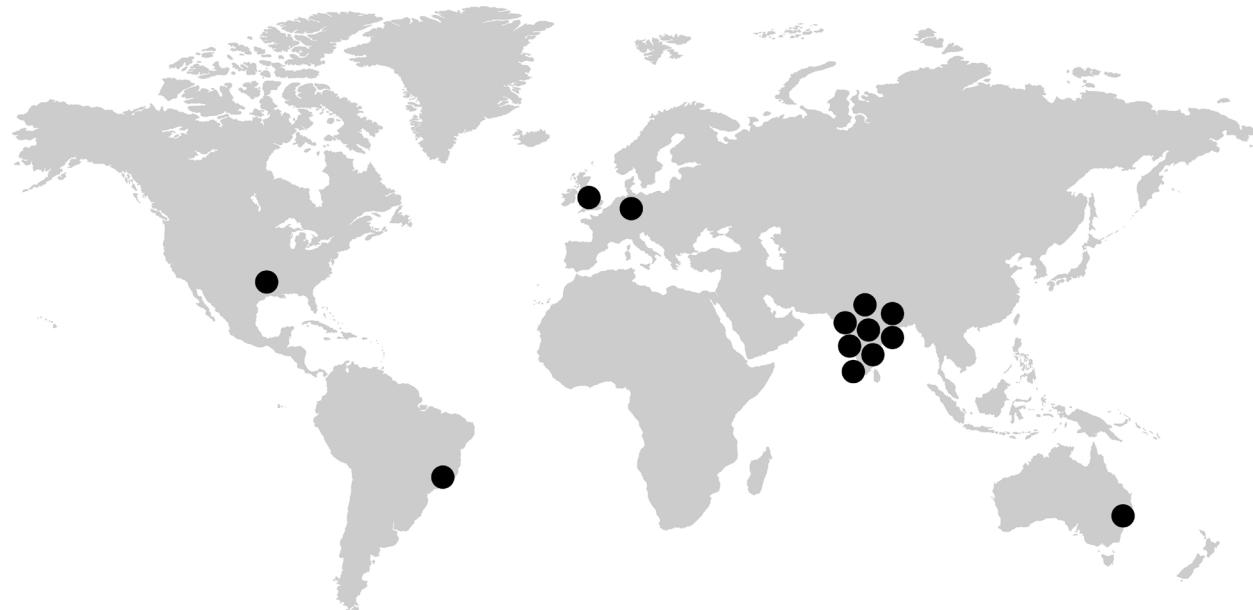
Wipro CRS is a leading cybersecurity consulting firm and the trusted cybersecurity transformation and risk services partner to global enterprises. We enable digital transformations that drive operational growth, defend business operations and build future-proof cyber resilience at scale using a strategy-first,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

Wipro CyberTransform<sup>SM</sup> is our integrated suite of cybersecurity services that includes strategy and implementation. Wipro CyberShield<sup>SM</sup> is our industry-leading suite of managed services. Together, these comprehensive cyber offerings empower organizations to protect against current and future threats and maintain compliance across the constantly evolving cybersecurity and regulatory landscape.



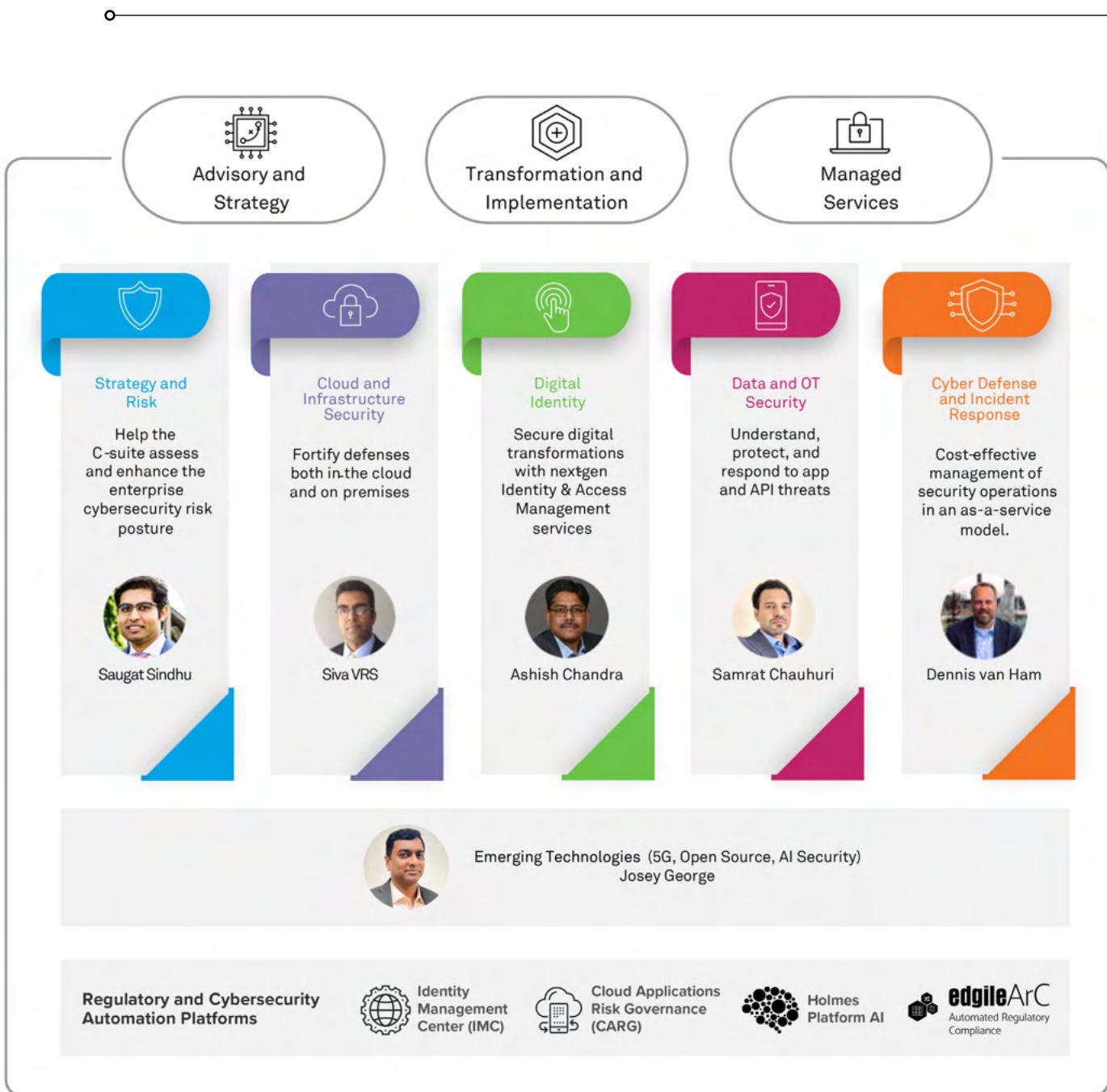
## Cyber Defense Centers

Our expert 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.



# Holistic end-to-end cybersecurity services

Our award-winning service portfolio and consulting capabilities include strategy, implementation and managed services delivered across five practice areas.



# Connect with Wipro

To contact us about Wipro's cybersecurity and risk services,  
please visit: [wipro.com/cybersecurity-experts](http://wipro.com/cybersecurity-experts).



## Americas 1



Rajesh Pillai  
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



John Hermans  
Head of Europe



## Asia Pacific Middle East Africa



Rene Morel  
Head of APMEA

# Authors

## Chief Editor

### **Josey V George**

*General Manager, Cybersecurity & Risk Services*

## Core Research, Content and Editorial Team

### **Moumila Das**

*Sub-Editor*

*Senior Consultant, Cybersecurity & Risk Services*

### **Karthikeyan S**

*Consultant, Cybersecurity & Risk Services*

### **Sayan Sarkar**

*Consultant, Cybersecurity & Risk Services*

## Content & Research Inputs

### **Sudipta Ghosh**

*Head - Intellectual Property Management*

## **CDC Engineering Team**

*Cybersecurity & Risk Services*

# References

- <https://www.cfr.org/cyber-operations/>
- <https://www.sec.gov/rules/proposed/2022/33-11038.pdf>
- <https://iapp.org/resources/>
- <https://piwik.pro/privacy-laws-around-globe/>
- <https://www.dlapiperdataprotection.com/>

## **Disclaimer:**

This document is an informative report on cybersecurity and cyber risk and should not be misconstrued as professional consultancy. No warranty or representation, expressed or implied, is made by Wipro on the content and information shared in this report. In no event shall Wipro or any of its employees, officers, directors, consultants or agents become liable to users of this report for the use of the data contained herein, or for any loss or damage, consequential or otherwise. Some of the content and data have been contributed by partner companies or collected from third-party sources with professional care and diligence, and have been reported herein; nonetheless, Wipro doesn't warrant or represent the accuracy and fitness for purpose of the content and data.