STATE OF CYBERSECURITY
REPORT 2023

Europe Executive Summary

Cyber Resilience in an Age of Continuous Disruption

wipro cybersecurity
by cybersecurists

Executive Summary
Europe Region

TONY BUFFOMANTE

SVP & Global Head –
Cybersecurity & Risk Services
Wipro Ltd.
linkedin.com/in/buffomante

Today we find ourselves in an age of continuous disruption that is driving modern enterprises to rethink their approach to cybersecurity threats and risk management. We believe the best response to continuous disruption is continuous innovation. Wipro is committed to delivering innovative strategic consulting and managed services to help our clients meet evolving cybersecurity challenges now and into the future.

JOHN HERMANS

Head of Europe
Cybersecurity & Risk Services
Wipro Ltd.
linkedin.com/in/jamhermans

The findings in the 2023 SOCR once again emphasize the importance of having the right cyber resilience strategy in place to protect your organization. To keep cyber security and compliance affordable and cost-effective, enterprises must consider applying digital transformation principles while optimizing their cyber security and risk processes using emerging technologies such as next-gen monitoring, orchestration and AI.

The 2023 State of Cybersecurity Report (SOCR) offers a perspective and framework to help enterprises achieve cyber resilience. We surveyed the CXOs of 345 organizations across 21 countries, and collaborated with our security product partners to identify the most relevant trends within the changing cybersecurity landscape.

SECURITY TRENDS

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

Board's Cyber Expertise

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

Security Budget

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

CISO Reporting

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

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

Top 2 Cyber Risks

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

3rd Party Security Breaches

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

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

Adopting a cloud-first mindset

Global enterprises have been leveraging innovative technology to modernize business operations and grow at scale. One example is the migration of data and workloads to the cloud, which delivers almost unlimited scalability. Enterprises are adopting a cloud-first mindset as hosting risks have declined to 31% in 2022, from 54% in 2019.

As cloud footprints expand, security loopholes such as misconfigurations, blind spots, shadow IT and lack of visibility create challenges for CXOs. A resilient cloud environment requires enterprises to build a secure cloud architecture and adopt standards and best practices for cloud security governance. The top security investments include security orchestration and automation (79%), Zero Trust networks (71%) and risks for third-parties and supply chains (67%).

Accelerating growth objectives with generative AI

Businesses are focused on efficiently growing at scale, and many organizations are rapidly adopting generative AI tools to accelerate their growth objectives. AI, along with its machine learning (ML) component, can help implement greater operational efficiencies by automating simple, repetitive tasks and enhancing complex communications.

Key challenges surrounding the increased use of AI include:

Disruption

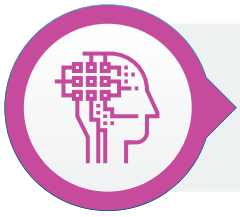
Millions of jobs may be eliminated by generative AI unless intended use guidelines and policies are established and enforced

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 brand reputation damage

Cybersecurity

Hackers can use AI to increase the volume and sophistication of attacks to steal confidential data sets and AI models for sale on the dark web

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

Expanding cybersecurity expertise in the boardroom

One critical change enterprises are embracing is adding experienced cybersecurity talent to the board. Having directors with cybersecurity experience enables the board to understand security data and improve the quality of critical security briefings. We found that globally, 87% of organizations have board level cyber oversight. Across Europe, the number is 85%.

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.

Improving cyber resilience with attack simulation exercises

Our research found that just 9% of CIOs are confident in the ability of their enterprises to recover quickly from an attack. For example, following a ransomware attack, 65% of organizations faced more than six days of downtime before they could restore systems.

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.

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.

Improving cyber resilience with attack simulation exercises

Our research found that just 9% of CIOs are confident in the ability of their enterprises to recover quickly from an attack. For example, following a ransomware attack, 65% of organizations faced more than six days of downtime before they could restore systems.

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.

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.

Next-generation cybersecurity monitoring

1

Attacks of all kinds happen

The proper defenses can minimize attacks, but nothing can prevent them. This is what makes post-breach forensic investigations so crucial. It is essential for the enterprise to have a suite of robust and comprehensive tools to quickly and accurately locate any and all security holes. The quicker these holes are identified, the faster and more completely they can be patched.

2

Bad guys talk to each other

The reason identifying and fixing security holes is mission-critical is that the bad guys talk to each other, typically on the dark web. Once a hole is discovered and leveraged by one criminal gang, it will immediately be shared with others. And those other criminals know that they have a limited attack window before the hole is fixed. So they tend to attack quickly and repeatedly.

3

Attacks must be identified and detailed as quickly as possible

Many enterprises get penetrated by malware that lies dormant for many months before the bad guys launch an attack. Sometimes, the attack – such as an exfiltration of valuable data – can happen and the enterprise might not learn of the attack for an extended period. It is not unusual for an enterprise to never discover the attack directly. Rather they learn about it when stolen data is discovered on the dark web, or law enforcement learns of the breach after an arrest is made, or a credit card brand (Visa, MasterCard, Amex, etc.) discovers the breach when the enterprise is the common point of purchase for a massive number of fraud attempts.

SURVEY METHODOLOGY

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

DOWNLOAD THE FULL REPORT

To read the full report, visit:
wipro.com/socr/

Ambitions Realized.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

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

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

Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With 250,000 employees and business partners across more than 60 countries, we deliver on the promise of helping our clients, colleagues, and communities thrive in an ever-changing world.

For more information, please write to us at info@wipro.com

EUROPE/CRS/SEPT 2024