STATE OF CYBERSECURITY
REPORT 2023

Americas Executive Summary

Cyber resilience in an age of continuous disruption

wipro cybersecurity
by cybersecurists

Executive Summary
Americas Region

TONY BUFFOMATE

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

@TonyBuffomate
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.

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

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*

Top 2 Cyber Risks

87% view ransomware attacks as their top risk

82% view email phishing as their top risk

Recent Data Breaches

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

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

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

*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 third-party risk/-supply chain security (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

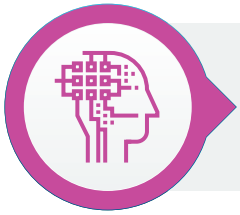
Millions of jobs may be eliminated by generative AI unless intended use guidelines and policies are established and enforced

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 the Americas, the number is 85%.

Security and risk management can no longer be considered just a cost center. It 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 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.

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 nearly 245,000 employees and business partners across 65 countries, we deliver on the promise of helping our clients, colleagues, and communities thrive in an ever-changing world. For additional information, visit us at www.wipro.com

AMERICAS/CRS/OCT 2024