STATE OF CYBERSECURITY
REPORT 2023

Spotlight on AI

Cyber resilience in an age of continuous disruption

wipro cybersecurity
by cybersecurists

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. The risk and compliance challenges posed by AI, along with some best practices are discussed below.

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 surrounding the increased use of AI include:

Disruption

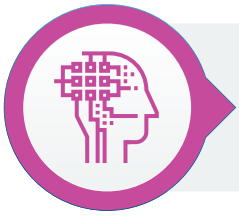
Millions of jobs may be eliminated by generative AI unless intended use guidelines and policies are established and enforced

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

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

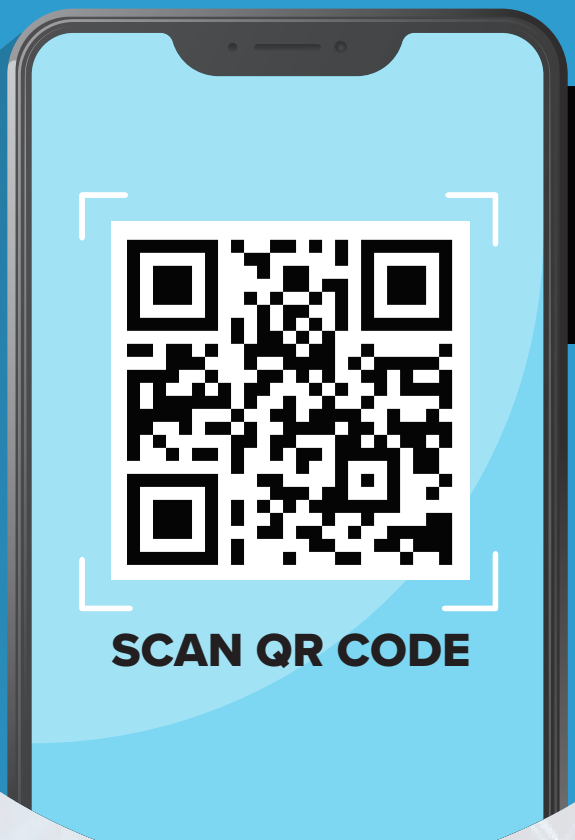
AI/ML risk governance action steps

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.



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