**November 17, 2020**

The Manager- Listing
BSE Limited
(BSE: 507685)

The Manager- Listing
National Stock Exchange of India Limited,
(NSE: WIPRO)

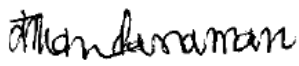
The Market Operations,
NYSE: New York
(NYSE: WIT)

Dear Sir/Madam,

**Sub: Press Release**

Please find attached herewith copy of the Press Release which is being released today.

**For Wipro Limited**



**G Kothandaraman**
**General Manager- Finance**

Registered Office:
Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru 560 035
India

T : +91 (80) 2844 0011
F : +91 (80) 2844 0256
E : info@wipro.com
W : wipro.com
C : L32102KA1945PLC020800

# Wipro's Annual State of Cybersecurity Report Finds Increasing Adoption of AI in Cybersecurity to Tackle Advanced Adversaries

*Nearly half (49%) of organizations plan to extend Cognitive and AI capabilities for security to detect and respond to attacks faster*

**East Brunswick, New Jersey, USA and Bangalore, India – November 17, 2020:** Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO)**,** a leading global information technology, consulting and business process services company, today released its annual State of Cybersecurity Report (SOCR) that presents changing perspectives of cybersecurity globally.

The report provides fresh insights on how Artificial Intelligence (AI) will be leveraged as part of defender stratagems as more organizations lock horns with sophisticated cyberattacks and become more resilient. There has been an increase in R&D with 49% of the worldwide cybersecurity related patents filed in the last four years being focussed on AI and Machine Learning (ML) application. Nearly half the organisations are expanding cognitive detection capabilities to tackle unknown attacks in their Security Operations Center (SOC).

The report also illustrates a paradigm shift towards cyber resilience amid the rise in global remote work. It considers the impact of COVID-19 pandemic on cybersecurity landscape around the globe and provides a path for organizations to adapt with this new normal.

The fourth edition of the SOCR saw a global participation of 194 organizations and 21 partner academic, institutional and technology organizations over four months of research.

Additional highlights from State of Cybersecurity Report, include:

**Global macro trends in cyber security**

- **Nation State Attacks Target Private Sector:** 86% of all nation-state attacks fall under espionage category, and 46% of them are targeted towards private companies.
- **Evolving threat patterns have emerged in the Consumer and Retail Sectors:** 47% of suspicious social media profiles and domains were detected active in 2019 in these sectors.

**Cyber Trends sparked by COVID-19 Global Pandemic**

- **Cyber Hygiene proven difficult during remote work enablement:** 70% of the organizations faced challenges in maintaining endpoint cyber hygiene and 57% in mitigating Virtual Private Network (VPN) and Virtual Desktop Infrastructure (VDI) risks.

- **Emerging post-COVID Cybersecurity priorities:** 87% of the surveyed organizations are keen on implementing zero trust architecture and 87% are planning to scale up secure cloud migration.

**Micro Trends: An inside-out enterprise view**

- **Low Confidence in Cyber Resilience:** 59% of the organizations understand their cyber risks but only 23% of them are highly confident about preventing cyberattacks.
- **Strong Cybersecurity spend due to Board Oversight & Regulations:** 14% of organizations have a security budget of more than 12% of their overall IT budgets.

**Micro Trends: Best Cyber practices to emulate**

- **Laying the foundation for a Cognitive SOC**: 49% of organizations are adding cognitive detection capabilities to their SOC to tackle unknown attacks.
- **Concerns about OT Infrastructure attacks increasing:** 65% of organizations are performing log monitoring of Operation Technology (OT) and Internet of Things (IoT) devices as a control to mitigate increased OT Risks.

**Meso Trends: An overview on Collaboration**

- **Fighting cyber-attacks demands stronger collaboration**: 57% of organizations are willing to share only Indicators of Compromise (IoCs) and 64% consider reputational risks to be a barrier to information sharing.
- **Cyber-attack simulation exercises serve as a strong wakeup call:** 60% participate in cyber simulation exercises coordinated by Industry regulators, National Computer Emergency Response Team (CERTs) and third-party service providers and 79% organizations have dedicated cyber insurance policy in place.

**Future of Cybersecurity**

- **5G security is the emerging area for patent filing:** 7% of the worldwide patents filed in the cyber domain in the last four years have been related to 5G security.

**Vertical insights by industry**

- **Banking, Financial Services & Insurance:** 70% of financial services enterprises said that new regulations are fuelling increase in security budgets, with 54% attributing higher budgets to board intervention.
- **Communications:** 71% of organizations consider cloud-hosting risk as a top risk.
- **Consumer:** 86% of consumer businesses said email phishing is a top risk and 75% enterprises said a bad cyber event will lead to damaged band reputation in the marketplace.
- **Healthcare & Life Sciences:** 83% of healthcare organizations have highlighted maintaining endpoint cyber hygiene as a challenge, 71% have highlighted that breaches reported by peers has led to increased security budget allocation.

- **Energy, Natural Resources and Utilities:** 71% organizations reported that OT/IT Integration would bring new risks.
- **Manufacturing:** 58% said that they are not confident about preventing risks from supply chain providers.

**Bhanumurthy B.M, President and Chief Operating Officer, Wipro Limited** said, "There is a significant shift in global trends like rapid innovation to mitigate evolving threats, strict data privacy regulations and rising concern about breaches. Security is ever changing and the report brings more focus, enablement, and accountability on executive management to stay updated. Our research not only focuses on what happened during the pandemic but also provides foresight toward future cyber strategies in a post-COVID world".

To access the full report, click here.

**About Wipro Limited**
Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 180,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

**Media Contact:**
Nisha Chandrasekaran
Wipro Limited
nisha.chandrasekaran@wipro.com

**Forward-Looking Statements**
The forward-looking statements contained herein represent Wipro's beliefs regarding future events, many of which are by their nature, inherently uncertain and outside Wipro's control. Such statements include, but are not limited to, statements regarding Wipro's growth prospects, its future financial operating results, and its plans, expectations and intentions. Wipro cautions readers that the forward-looking statements contained herein are subject to risks and uncertainties that could cause actual results to differ materially from the results anticipated by such statements. Such risks and uncertainties include, but are not limited to, risks and uncertainties regarding fluctuations in our earnings, revenue and profits, our ability to generate and manage growth, complete proposed corporate actions, intense competition in IT services, our ability to maintain our cost advantage, wage increases in India, our ability to attract and retain highly skilled professionals, time and cost overruns on fixed-price, fixed-time frame contracts, client concentration, restrictions on immigration, our ability to manage our international operations, reduced demand for technology in our key focus areas, disruptions in telecommunication networks, our ability to successfully complete and integrate potential acquisitions, liability for damages on our service contracts, the success of the companies in which we make strategic investments, withdrawal of fiscal governmental incentives, political instability, war, legal restrictions on raising capital or acquiring companies outside India, unauthorized use of our intellectual property and general economic conditions affecting our business and industry. The conditions caused by the COVID-19 pandemic could decrease technology spending, adversely affect demand for our products, affect the rate of customer spending and could adversely affect our customers' ability or willingness to purchase our offerings, delay prospective customers' purchasing decisions, adversely impact our ability to provide on-site consulting services and our inability to deliver our

customers or delay the provisioning of our offerings, all of which could adversely affect our future sales, operating results and overall financial performance. Our operations may also be negatively affected by a range of external factors related to the COVID-19 pandemic that are not within our control. Additional risks that could affect our future operating results are more fully described in our filings with the United States Securities and Exchange Commission, including, but not limited to, Annual Reports on Form 20-F. These filings are available at www.sec.gov. We may, from time to time, make additional written and oral forward-looking statements, including statements contained in the company's filings with the Securities and Exchange Commission and our reports to shareholders. We do not undertake to update any forward-looking statement that may be made from time to time by us or on our behalf.