



August 6, 2019

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

We are enclosing a copy of Press Release which is being released today.

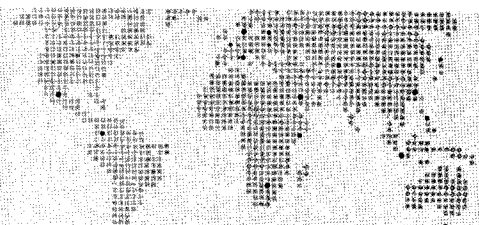
For WIPRO LIMITED

Vinay M A
Senior Manager- Corporate Secretarial & Compliance

Registered Office:

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru 560 035
India

T : +91 (80) 2844 0011
F : +91 (80) 2844 0054
E : info@wipro.com
W : wipro.com
C : L32102KA1945PLC020800





Wipro's Third Annual State of Cybersecurity Report Finds Organizations Focusing on IoT and Cloud While Developing Cyber Defense Systems

Digital transformations are driving organizations to rethink security threats

Bangalore, India and East Brunswick, New Jersey, USA – August 6, 2019: Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO), a leading global information technology, consulting and business process services company, today released its 2019 State of Cybersecurity Report that highlights the rising importance of cybersecurity defense to global leaders, the emergence of the CISO as a C-Suite role, and an unprecedented focus on security as a pervasive part of the business operations.

The study found that one in five CISOs are now reporting directly to the CEO, 15% of organizations have a security budget of more than 10% of their overall IT budgets, 65% of organizations are tracking and reporting regulatory compliance, and 25% of organizations are carrying out security assessments in every build cycle. In addition, 39% of organizations now have a dedicated cyber insurance policy. All of these points showed dramatic increases from previous years.

The annual study is based on three months of primary and secondary research, including surveys of security leadership, operational analysts, and 211 global organizations across 27 countries.

Additional highlights from the report:

1. **More data exposed, yet a decline in the number of publicly disclosed breaches.** While the number of significant publicly reported breaches decreased by 25%, the number of records exposed during attacks increased by 164% to 232 records exposed per second. Attackers also targeted more specific information perceived to have higher monetary value: 38% of the data records breached/targeted were a combination of personally identifiable information and security credentials such as passwords.
2. **Cryptominers are the new big threat.** Cryptominer malware surged to become the new emerging threat: 25% of global organizations were targeted by Coinhive malware alone in 2018. 80% of all cryptomining attacks originated from just three sources: Coinhive, Cryptoloot, and JSEcoin. Ransomware attacks by contrast declined in 2018.

Yet organizations are aligning themselves to cyber-resilient strategies in new ways



1. **Cloud and IoT security strategies on the radar.** With cloud and IoT adoption on the rise, 28% of organizations perceive cloud account hijacking as one of the top security threats to their cloud environments. 26% of organizations are prioritizing security assessment of IOT devices to mitigate new risks.
2. **Collective wisdom trumps learning in isolation:** 67% of organizations are now willing to share indicators of compromise (malicious IPs, URLs, domains), and 33% of organizations are willing to share attacker tactics, techniques, and procedures with industry peers. Information sharing and timely threat intelligence have become critical enablers in anticipating and mitigating new and developing attacks.
3. **More pervasive approach to protection.** 39% of organizations now have a dedicated cyber insurance policy, up by 12% from 2017; 28% of organizations participate in cyberattack simulation exercises coordinated by industry regulators; and 1 in 4 organizations now carry out security assessments in every build cycle.

Raja Ukil, Global Head for Cybersecurity & Risk Services, Wipro Limited said, "With organizations riding the digital wave, security strategies need to be enhanced to address the changing landscape and enable a smooth and safe transition. Security is also evolving to be a pervasive part of core business operations, and countries are establishing active cyber defence strategies and functions to foster partnerships with the private sector enterprises and with other countries. Amidst growing threats, leaders are collaborating more than ever before in new and innovative ways to mitigate the risks."

Wipro's in-depth report demystifies the forces that have shaped the environmental conditions of this battleground and provides needed insight into the future of cybersecurity.

The full report can be found here [<https://www.wipro.com/applications/form/the-state-of-cybersecurity-report-2019/?asd>].

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 170,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

Wipro Media Contact:

Purnima Burman
Wipro Limited
purnima.burman@wipro.com

Forward-looking and Cautionary Statements

Certain statements in this release concerning our future growth prospects are forward-looking statements, which involve a number of risks, and uncertainties that could cause actual results to differ materially from those in such forward-looking statements. The risks and uncertainties relating to these statements include,



but are not limited to, risks and uncertainties regarding fluctuations in our earnings, revenue and profits, our ability to generate and manage growth, 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. Additional risks that could affect our future operating results are more fully described in our filings with the United States Securities and Exchange Commission. 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.

