



June 15, 2017

The Manager – Listing
BSE Limited
(BSE: 507685)

022 22723121

The Manager – Listing
National Stock Exchange of India Limited.
(NSE: WIPRO)

022 26598237

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

0012126565780

Dear Sir,

Subject: Press release

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

For WIPRO LIMITED

G Kothandaraman
Head- Secretarial and Compliance
Encl: As Above





Wipro Launches 'State of Cybersecurity Report 2017'

Study Finds Significant Rise in Cyber Security Threats due to Disruptive Technology

East Brunswick, New Jersey, USA and Bangalore, India – June 15, 2017: Wipro Limited (NYSE:WIT, BSE: 507685, NSE: WIPRO), a leading global information technology, consulting and business process services company today announced the launch of its first 'State of Cybersecurity Report, 2017' which highlights the macro, micro and meso environmental trends in cybersecurity in 2016 and imminent disruptions that can affect future trends.

The 'State of Cybersecurity Report, 2017' was developed after interviewing the CISO teams of 139 organizations across various industry sectors. The survey covered 11 countries in North America, Europe, APAC, Middle East and South Asia to evaluate trends in current security practices and analyzing thousands of attempted security attacks and incidents captured in Wipro's Cyber Defence Centres during 2016. A secondary research was also done on impending disruptions in the cybersecurity domain. The report has key takeaways for both executive management tasked by the board of respective companies to minimize cyber risks and for the security analyst teams that are battling daily attacks in various Security Operations Centres around the globe.

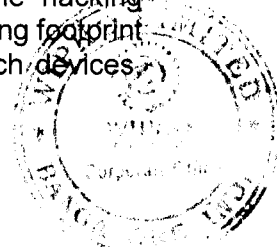
According to the report, 2016 saw an alarming 53.6% increase in the number of records stolen across the globe as opposed to 2015. Data breaches once made public, resulted immediately in high peaking of negative sentiments on social media against the enterprise concerned, indicates the post facto twitter sentiment analysis. 56% of breaches reported had user credentials (passwords) as part of the types of data stolen, implying that further damage could be perpetrated using the stolen data.

Another finding of the report highlights that at 33.3%, angler was the most observed exploit kit. Angler, RIG, Nuclear were some of the most common types of exploit kits used by cyber criminals.

According to the report, the Cyber Defence Center (CDC) data analysis points out that 56% of all the malware attacks that have taken place in 2016 were a result of Trojans. Likewise, viruses and worms accounted for 19% and 20% respectively. Other types of malware threat categories like PUA, adware and ransomware, together, though accounted for only 4% of attacks, often can lead to significant damages.

The study found that majority of the security products were themselves vulnerable to exploitation and CISOs will be required to keep track of vulnerabilities in the security products themselves.

Interestingly, emergence of new Internet of Everything "surfaces" like connected cameras, cars, health and industrial automation devices proves to be a great launch pad for the "hacking for hire" industry. The emerging IoT devices come with a low memory and processing footprint and usually accommodate very little security capabilities including patching. Such devices



once "online" with an IP address, are easy prey for sophisticated hacking syndicates. These syndicates can develop custom malware to take control of IoT devices en masse and use them as a launch pad for cyber-attacks. The report notes that the responsibility for governance of data privacy is still highly centralized, lying with either the CIO, CISO or CPO for 71% of organizations. Managing privileged access to data was ranked as the highest control amongst data security controls.

"Cyber security is becoming a top priority for businesses. It has become very critical to identify risks near real-time and empower stakeholders to take actions and decisions based on priority. The report highlights crucial findings on attacks, vulnerabilities and cyber defence that are useful for teams across cybersecurity strategy, operations and risk management," said **Sheetal Mehta, Vice President and Global Head, Cybersecurity & Risk Services, Wipro Limited.**

The State of Cybersecurity Report, 2017 brings together an interesting mix of research and analysis on attacks, vulnerabilities, and cyber weapons and contrasts their impact on existing defense mechanism. Download the complete report at [http:// http://www.wipro.com/microsite/state-of-cyber-security-2017/](http://http://www.wipro.com/microsite/state-of-cyber-security-2017/)

About Wipro Limited

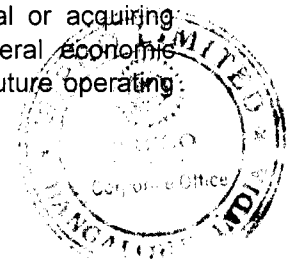
Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital 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 a dedicated workforce of over 170,000, serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

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.

