Indian businesses continue having cybersecurity concerns with remote working, one year into the pandemic, finds Thales

- 40% of respondents from India reported an increase in the volume, severity, and/or scope of cyber-attacks in the last 12 months in comparison to the global figure of 47%
- Nearly 2 in 5 (35%) of respondents, globally, find malicious insiders as the biggest threat to data security
- 48% of respondents in India (38% worldwide) consider third-party vendor networks to be the biggest target for cyber attackers

Despite being over a year into remote working and the possibility of a likely shift to hybrid remote/in-office working models, security remains a key concern for respondents both globally and in India. While 38% of respondents from India continue to be very concerned about the security risks while working remotely, globally, this figure stands at 39%.

This is just one of the key insights from the 2021 Thales Global Data Threat Report, a commissioned study conducted by 451 Research, part of S&P Global Market Intelligence, which reveals that managing security risks is undoubtedly getting more challenging, with almost 40% of respondents from India reporting an increase in the volume, severity, and/or scope of cyber-attacks in the last 12 months.

Attacks On The Rise
Talking about global stats, of those who have ever experienced a breach, two in five (41%) had it happen in the last year. This number has nearly doubled from 21% in 2019 globally, marking a significant shift in the threat posed.

For respondents from India, malware (56%) is the leading source of security attacks followed by ransomware (53%), and phishing and credential stuffing (both 43%). Yet, when it comes to how attacks occur, the message is clear: internal threats as well as external attackers are still of great concern to industry. Malicious insiders (40%), external attacks (25%) and human error (25%) have been spotted by respondents from India as the types of attacks seen with the greatest threat.

Despite the increased risk remote working has posed to enterprises throughout the pandemic, nearly half (48%) of respondents from India report that their security infrastructure was not prepared to handle the risks caused by Covid-19. In fact, only one in five (21%) of organisations believe it was very prepared.

Major targets for Cyber-Attacks
Forty-eight percent of respondents from India rank third-party vendor networks as the biggest target for cyber attacks, followed by on-premises legacy applications (44%), cloud based storage (40%) and web applications (38%).

Ashish Saraf, VP and Country Director – India, Thales, comments: “Many organizations experienced heightened security challenges over the last year and with the increasing number
of ransomware attacks, organizations are now facing a double extortion threat. Not only could they be locked out of their critical IT & OT systems but also have their sensitive data released on the internet. The traditional aspect of just relying on a sound backup and restore strategy is no longer sufficient, organizations need to implement a comprehensive digital security including controlling access to data, encryption of sensitive data coupled with secure management and control of encryption keys. It is important for all the stakeholders in the data flow chain to embrace cutting-edge technology solutions to mitigate these risks.”

Multicloud Complexity Increases Risks Globally

As increases in attacks continue, businesses are turning to the cloud to store their data in this digital-first world. More than half (55%) of businesses, globally, report that more than 40% of their data is stored in external cloud environments. Despite this, only 17% of businesses have encrypted at least half of their sensitive data stored in the cloud. On top of this, complexity is an increasing issue, with many respondents now using at least two PaaS (Platform as a Service) providers (45%) and/or two IaaS providers (Infrastructure as a Service). A quarter (27%) of businesses are currently using more than 50 SaaS (Software as a Service) apps.

Future Challenges and the Road Ahead

Globally, companies are recognising the issues they are facing and are attempting to address them with Zero Trust strategies. More than three quarters (76%) of respondents’ cloud strategy reportedly rely to some degree on Zero Trust security. Almost half (44%) of respondents selected Zero Trust network access (ZTNA)/software-defined perimeter (SDP) as the leading technology to invest in during the pandemic. This was followed by cloud-based access management (42%) and conditional access (41%). In fact, a third (30%) of global respondents claim to have a formal Zero Trust strategy and, interestingly, those with a formal Zero Trust strategy are less likely to also report having been breached.

However, despite businesses making moves to stop current threats, worries are growing about future challenges on the horizon. Looking ahead, 82% respondents from India have shown concerns about the security threats of quantum computing, a threat arguably exacerbated by the increasing complexity of cloud environments.

Eric Hanselman, Chief Analyst at 451 Research, part of S&P Global Market Intelligence added: “The native controls and protections available in cloud environments address a set of necessary capabilities, but they’re often insufficient to deliver effective protections for sensitive data and workloads, especially when it comes to compliance with regulations such as GDPR and the implications of the Schrems II ruling. Organizations need to increase their use of encryption and ensure they take full advantage of encryption’s benefits by controlling the secrets that protect their data through BYOK (Bring Your Own Key), HYOK (Hold Your Own Key) or BYOE (Bring Your Own Encryption) approaches. Organisations also need to make internal changes to ensure that personnel at all levels understand the security challenges and to properly align investment priorities. Senior executives need to obtain a more complete understanding of the levels of risk and attack activity that their front-line staff are experiencing.”

About the 2021 Thales Global Data Threat Report
The 2021 Thales Global Data Threat Report was based on a global 451 Research survey commissioned by Thales of more than 2,600 executives with responsibility for or influence over IT and data security. Respondents were from 16 countries: Australia, Brazil, France, Germany, Hong Kong, India, Japan, Mexico, Netherlands, New Zealand, Singapore, South Korea, Sweden, the United Arab Emirates, the United Kingdom, and the United States. Organisations represented a range of industries, with a primary emphasis on healthcare, financial services, retail, technology, and federal government. Job titles ranged from C-level executives including CEO, CFO, Chief Data Officer, CISO, Chief Data Scientist, and Chief Risk Officer, to SVP/VP, IT Administrator, Security Analyst, Security Engineer, and Systems Administrator. Respondents represented a broad range of organizational sizes, with the majority ranging from 500 to 10,000 employees. The survey was conducted in January - February 2021.

About Thales

Thales (Euronext Paris: HO) is a global leader in advanced technologies, investing in digital and “deep tech” innovations – connectivity, big data, artificial intelligence, cybersecurity and quantum computing – to build a confident future crucial for the development of our societies. The Group provides its customers – businesses, organisations and governments – in the defense, aeronautics, space, transport, and digital identity and security domains with solutions, services and products that help them fulfil their critical role, consideration for the individual being the driving force behind all decisions.

Thales has 81,000 employees in 68 countries. In 2020 the Group generated sales of €17 billion.

About Thales in India

Present in India since 1953, Thales is headquartered in Noida and has other operational offices and sites spread across Delhi, Gurugram, Hyderabad, Bengaluru and Mumbai, among others. Over 1,800 employees are working with Thales and its joint ventures in India. Since the beginning, Thales has been playing an essential role in India’s growth story by sharing its technologies and expertise in Defence, Transport, Aerospace and Digital Identity and Security markets. Thales has two engineering competence centres in India - one in Delhi NCR focused on digital identity and security business, while the one in Bengaluru focuses on hardware, software and systems engineering capabilities for both the civil and defence sectors, serving global needs.

PRESS CONTACT

Thales, Media Relations
Security
Constance Arnoux
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com

Thales, Communications in India
Pawandeep Kaur
+91 9990098828
pawandeep.kaur@thalesgroup.com

Chase India
Anuradha Chawla/ Tulika Bhardwaj
+91 9899965560/ + 91 8851646206
Anuradha@chase-india.com/ Tulika@chase-india.com