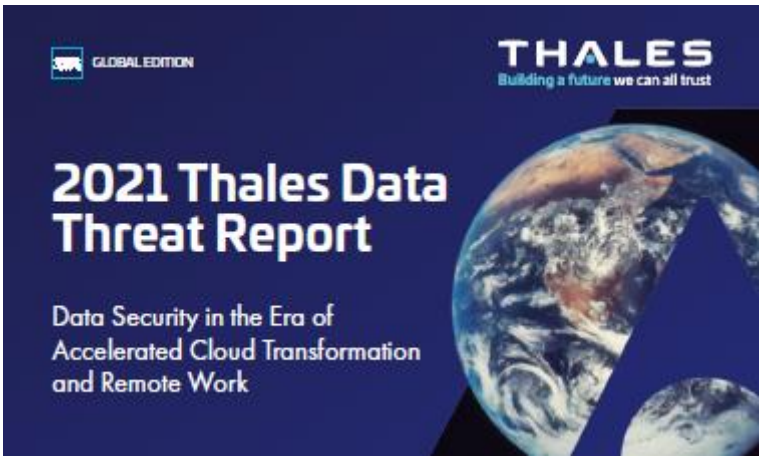
THALES
Building a future we can all trust

PRESS RELEASE
2 June 2021
Paris La Défense

Majority of businesses still have remote working cybersecurity concerns one year into the pandemic, finds Thales

- Four in five (82%) businesses remain concerned about the security risks of employees working remotely, despite many exploring potential hybrid working models
- Nearly half (47%) report an increase in the volume, severity, and/or scope of cyber-attacks in the last 12 months
- Of those who have ever experienced a breach, 41% had it happen in the last year, almost double the number (21%) compared to 2019
- Retailers are most at risk, with 61% experiencing a breach or failed an audit in 2020, raising concern for suppliers and consumers alike



©Thales

Despite being over a year into remote working and looking ahead to likely shifts to hybrid remote/in-office working models, four fifths (82%) of businesses still remain concerned about the security risks of employees working remotely.

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 nearly half (47%) of businesses seeing an increase in the volume, severity, and/or scope of cyber-attacks in the past 12 months.

Attacks On The Rise

In fact, of those who have ever experienced a breach, two in five (41%) happened in the last year. This number has nearly doubled from 21% in 2019, marking a significant shift in the threat posed.

Globally, malware (54%) is the leading source of security attacks, followed by ransomware (48%), and phishing (41%). Yet, when it comes to how attacks occur, the message is clear: internal threats and human error are still of great concern to industry. A third of businesses stated that malicious insiders (35%) and human error (31%) are the greatest risks to them, followed by external attackers (22%).

Despite the increased risk remote working has posed to enterprises throughout the pandemic, nearly half (46%) of businesses report that their security infrastructure was not prepared to handle the risks caused by Covid-19. In fact, only one in five (20%) of organisations believe it was very prepared.

Multiple Industries at Risk

This lack of protection is affecting some industries more than others it seems, with just under two thirds (61%) of retailers surveyed experiencing a breach or failing an audit involving data and applications stored in the cloud in the past year – the most of any industry surveyed. Over half of organisations in the legal (57%), call centre (55%), transportation (54%), and telecommunications (52%) sectors also suffered the same fate in the last 12 months.

Multicloud Complexity Increases Risks

As increases in attacks continue, businesses are turning to the cloud to store their data in this digital-first world. Half (50%) of businesses 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.

Sebastien Cano, Senior Vice President for Cloud Protection and Licensing activities at Thales comments: *"Teams across the globe have faced huge security challenges over the last year as companies accelerated their digital transformation and cloud adoption initiatives. When migrating to multicloud solutions, data management can quickly spiral out of control. Organisations not only risk losing track of where their data is stored across multicloud environments but also fail to protect sensitive data in the cloud. With once unprecedented amounts of data now being used and stored in the cloud, it is vital that businesses deploy a robust security strategy based on data discovery, protection and control."*

Future Challenges and the Road Ahead

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, 85% of global respondents are concerned about the security threats of quantum computing, a threat arguably exacerbated by the increasing complexity of cloud environments.

Garrett Bekker, Senior Security Research 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. Organisations 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."

Thales and 451 Research will discuss the findings in more detail during its upcoming Crypto Summit on 16 June 2021. To join, please visit the registration page.

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.

PRESS CONTACT

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

PLEASE VISIT

Thales Group
Security