Global cloud tipping point: the 2020 Thales Data Threat Report-Global Edition shows organizations struggle with security post digital transformation

- Half (50%) of all data is now stored in cloud environments, and 47% of organizations experienced a breach or failed a compliance audit in the past year
- Multi-cloud world causing profound security challenges, triggering security vulnerabilities as 100% of respondents have some sensitive data in the cloud that's not encrypted
- Impact of quantum computing imminent as 72% of organizations surveyed see it affecting them in the next five years

According to the 2020 Thales Data Threat Report – Global Edition with research and analysis by IDC, organizations reached a global cloud tipping point causing them to struggle with security challenges of digital transformation (DX). Today, half (50%) of all corporate data is stored in the cloud and nearly half (48%) of that data is considered sensitive. With multi-cloud usage becoming the new normal for companies, all respondents said at least some of the sensitive data stored in the cloud is not encrypted and 49% globally indicated that they have experienced a breach. In addition to DX and multi-cloud complexities, the global study shows that quantum computing has skyrocketed as a major concern with 72% of organizations claiming it will affect their security and cryptographic operations in the next five years.

Thales will host a **webinar,** "The Global State of Data Security: Zero Trust in a Multi-Cloud World," to discuss the global report in more detail on Thursday, March 5 at 11:00 a.m. ET. To join, please visit the registration page.

The rush for digital transformation and the security fallout

With input from 1,723 executives with responsibility for, or influence over, IT and data security around the world, this year's threat report dove deeper into the specific security challenges resulting from the "DX Era." The report revealed that the more digitally transformed, the more likely an organization is to

be breached. While organizations pursing DX are capturing competitive advantages, the worldwide rush to implement disruptive technologies is creating new vulnerabilities resulting in data breaches and compliance audit failures. According to the report, 45% of organizations in the top two DX categories, Software as a Service (SaaS) and social media, experienced a breach in the past year.

Multi-cloud is the new normal, but a top barrier to data security

Companies are using multiple Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) environments, as well as hundreds of SaaS applications. Eighty-one percent are using more than one IaaS vendor (*the U.S. figure is 86%),* 81% have more than one PaaS vendor *(the U.S. figure is 86%*), and 11% have more than 100 SaaS applications to manage. As more data migrates to the cloud, security becomes more complex. Nearly 40% of respondents rate complexity as their top perceived barrier to implementing data security, down slightly from 44% last year.

Quantum computing is on the horizon

The global report draws new attention to the anticipated impact of quantum computing. Within the next five years, 72% of organizations believe quantum computing power will affect their data security operations while 27% see it as a threat within the next year, highlighting the need for organizations to improve their post-quantum encryption strength.

Not all industries are embracing digital transformation at the same rate

The 2020 Thales Data Threat Report-Global Edition also explores how government, financial services, healthcare, and retail sectors embrace digital transformation in varying degrees and the associated security challenges. Global federal government organizations view themselves as most advanced, with nearly half (49%) of government respondents as either aggressively disrupting the markets they participate in, or are embedding, digital capabilities that enable greater enterprise agility. Healthcare followed closely at 47%, retail at 45%, and financial services at 30%. Fifty- four percent of financial services respondents experienced a data breach or failed compliance audit this year, followed by government at 52%, retail at 49%, and healthcare at just 37%.

Key takeaways for improving data security

Data security is challenging, but across big data, IoT and containers, encryption is a key driver for adoption and usage. Based on this year's findings, IDC recommends the following key strategies for security professionals:

- Invest in modern, hybrid and multi-cloud-based data security tools that make the shared responsibility model work.
- Consider a zero-trust model to secure data.
- Increase focus on data discovery solutions and centralization of key management to strengthen data security.
- Focus on the threat vectors within their control.
- Utilize encryption to remain vigilant against today's data risk reality.

For more key findings and security best practices, download a copy of the 2020 Thales Data Threat Report – Global Edition.

"As organizations face expanding and more complex cybersecurity challenges because of multi-cloud adoption and digital transformation, they need smarter and better ways to approach data protection. Zero trust is a fantastic initiative to authenticate and validate the users and devices accessing applications and networks but does little to protect sensitive data should those measures fail. Employing robust data discovery, hardening, data loss prevention, and encryption solutions provide an appropriate foundation for data security, completing the objective of pervasive cyber protection."

Frank Dickson, program vice president, cybersecurity products, IDC

"The Thales 2020 Data Threat Report-Global Edition clearly demonstrates that unprecedented amounts of sensitive data are being stored in multi-cloud environments by organizations all over the world. Having the right cloud security in place has never been more critical. As 5G networks are rolled out, IoT continues to expand and quantum computing creeps closer to becoming a reality, organizations must adopt a more modern data protection mindset. The first step towards protecting sensitive data is knowing where to find it. Once classified, this data should be encrypted and protected with a strong multi-cloud key management strategy."

Tina Stewart, vice president of global market strategy for cloud protection and licensing activity at Thales

Industry insight and views on the latest data security trends can be found on the Thales blog at blog.thalesesecurity.com.

Follow Thales on Twitter, LinkedIn, Facebook and YouTube**.**