THALES

PRESS RELEASE
December 4, 2019
Austin, Texas

Thales study: U.S. financial institutions have highest rate of data breaches despite strict compliance mandates

- *62% of U.S. financial service organizations experienced data breaches, but security spending and encryption rates are decreasing*
- *Data security is not keeping pace with rapid industry change being driven by digital transformation*
- *Top data security concerns are cyberterrorism, internal threats and industrial espionage*

©Thales

A new global study from Thales, with research from global market intelligence firm IDC, reveals that U.S. financial institutions have the highest rate of data breaches compared to other industries. In fact, nearly two thirds (62%) have experienced a breach in their history, and 41% had one occur in the last year alone. According to the 2019 Thales Data Threat Report – Financial Services Edition, U.S. financial services institutions are leading other industries when it comes to implementing digitally transformative technologies with nearly all (97%) surveyed claiming they use sensitive data within digitally transformative environments. However, the study also found that encryption rates for the U.S. organizations surveyed are 31% or less, even though sensitive financial and payment data remains an attractive target for cybercriminals.

"Today sensitive data resides in digitally transformative, complex environments that span multiple clouds. These low encryption rates indicate U.S. financial institutions have a false sense of security as they also have the highest rate of data breaches compared to other sectors studied," With the proliferation of cloud adoption, the advancement of new banking systems and strict data privacy regulations, there's a disconnect between the reality of how vulnerable data is and the lack of adequate protection being utilized. The important message this study underscores is that financial services institutions need new data security methods to protect precious data everywhere in today's digital IT landscape."

***Rivka Gerwitz Little, research director at IDC Financial Insights**.*

Pervasive digital transformation puts sensitive data at risk

Technologies such as big data, cloud, IoT, mobile payments and others introduce new threats to sensitive data. This year's report found that almost half (47%) of respondents said they're either aggressively disruptive in their use of these technologies or are tightly linking them to an agile management vision. As financial service organizations struggle to protect data in new technology environments, they become a prime target for malicious insiders and external attackers motivated by either financial gain or the desire to create chaos in financial systems. In fact, according to the report, external attackers are now the top threats:

- 54% – Cyberterrorists
- 50% - Partners with internal access
- 46% – Competitors
- 45% – Cybercriminals
- 44% – Nation states
- 44% - Other IT accounts

Security spending not on track with fast-changing technology

When financial institutions first began to open digital channels and enable mobility of both employees and customers, financial institutions invested in data protection. However, budgets have not kept up with fast-changing security threats. The report shows that security spending has decreased by 30 percentage points over the past year from 84% to 54%. Additionally, sophisticated fraud rings have trained their own machine learning platforms and bots to crack financial systems. The research also found that collaboration with third-party fintech partners to launch new services (open banking) is increasing the attack surface for cybercriminals, and creating opportunities for industrial espionage perpetrated by competitors who use the same partners.

Encryption – a fundamental control – is underutilized

A key finding of the report is that although organizations report having plans for adopting data security technologies, like encryption and tokenization, actual implementation rates are low. The survey uncovered that in some sensitive data use cases, less than a quarter of respondents said they were using encryption to protect cloud environments as well as newer sources like big data, blockchain, containers, IoT and mobile payments.

"Fraud and security teams are expected to be the enablers of innovation while securing an increasingly complex financial services environment. Rapid digital transformation is being driven by agile fintech start-ups and the open banking trend shows no signs of slowing down. In addition,

protecting sensitive data becomes even more difficult with shrinking security spending and encryption rates that are far too low. The report demonstrates the need for security professionals in the financial services sector to encrypt everything and adopt the right tools and technology that will protect sensitive data and mitigate risk during ongoing digital transformation initiatives."

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

Broad multi-cloud adoption in financial services sector

As with other industries studied, financial institutions are shifting resources to the cloud and are implementing complex hybrid and multi-cloud environments. In fact, nearly half of the respondents have 50 or more Software-as-a-Service (SaaS) applications, 83% have two or more Platform-as-a-Service (PaaS) applications and 85% of respondents have two or more Infrastructure-as-a-Service (IaaS) applications. Financial institutions are finding that managing multiple cloud instances introduces new challenges for their IT departments, so it is no surprise that more than half (53%) of those surveyed rated complexity as a top barrier to implementing data security.

Financial services face strict regulations

Financial institutions have to adhere to some of the toughest regulations and 87% say they are impacted by a variety of federal (Dodd-Frank and Sarbanes-Oxley), state (New York Department of Financial Service 500 and the California Consumer Privacy Act) and global (General Data Protection Regulation) privacy and compliance regulations. Fortunately, the report showed that U.S. financial services institutions use encryption and tokenization at higher rates than other industries studied, and more than half (57%) plan to use these technologies to help meet regulatory requirements.

Key IDC recommendations to help mitigate risk

IDC recommends the following key strategies for financial services security professionals as they work to continually digitally transform their organizations:

1. Focus on all threat vectors;
2. Invest in modern, hybrid and multi-cloud based data security solutions that scale to modern architectures;
3. Look for solutions that enable doing more with less;
4. Prioritize compliance issues; don't confuse compliance and security;
5. Data security, starting with encryption and access management, is an important part of the mix; and,
6. Invest in agility.

For more key findings and security best practices, download a copy of the 2019 Thales Data Threat Report – Financial Services Edition. Thales also will host a **webinar** about "The State of Data Security in Financial Services" on Thursday, Dec. 12 at 2:00 p.m. ET. To join, please visit the registration page.

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.

About Thales

Thales (Euronext Paris: HO) is a global technology leader shaping the world of tomorrow today. The Group provides solutions, services and products to customers in the aeronautics, space, transport, digital identity and security, and defence markets. With 80,000 employees in 68 countries, Thales generated sales of €19 billion in 2018 (on a pro forma basis including Gemalto). Thales is investing in particular in digital innovations — connectivity, Big Data, artificial intelligence and cybersecurity — technologies that support businesses, organizations and governments in their decisive moments.

PRESS CONTACT

Thales, Media Relations
Adam Kostecki
+1 (703) 838-5645
adam.kostecki@us.thalesgroup.com

PLEASE VISIT

Thales Group

Security

@Thalesgroup