
THALES

The Changing Face of Data Security

2019 Thales Data Threat Report – India Edition

The report concentrates on the results from 100 IT security professionals from Indian firms with responsibility for, or influence over, IT and data security from within a total survey set of 1,200 global respondents. Survey, reporting and analysis conducted by IDC, and sponsored by Thales.

Use of sensitive data with digital transformation is widespread

97%

of respondents will use sensitive data with digital transformation technologies.

THALES

less than

38%

of respondents are using **data encryption** within these environments today.

The reality of the multi-cloud enterprise

Multi-cloud environments make the task of protecting sensitive data more complex.

The rate of growth of security spend in U.S. retail is slowing

This year's study showed a decline in the rate of growth in security spending across the board, and the retail industry was no exception. The percent of global retail respondents telling us that security spend is increasing (53%) is down from Thales' report from last year (67%). In the U.S., 62% of retail firms say security budgets are increasing, down from 84% last year (see Figure 2). In the U.S., those who say spending will decrease went up slightly (12% compared to 9%) and the number saying their spend will stay the same nearly quadrupled (26% compared to 7%). But retail's spending slowdown is not as severe as other industries; those who say spending is increasing (53%) is higher than the global total (50%).

"This year's study showed a decline in the rate of growth in security spending across the board, and the retail industry was no exception."

Figure 2 – IT security spend in U.S. retailers
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

Of course, the budget conversation differs from retailer to retailer, with larger born-in-the-cloud retailers investing more and devoting greater focus to effect change. Smaller, brick-and-mortar-based retailers can struggle to match their spend levels in comparison. As security needs continue to cross multiple environments – on-premise as well as emerging cloud environments – providers will need to implement security tools and platforms designed for modern, hybrid and multicloud architectures, not jerry rigged from legacy technologies. Cloud based solutions delivered "as a service" and "as a platform" that cross environments are examples of such solutions that can reduce cost and complexity and make the job more manageable.

Threat vectors for retailers are broadening

One of the big messages coming from this year's data threat report is that no one is safe. Even the most sophisticated companies are getting breached, and in fact, our study shows that across all industries, the greater the level of sophistication, the more likely respondents are to say that they have been breached. Sixty four percent of companies across all industries that spend more than 10% of their IT budget on security say they have experienced at least one breach and, of those, 34% say that they have experienced a breach in the past year. Compare this to organizations that spend 10% or less of their IT budget on security.

Forty seven percent of those say that they have experienced at least one breach in the company's history, while 17% say that they experienced a breach in the last year. It may be that organizations that spend more are larger and more technology focused, and therefore have a greater attack surface contributing to an increased risk of being breached. Conversely, those that spend less are less mature and may be unaware of past breaches or have yet to discover ongoing ones. At the very least, the finding demonstrates that no matter the spend, no company can rest easy.

Looking at retailers in particular, a significant number report having experienced a breach, 62% of U.S. retail respondents say they have been breached at any point in their history, similar to U.S. financial services and federal government verticals (see Figure 3).

"Top concerns regarding data security threats are balanced between external and internal actors, with cyberterrorists, hacktivists, and IT administrators leading the list."

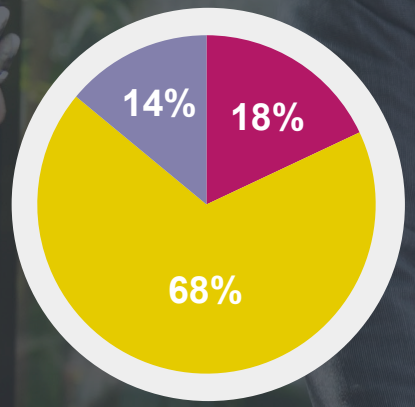
Figure 3 – Breach: Number ever (at any time)
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

They are also relatively concerned about their vulnerability: 39% of U.S. retailers consider themselves "very" or "extremely" vulnerable, a higher percentage than either their global counterparts or the global sample as a whole (see Figure 4).

Figure 4 – Vulnerable/very vulnerable to security threats (U.S.)
Source: 2019 Thales Data Threat Report Survey, IDC, November 2018

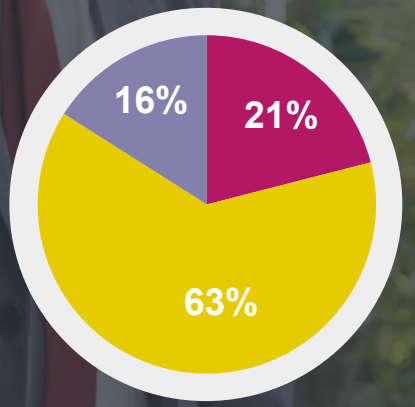
Number of cloud environments

THALES



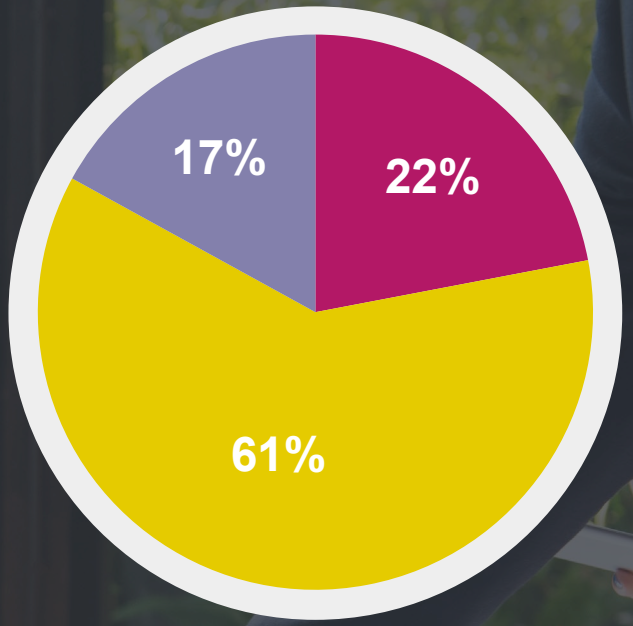
IaaS

- 4 or more
- 2 or 3
- 1



PaaS

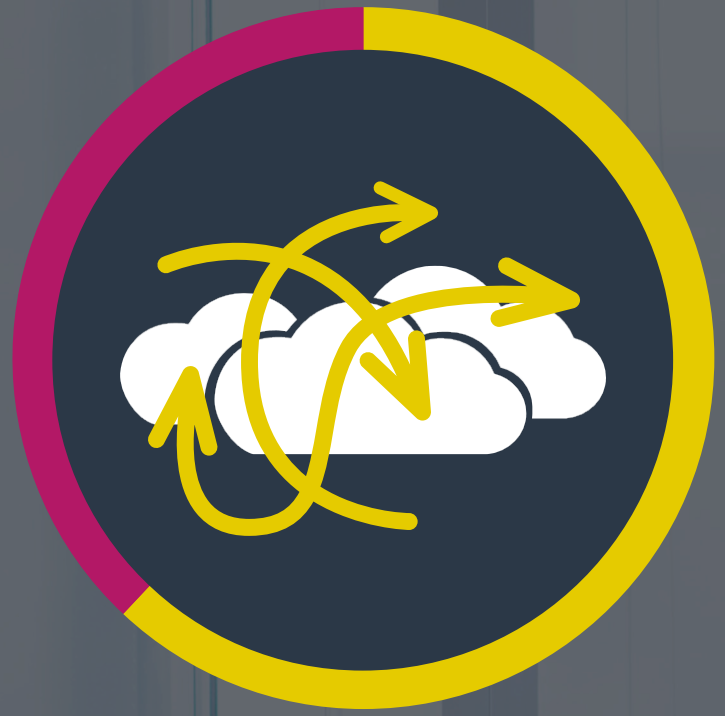
- 4 or more
- 2 or 3
- 1



SaaS

- More than 50
- 11 - 50
- 10 or less

THALES



Driven by the need to protect digital transformation's complex data environments,

62%

rated complexity as the top barrier to implementing data security.

Data breach resistance: No one is immune

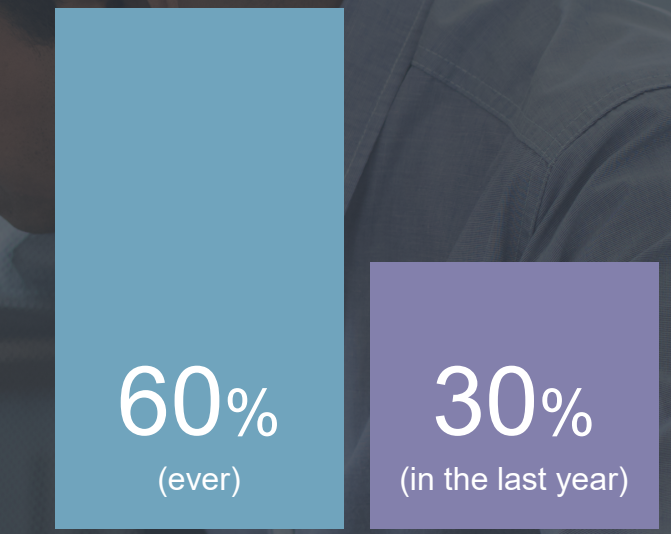
THALES

49%

of IT security professionals of Indian firms surveyed say that they have been breached at any time in their history, with…

20%

... breached in the last year.



Global Data Breach Rates

Encryption rates are low

Despite recognising the importance of protecting sensitive data, encryption rates throughout enterprises are surprisingly low.

THALES

38 or less %

say they use encryption for the vast majority of use cases studied

Data privacy and sovereignty regulations impact nearly all

Indian firms face a daunting array of privacy and compliance regulations such as UIDAI/AADHAAR, and the upcoming Data Protection Bill. Multinationals must also comply with international privacy laws such as the European GDPR.

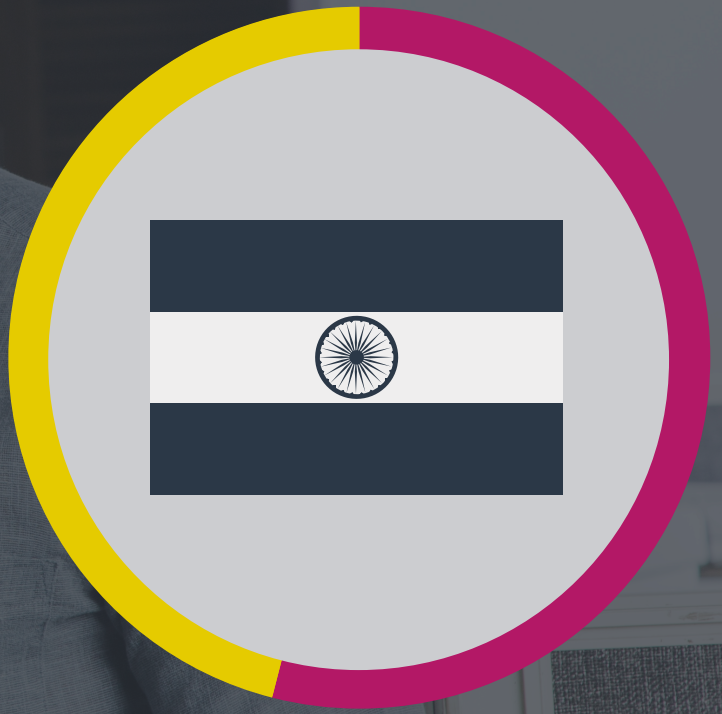
THALES

89%

will be affected by data privacy and sovereignty regulations.

60%

will use encryption and tokenization to meet these requirements.



Data Security doesn't have to be hard

Organisations need to take a fresh look at how they provide data security. Visit the Thales website to download the full report, including IDC recommendations.

IDC guidance/key takeaways

Data security is not easy. As they work to continue digitally transforming their operations, retailers must take care to ensure they are not introducing new security loopholes. This is particularly true of retailers that have been targets of a number of high-profile attacks in recent years. In particular, IDC recommends retail security professionals consider the following:

- **Focus on all threat vectors.** Today's threats come from all over, and retailers are a particular target in today's environment. As bad actors continue to evolve their methods, retailers need to continually evolve to guard against them. As guardians of sensitive customer data, retailers must take this responsibility seriously.
- **Invest in modern, hybrid and multi-cloud-based data security solutions that scale to modern architectures.** You can't protect against the myriad of data threats facing your organization with tools that are no longer sufficient to protect against the many of data threats facing your organization. With more devices at the edge, the expanding "threat surface" is increasingly borderless, so the legacy perimeter approach doesn't work. Retail providers must recognize the increased complexity of today's security environment and implement solutions that span legacy concerns as well as modern, cloud-based digital transformation technologies.
- **Look for solutions that let you do more with less.** Even as C-level executives understand the mandate for enterprise security, the free-spending days marked by astronomically increasing budgets and companies "throwing money at the problem" are on the decline. C-Os are questioning the ROI of security spending and security professionals are going to need to identify solutions that let them address multiple layers of security concerns in a cost effective manner. "As a service" and "platform" solutions that cross environments can help eliminate much of the complexity and cost, making the job much more manageable.
- **Prioritize compliance issues.** Retailers must stay well on top of regulations around the world governing the need to protect customer data. They must ensure they are not only diligently following current regulatory compliance mandates, but that they also have sufficient flexibility built into their technologies to handle new requirements when they emerge.
- **Don't confuse compliance and security.** Proactively addressing compliance is important, but addressing compliance in a "pass the annual audit" fashion is not a recipe for security success. Proactive data security is a 365-days-a-year job.
- **Data security, starting with encryption and access management, is an important part of the mix.** As data migrates away from the enterprise premises and to the cloud, network security is no longer sufficient to protect data. Retailers need new data security methods to protect precious data everywhere in today's digital IT landscape.

Principal analyst profiles

Frank Dickson
Frank Dickson is a Program Vice President within IDC's Security Products research practice. In this role, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

Leslie Hand
As Vice President for IDC Retail Insights, Leslie Hand is responsible for the research direction for IDC Retail Insights, and leads research activities in the digital transformation of retail omnichannel operations. Hand works with retailers and technology providers on developing best practices and strategies, aligned with where they are, and where they want to go, leveraging IDC quantitative and qualitative data sets.

About International Data Corporation (IDC)

IDC is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries.

IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG), the world's leading media, data and marketing services company that activates and engages the most influential technology buyers.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Follow us on:

Visit thalesesecurity.com/dtr-india

Thank you to our sponsors:

PURESTORAGE

CSA cloud security alliance SM

RESEARCH AND ANALYSIS FROM:

IDC ANALYZE THE FUTURE