

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.

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 in 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 their security spend is increasing (50%) is down from Toles' 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 they will decrease spend went up slightly (12% compared to 9%), and the number saying their spend will stay the same nearly tripled (62% 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.”

Category	2018	2019
Decrease	9%	12%
About the same	7%	26%
Increase	84%	62%

Figure 2 Rate of growth in U.S. retail
Source: 2019 Toles Data Threat Report Survey, IDC, November 2019

Of course, the budget conversation differs from retailer to retailer, with larger brands in the cloud retailers investing more and devoting greater focus to elastic change. Smaller, back-and-forth-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 multi-cloud architectures, not just rugged from legacy technologies. Cloud-based solutions delivered “as a service” and “as a platform” in 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 a breach in the past year. Conversely, 34% say they have experienced a breach in the past year. Conversely, 34% say that they have experienced a breach in the past year. Conversely, 34% say that they have experienced a breach in the past year. Conversely, 34% say that they have experienced a breach in the past year.

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

Forty-seven percent of those who 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 technologically 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 vendors (see Figure 3).

Industry	2019
Healthcare	70%
Retail	62%
Financial Services	62%
Federal	60%

Figure 3 Breach history across various industries
Source: 2019 Toles Data Threat Report Survey, IDC, November 2019

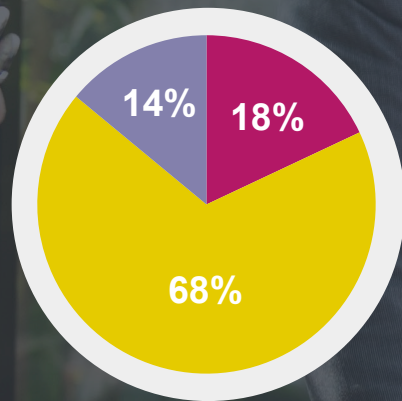
They are also relatively concerned about their vulnerability: 39% of U.S. retailers consider themselves “very” or “extremely” vulnerable, a higher percentage than either their global counterparts or the global sample as a whole (see Figure 4).

Category	2019
U.S. retail services	39%
Global retail services	34%
Global	34%

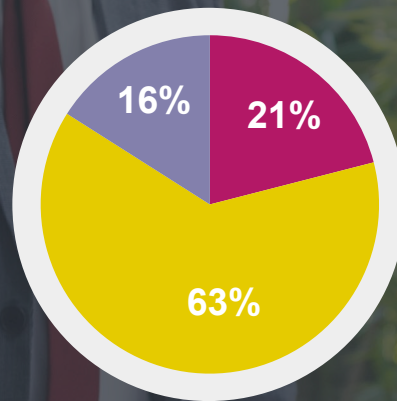
Figure 4 U.S. retailers very concerned to security threats (U.S.)
Source: 2019 Toles Data Threat Report Survey, IDC, November 2019

2019 Toles Data Threat Report | [View Edition](#)

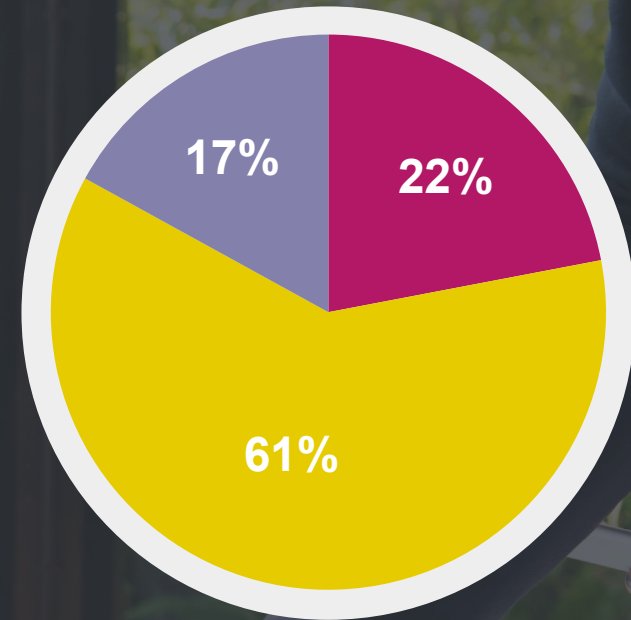
Number of cloud environments



IaaS

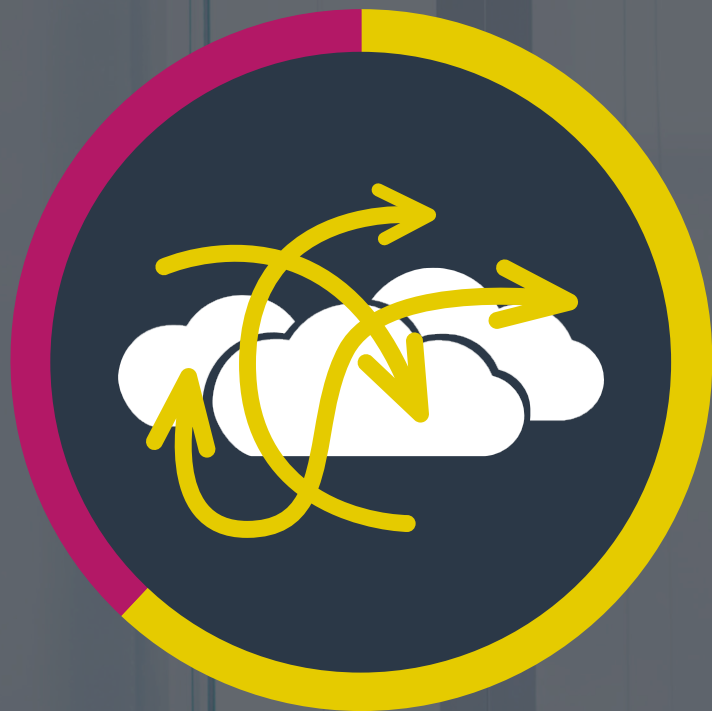


PaaS



SaaS





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

49%

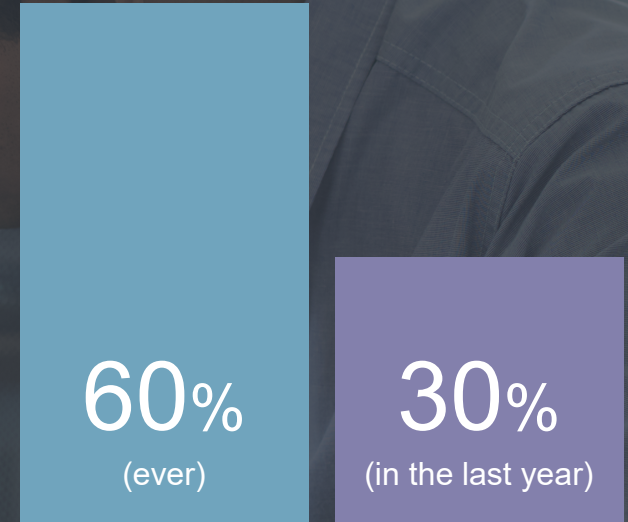
.....
of IT security professionals of Indian firms surveyed say that they have been breached at any time in their history, with...



.....

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.

Complicating life for retailers, the three vectors they face are extremely broad. U.S. retail respondents' top concerns regarding data security threats are balanced between external and internal actors, with cybercriminals, hacktivists, and IT less concerned with cybercriminals than either the global counterparts or the global sample as a whole. When retail becomes a digital business, its organizational crime elements are not previously plugged into a legal or security framework. These threats haven't faded, there is being addressed with video, sensors, and analytics that identify sources of revenue leakage.

“U.S. retailers are complacent. They have a false sense of complacency.”

The level of concern from the U.S. retail respondents for “cybercriminals” was surprisingly low, especially given the concerns voiced by global retail respondents. The interpretation of this research is that retailers are more complacent with increasing technology in a crowded market, not because of the importance of the business. In an era of digital, the sale, distribution or service (DOoS) attacks become the weapon of choice for hackers. In 2015, a retail listing provider (CVT) was hit with a record DOoS attack with peaks reaching 11.1Tbps. CVT was not the only provider of Microsoft listing services was. These providers are on the same platform, resulting in specific attacks. Likewise, the “byzantine” can have a devastating impact on the website of an “omni-channel” retailer. For example, Black Friday or Cyber Monday, the website of an “omni-channel” retailer is unavailable or critical lines such as Black Friday or Cyber Monday. For example, the website of an “omni-channel” retailer is unavailable or critical lines such as Black Friday or Cyber Monday. For example, the website of an “omni-channel” retailer is unavailable or critical lines such as Black Friday or Cyber Monday.

“Managing multiple cloud instances introduces challenges for retail IT departments. It is hard enough to encrypt, tokenize, and manage access to sensitive data within a single cloud instance, let alone dozens of them.”

Respondents believe they have adequate security, indicating a false sense of complacency.

Retailers generally believe they have adequate security, particularly in the U.S. Among the majority of U.S. retail respondents believe they have adequate security in new technology developments, 78% more than the global total of 68%. Seventy eight percent of them also believe they have adequate security in traditional technologies, which is generally in line with other U.S. verticals, but significantly higher than non-U.S. retail respondents and the rest of the global sample (see Figure 9).

The real cybercriminals became a real threat when the result of a security breach drove a significant and sustained loss of revenue and profit for the retailer impacted. When security breaches become a real threat, the cybercriminals that cybercriminals cause, the danger is evidenced by the large-scale loss of personally identifiable information (PII) such as credit card information. Retailers offer invest more in security to remediate the situation after a breach has occurred. Over the last few years, the U.S. has the highest number of 500 retailers, and with that the largest pool of consumer data to steal. It is surprising that investment levels are not higher.

Few cybercriminals' attacks have entered the public sphere, but retail respondents' concern over data loss is high, as is concern voiced by respondents from India, Mexico, and other geographies. While few cybercriminal activities are apparent today, we have seen the real threat of ransomware, and the awareness of the potential for cybercriminal attacks on the future is huge. And with large losses of sensitive customer data such as credit card information, retail has proven to be a high profile target in recent years.

Figure 8 Credit card usage by retail respondents worldwide (Q1 2016) (Percentage)

Country	U.S. Retailers	Global Retailers	Global
Canada	94%	88%	90%
France	93%	88%	90%
Germany	92%	88%	90%
India	91%	88%	90%
Japan	90%	88%	90%
UK	89%	88%	90%
U.S.	88%	88%	90%
Mexico	87%	88%	90%
Other	86%	88%	90%
China	85%	88%	90%
South Korea	84%	88%	90%
Spain	83%	88%	90%
Brazil	82%	88%	90%
Italy	81%	88%	90%
Other	80%	88%	90%
South Africa	79%	88%	90%
Other	78%	88%	90%

Figure 9 Retailers' belief in having adequate security in new technologies (Q1 2016) (Percentage)

Category	U.S. Retailers	Global	Global Retailers
Traditional technologies	78%	68%	69%
New technologies	78%	68%	69%
Both	16%	12%	13%

Figure 10 Retailers' belief in having adequate security in traditional technologies (Q1 2016) (Percentage)

Category	U.S. Retailers	Global	Global Retailers
Traditional technologies	78%	68%	69%
New technologies	16%	12%	13%
Both	6%	20%	18%

Figure 11 Retailers' belief in having adequate security in new technologies (Q1 2016) (Percentage)

Category	U.S. Retailers	Global	Global Retailers
Traditional technologies	6%	20%	18%
New technologies	16%	12%	13%
Both	78%	68%	69%

2016 Trust, Data, Trust & Power Report | Page 14

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.

Healthcare providers should look at mobile payments as a means of providing a convenient payment option for their patients.

As digital health-related components of any digital health solution in the form of...
...putting their patients at the center, but it is essential, contractor, or regulator...
...receives can engage with their customers in a more compelling manner and provide...
...a better overall experience. But edge technologies also increase complexity and...
...disruptions in connectivity. While cloud-based applications have helped to reduce...
...but in data, compliance, and blockchain are also enabling technology that help...
...expand and customize edge computing.

Mobile payments
Mobile in general, and mobile payments in particular, are an important part of...
...most retailers' online channels. U.S. retailers' concerns regarding mobile payments...
...rank the global market for mobile payments as the most important area of...
...investment of potentially disruptive technologies (PDT) over the next five years (see...
...see Figure 19).

Payment method	Smartphone	Other mobile device	Global
Online payment (percentage of total)	~45%	~35%	~40%
Mobile payment (percentage of total)	~35%	~25%	~30%
Mobile payment (percentage of total)	~25%	~15%	~20%
Mobile payment (percentage of total)	~15%	~10%	~15%
Mobile payment (percentage of total)	~10%	~5%	~10%
Mobile payment (percentage of total)	~5%	~2%	~5%

Internet of Things
U.S. retailers' primary concerns regarding Internet of Things (IoT) are providing...
...and sensitive data generated by or on devices, lack of IoT security standards, and...
...lack of secure connections/service authentication (see Figure 20) or the following...
...in general. Whether it is a smart home or a smart car, IoT devices, systems...
...integration to real-world, existing point-of-sale (POS) systems, HVAC, systems...
...industry. IoT devices and services systems are barcode readers to name a few...
...of security is not a one-size-fits-all problem, it is a retail challenge. Global retailers...
...and more concerned about IoT security. U.S. retailers are more concerned about...
...providing operational flexibility. U.S. retailers are more concerned about...
...more attention given to IoT security in their stores.

03 security concerns and methods of alleviation by data technology environment

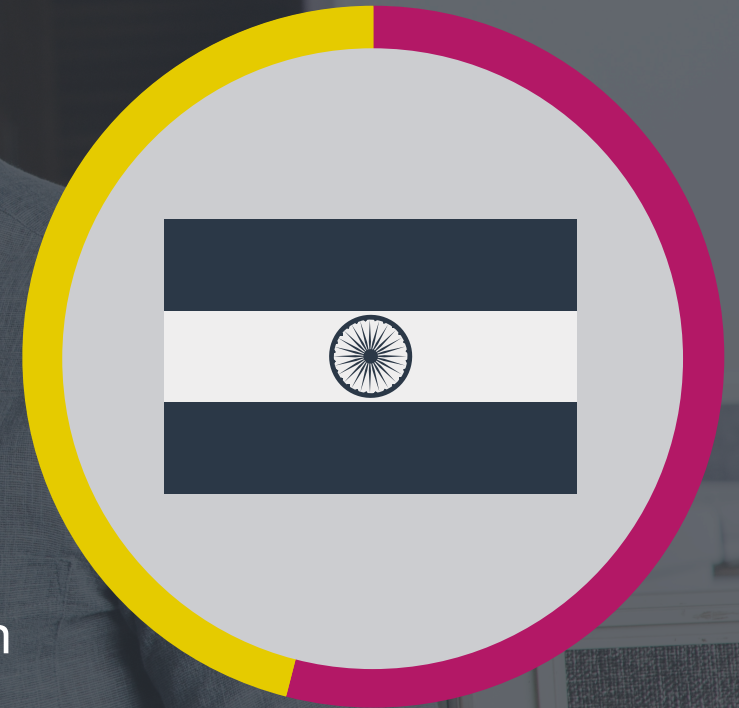
© 2017 Deloitte LLP

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 prime target. Today's environment, as well as the continuous evolution of threat vectors, means retailers need to continually evolve to guard against them. As a result, retailers need to take the responsibility seriously.

- **Invest in modern, hybrid and multi-cloud-based data security solutions that scale to modern architectures.** No one day's patch of security solutions will be sufficient to protect against the myriad of modern threats facing your organization. With more devices at the edge, the expanding threat surface, and increasingly sophisticated attacks, the legacy perimeter approach doesn't work. Retailers 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 time-spend money and the problem are on the decline. CIOs 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 result, retailers must look for solutions that can help eliminate much of the complexity and cost, making the job much more manageable.

- **Prioritize compliance issues.** Retailers must deal with a multitude of regulations around the world governing the need to protect consumer data. They must ensure they are not only compliant following current regulatory requirements, 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 ensuring compliance is a "pass the annual audit" fashion is not a recipe for security success. Proactive data security is a 365-day-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 landscape.

Principal analyst profiles



Frank Dickson

Frank Dickson is a Program Vice President with IDC's Security Products research practice. In his 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 cover transitioning a customer's 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 related to the digital transformation of retail operational 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, telecom, 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 analysts 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, and an operating service company that activates and engages the most influential technology buyers.

About Thales

The people you rely on to protect your security 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 Thales to secure your digital transformation.

Decisive technology for decisive moments.

Follow us on:



Thank you to
our sponsors:



RESEARCH AND ANALYSIS FROM:



Visit thalessecurity.com/dtr-india