Enterprises in India

- 100% - INR ₹6.7B, US $100M
- 62% - INR ₹3.35B, US $500M
- 37% - INR ₹67B, US $1B
Data Under Siege across India

Breaches rise even as digital transformation expands threat landscapes

Rates of data breaches in India

- **Breached ever**: 75%
  - 3 out of 4 have encountered a data breach
- **Breached in the last year**: 52%
- **Breached multiple times**: 23%
  - Over half breached in the last year
  - Have been breached in the last year and previously

Comparative breach rates

- **U.S.**
  - Breached ever: 71%
  - Breached in the last year: 46%
- **Europe**
  - Breached ever: 71%
  - Breached in the last year: 32%
- **Japan**
  - Breached ever: 39%
  - Breached in the last year: 9%
- **Korea**
  - Breached ever: 44%
  - Breached in the last year: 16%

Rates of data breaches in India: Breaches rise even as digital transformation expands threat landscapes.
Digital Transformation is Increasing Risks

The problem: massive adoption combined with sensitive data in India

Adoption rates for digitally transformative technologies

- 100% Use cloud
- 100% Use Big Data
- 100% Implement IoT
- 99% Working on or using mobile payments
- 99% Blockchain project implemented or in process

Rates of sensitive data use with digital transformation technologies

- 92% Cloud
- 55% Big Data
- 48% IoT
- 15% Containers
- 49% Mobile Payments
- 26% Blockchain
Doing what we have been doing for decades is no longer working. The more relevant question on the minds of IT and business leaders is directly spoken:

“What will it take to stop the breaches?”

Garrett Bekker - Principal Analyst for Information Security, 451 Research
Data Security Threats have Changed and Evolved
Security Strategies have Not

IT Security pros know data at rest security highly effective at protecting sensitive information – but aren’t prioritizing increased spending

- Data of rest defenses: 73% rated very or extremely effective, 36% spending increase
- Data in motion defenses: 72% rated very or extremely effective, 42% spending increase
- Analysis & correlation tools: 69% rated very or extremely effective, 44% spending increase
- Network defenses: 68% rated very or extremely effective, 44% spending increase
- Endpoint & mobile device defenses: 60% rated very or extremely effective, 51% spending increase
How Are Enterprises Responding? Massive Spending Increases

### IT Security Spending Plans For 2018 in India

<table>
<thead>
<tr>
<th>Response</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Much higher</td>
<td>56%</td>
</tr>
<tr>
<td>Somewhat higher</td>
<td>37%</td>
</tr>
<tr>
<td>The same</td>
<td>4%</td>
</tr>
<tr>
<td>Lower</td>
<td>3%</td>
</tr>
</tbody>
</table>

“A striking 93% of Indian respondents’ plan on increasing IT security spending this year, the highest among all countries surveyed and well above the global average (78%).”

How Are Enterprises Responding? Making Changes

Changing To Address Global and Local Data Privacy Requirements

- 30% Encrypting personal data
- 25% Tokenizing personal data
- 10% Migrating data
- 20% Using local cloud providers

Implementing Data Security Tools To Protect Sensitive Information

Implementing these tools now

- 73% Data masking
- 70% Database and file encryption
- 64% Cloud-native encryption tools
- 62% Data Loss Prevention tools (DLP)
Cloud Usage is the Top Problem

- **100%** Using cloud: Every enterprise using at least one of SaaS, IaaS or PaaS
- **47%** Cloud: Behind only Brand and Reputation as a top IT security spending priority
- **92%** Using sensitive data: In cloud environments

"As organizations increasingly engage with multiple cloud providers, who maintains control over encryption keys has become a huge potential issue, particularly for those who take advantage of native encryption services."

Garrett Bekker – Principal Analyst for Information Security, 451 Research

- **85%** Use more than 25 SaaS applications
- **65%** Use 2 or more IaaS vendors
- **96%** Using 2 or more PaaS environments

Multi-cloud usage is high, bringing even more risk
Cloud Computing Concerns and Required Security Tools

Top Concerns with Cloud Computing

- 86%: Lack of control over data location/data residency concerns
- 86%: Security breaches/attacks at the service provider
- 82%: Managing monitoring and deploying multiple cloud native security tools
- 81%: Managing encryption keys across multiple cloud environments

Top IT Security Tools Needed to Expand Cloud Computing Use

- 54%: Exposure of detailed security monitoring data
- 53%: Encryption with CSP key management
- 51%: Mapping of service provider admin roles
- 49%: Encryption with enterprise key management
- 48%: Compliance commitments

“Attacks and breaches at the cloud provider remains the top cloud security concern globally at 64%, up from 59% last year. India is even more concerned about security breaches and attacks at the service provider, ranking it at the top of the list concerns (86%) along with concerns about data residency (86%).”

Garrett Bekker – Principal Analyst for Information Security, 451 Research
Controlling Data in the Cloud

72% Very or extremely concerned about custodianship of cloud encryption keys

49% Would increase cloud use if able to control their own encryption keys from their data center

81% Are very or extremely concerned about managing encryption keys across multiple cloud providers

“As organizations increasingly engage with multiple cloud providers, who maintains control over encryption keys has become a huge potential issue, particularly for those who take advantage of native encryption services”

### Everybody is Using Big Data

Sensitive Data Use Compounds Problems

100%  
Of enterprises in India now use big data

55%  
Are using sensitive data within big data environments today

#### Top concerns for sensitive data within big data environments

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive data may be anywhere</td>
<td>44%</td>
</tr>
<tr>
<td>Security of reports</td>
<td>38%</td>
</tr>
<tr>
<td>Privileged user data access</td>
<td>35%</td>
</tr>
<tr>
<td>Privacy violations</td>
<td>35%</td>
</tr>
<tr>
<td>Lack of effective access controls</td>
<td>34%</td>
</tr>
</tbody>
</table>

#### What’s needed to speed Big Data adoption?

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved monitoring and reporting</td>
<td>46%</td>
</tr>
<tr>
<td>Stronger authentication</td>
<td>41%</td>
</tr>
<tr>
<td>Encryption and access controls within environment</td>
<td>38%</td>
</tr>
<tr>
<td>Data Masking within environment</td>
<td>38%</td>
</tr>
<tr>
<td>Sensitive data discovery/classification</td>
<td>37%</td>
</tr>
</tbody>
</table>
Mobile Payments on the Rise
Encryption Required

99%
Using or planning to use mobile payments

26% In pilot or testing
46% Evaluating
27% Already in production

47%
Are using sensitive data with mobile applications

Top concerns with mobile payments

54%
PII data
39%
Payment card information
44%
Weak authentication
37%
Fraudsters - account takeover
38%
Fraudsters - new account fraud

Encryption a key tool enabling safe use of mobile payments

- Encryption establishes secure identity with digital birth certificates for mobile devices
- Encryption protects data on devices
- Encryption protects data-in-transit
- Encryption and access controls help organizations meet compliance requirements for backend data stores

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part, or disclosed to a third party without prior written consent of Thales - Thales © 2017 All rights reserved.
**IoT**

**Encryption Required**

99% Using or planning to use IoT this year

**Top IoT Uses**
- Environmental: 47%
- Transportation: 41%
- Power/Energy: 40%

15% Are using sensitive data with IoT applications

**Top IT Security controls needed for further IoT adoption**
- Encryption of IoT data: 65%
- Secure digital IDs for IoT devices (Digital birth certificates): 56%
- Anti-malware: 54%
- Separate IoT networks with gateways: 49%
- Behavioral analytics/ anomaly detection: 47%

**Encryption a key tool enabling safe use of IoT**
- Encryption establishes secure identity with digital birth certificates for IoT devices
- Encryption protects data on devices
- Encryption protects data-in-transit
- Encryption and access controls help organizations meet compliance requirements for backend data stores
Encryption helps to drive adoption of the technologies needed for digital transformation

- **Cloud**: Required to increase cloud use (53%)
- **Big Data**: Encryption needed to drive adoption (38%)
- **IoT**: Encryption the top tool to increase ability to use IoT (48%)
- **Containers**: Encryption drives Container usage (42%)

**Encryption technologies 3 of the top 5 data security tools for this year (currently implementing):**

- Data masking: 73%
- Database/file encryption: 70%
- Data loss prevention: 62%
- Identity and access management: 61%
- Enabling cloud-native encryption capabilities: 64%

**Privacy Requirements**: Encryption the top tool needed to meet privacy requirements such as European GDPR (30%)
2018 Thales Data Threat Report

Trends in Encryption and Data Security

India Edition