2018 Thales Data Threat Report

Trends in Encryption and Data Security

Retail Edition
2018 Thales Data Threat Report - Respondent Demographics

1,200+ SENIOR IT SECURITY EXECUTIVES SURVEYED GLOBALLY
100 EACH INDIA, KOREA, JP, UK, DE, NE, SWE
500 U.S. TOTAL - 100 EACH RETAIL, HEALTHCARE, FINANCIAL SERVICES, FEDERAL GOVERNMENT
Data Under Siege in U.S. Retail

Breaches rise even as digital transformation expands threat landscapes

Rates of data breaches for U.S. Retail

- Breached ever: 75% (3 out of 4 have encountered a data breach)
- Breached in the last year: 50% (half breached in the last year)
- Breached multiple times: 26%

Comparative breach rates - U.S. verticals

- U.S. Retail: 75% (50% breached ever, 26% breached multiple times)
- U.S. Financial Services: 65% (36% breached ever, 29% breached multiple times)
- U.S. Federal Government: 70% (57% breached ever, 13% breached multiple times)
- U.S. Healthcare: 77% (48% breached ever, 29% breached multiple times)

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

- Use cloud: 100%
- Use Big Data: 95%
- Implement IoT: 99%
- Working on or using mobile payments: 98%
- Blockchain project implemented or in process: 92%

Rates of sensitive data use with digital transformation technologies

- Cloud: 85%
- Big Data: 56%
- IoT: 47%
- Containers: 39%
- Mobile Payments: 34%
- Blockchain: 31%
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**: 89% rated very or extremely effective, 57% spending increase
- **Data in motion defenses**: 90% rated very or extremely effective, 62% spending increase
- **Analysis & correlation tools**: 91% rated very or extremely effective, 69% spending increase
- **Network defenses**: 89% rated very or extremely effective, 64% spending increase
- **Endpoint & mobile device defenses**: 77% rated very or extremely effective, 72% spending increase
How Are Enterprises Responding? Massive Spending Increases

IT Security Spending Plans For 2018 in U.S. Retail

- Much higher: 28%
- Somewhat higher: 56%
- The same: 7%
- Lower: 9%

"Quite possibly in response to an uptick in breaches, 84% of U.S. retail respondents say their organizations will increase IT security spending this year, up sharply from last year (77%)."

How Are Enterprises Responding? Making Changes

Changing To Address Global and Local Data Privacy Requirements

- **49%** Encrypting personal data
- **12%** Tokenizing personal data
- **12%** Migrating data
- **13%** Using local cloud providers

Implementing Data Security Tools To Protect Sensitive Information

Implementing these tools now

- **75%** Database Access Monitoring
- **67%** Database and file encryption
- **74%** Data masking
- **63%** 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

49% The top IT security spending priority this year

85% 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

Multi-cloud usage is high, bringing even more risk

66% Use more than 25 SaaS applications

58% Use 3 or more IaaS vendors

57% Use 3 or more PaaS environments
Cloud Computing Concerns and Required Security Tools

### Top Concerns with Cloud Computing

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of control over data location/data residency concerns</td>
<td>80%</td>
</tr>
<tr>
<td>Security of data if cloud provider acquired</td>
<td>79%</td>
</tr>
<tr>
<td>Shared infrastructure vulnerabilities</td>
<td>78%</td>
</tr>
<tr>
<td>Security breaches/attacks at the service provider</td>
<td>78%</td>
</tr>
</tbody>
</table>

### Top IT Security Tools Needed to Expand Cloud Computing Use

<table>
<thead>
<tr>
<th>Tool</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed physical and IT security information</td>
<td>50%</td>
</tr>
<tr>
<td>Encryption with enterprise key management</td>
<td>49%</td>
</tr>
<tr>
<td>Encryption with CSP key management</td>
<td>49%</td>
</tr>
<tr>
<td>SLA terms in the event of a data breach</td>
<td>48%</td>
</tr>
<tr>
<td>Compliance commitments</td>
<td>38%</td>
</tr>
</tbody>
</table>

“Overall, U.S. retail is much more concerned about the IT security threats posed by the use of public cloud, likely because U.S. retail organizations are more likely to both use cloud and store sensitive data within cloud resources.”

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

- **67%** 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
- **72%** 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”


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.
Everybody is Using Big Data
Sensitive Data Use Compounds Problems

95%
Of enterprises in India now use big data

56%
Are using sensitive data within big data environments today

Top concerns for sensitive data within big data environments
- Sensitive data may be anywhere: 43%
- Security of reports: 38%
- Lack of security frameworks: 32%
- Privacy violations: 30%
- Lack of effective access controls: 32%

What's needed to speed Big Data adoption?
- Analyze and use encrypted data within the data lake: 46%
- Encryption and access controls: 44%
- Improved monitoring and reporting: 40%
- Stronger authentication: 39%
- Compliance certifications: 36%
# Mobile Payments on the Rise

Encryption Required

- **98%** Using or planning to use mobile payments
- **32%** In pilot or testing
- **48%** Evaluating
- **18%** Already in production

- **36%** Are using sensitive data with mobile applications

#### Top concerns with mobile payments

<table>
<thead>
<tr>
<th>Concern</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII data</td>
<td>45%</td>
</tr>
<tr>
<td>Payment card information</td>
<td>49%</td>
</tr>
<tr>
<td>Weak authentication</td>
<td>43%</td>
</tr>
<tr>
<td>Fraudsers - account takeover</td>
<td>50%</td>
</tr>
<tr>
<td>Fraudsers - new account fraud</td>
<td>45%</td>
</tr>
</tbody>
</table>

#### 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 back end data stores
IoT Encryption Required

99% of respondents are using or planning to use IoT this year.

Top IoT Uses:
- Manufacturing: 42%
- Power/Energy: 39%
- Environmental Monitoring: 38%

47% of respondents 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 - A Keystone Technology
For Protecting Data

Encryption helps to drive adoption of the technologies needed for digital transformation

Cloud: Encryption the top control needed for more cloud
- 49%

Big Data: Encryption needed to drive adoption
- 44%

IoT: Encryption the top tool to increase ability to use IoT
- 65%

Containers: Encryption drives Container usage
- 46%

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

- 49% - Privacy Requirements: Encryption the top tool needed to meet privacy requirements such as European GDPR
- 43% - CASB/Cloud Encryption Gateway
- 42% - SIEM
- 40% - Application Encryption
- 38% - Multifactor Authentication
- 35% - Tokenization
2018 Thales Data Threat Report

Trends in Encryption and Data Security

Retail Edition