“OUR 2017 REPORT FINDS A SITUATION WHERE SPENDING ON IT SECURITY IS SHARPLY INCREASED IN MEXICO – YET DATA BREACHES ARE ALSO UP SIGNIFICANTLY.”

“FUNDAMENTAL IT SECURITY STRATEGIES ARE ALSO NOT KEEPING UP WITH THE PACE OF TECHNICAL CHANGE. 75% OF MEXICAN RESPONDENTS INDICATED THAT NEW TECHNOLOGIES ARE DEPLOYED BEFORE DATA SECURITY IS IN PLACE”

“CLEARLY, THERE’S STILL A BIG DISCONNECT.”
OF MEXICAN RESPONDENTS FELT THEIR ORGANIZATIONS WERE VULNERABLE TO DATA THREATS

90%

WERE VERY OR EXTREMELY VULNERABLE – MORE THAN 3X THE 10% RATE IN 2016

31%
78% HAVE EXPERIENCED A DATA BREACH

- HIGHEST RATE MEASURED
- 34% IN THE LAST YEAR - UP FROM 10% IN 2016
- 19% WERE BREACHED BOTH THIS YEAR AND PREVIOUSLY

79% EXPECT THEIR SPENDING ON DATA SECURITY TO INCREASE

UP FROM 65% IN 2016
TOP DRIVERS FOR IT SECURITY SPENDING

Even with “LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES” in place - Preventing data breaches is only the third highest priority.

IT SECURITY SPENDING PRIORITIES (RATES OF TOP 3 SELECTION)

- 47% IT SECURITY BEST PRACTICES
- 42% INCREASED CLOUD USE
- 40% DATA BREACH PENALTIES
- 37% REPUTATION AND BRAND PROTECTION
- 30% EXECUTIVE DIRECTIVE
- 25% COMPLIANCE REQUIREMENTS
- 24% PARTNER AND PROSPECT REQUIREMENTS
- 24% COMPETITIVE/STRATEGIC CONCERNS
- 18% PREVIOUS DATA BREACH

DATA BREACH PREVENTION A LOWER PRIORITY IN SPITE OF FINES AND HIGHEST DATA BREACH RATES IN THE WORLD,

- 78% HIGHEST RATE OF DATA BREACHES MEASURED
- FINES UP TO 320,000 TIMES MEXICO CITY MINIMUM WAGE (LFPDPPP)
- $23M+ MXN
Increasing spending the most where defenses often fail to protect data

91% Believe Network Security Very/Extremely Effective at Protecting Data

77% Believe Endpoint Protection Very/Extremely Effective at Protecting Data

IT Security Defense Spending Increases

<table>
<thead>
<tr>
<th>Network</th>
<th>67%</th>
</tr>
</thead>
<tbody>
<tr>
<td>End Point &amp; Mobile</td>
<td>60%</td>
</tr>
<tr>
<td>Analysis &amp; Correlation</td>
<td>64%</td>
</tr>
<tr>
<td>Data in Motion</td>
<td>61%</td>
</tr>
<tr>
<td>Data at Rest</td>
<td>44%</td>
</tr>
</tbody>
</table>

“...spending on securing internal networks from external threats is less and less effective – and relevant – as both the data and the people accessing it are increasingly external.”

“...organizations keep spending on the same solutions that worked for them in the past but aren’t necessarily the most effective at stopping modern breaches”

Garrett Bekker, 451 Research
Data privacy has become a hot topic in light of concerns about government snooping, and not surprisingly a host of new privacy laws and regulations are in the process of being revised or enacted around the world, such as GDPR in Europe and LFPDPPP in Mexico.

Garrett Bekker
Principal Analyst
451 Research
### Perceived Complexity as the Top Barrier to Adoption Data Security

48% of respondents perceive complexity as the top barrier to adopting data security solutions. This is a 2% decrease from 2016.

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Perceived Barriers</th>
</tr>
</thead>
<tbody>
<tr>
<td>48%</td>
<td>Complexity</td>
</tr>
<tr>
<td>46%</td>
<td>Lack of Staff to Manage</td>
</tr>
<tr>
<td>40%</td>
<td>Lack of Perceived Need</td>
</tr>
<tr>
<td>39%</td>
<td>Lack of Organizational Buy In</td>
</tr>
<tr>
<td>31%</td>
<td>Potential Performance Impact</td>
</tr>
<tr>
<td>30%</td>
<td>Lack of Budget</td>
</tr>
</tbody>
</table>

---

“...The lack of skilled security staff has been a consistent theme in 451’s research efforts the past few years, and in conjunction with complexity, makes a strong case for data security functionality delivered as a service.”

Garrett Bekker
451 Research
**75%** OF ORGANIZATIONS SURVEYED ARE DEPLOYING NEW TECHNOLOGIES IN ADVANCE OF HAVING APPROPRIATE LEVELS OF DATA SECURITY IN PLACE

**99%** WILL USE SENSITIVE DATA IN AT LEAST ONE OF THESE ADVANCED TECHNOLOGY ENVIRONMENTS

### Rates of Sensitive Data Use by Environment Type

<table>
<thead>
<tr>
<th>Environment Type</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAAS</td>
<td>60%</td>
</tr>
<tr>
<td>IAAS</td>
<td>61%</td>
</tr>
<tr>
<td>PAAS</td>
<td>63%</td>
</tr>
<tr>
<td>MOBILE</td>
<td>45%</td>
</tr>
<tr>
<td>BIG DATA</td>
<td>39%</td>
</tr>
<tr>
<td>IOT</td>
<td>42%</td>
</tr>
<tr>
<td>CONTAINERS</td>
<td>22%</td>
</tr>
<tr>
<td>BLOCKCHAIN</td>
<td>15%</td>
</tr>
</tbody>
</table>
## Enterprise Concerns with Cloud/SAAS Environments

### Threats - Rates of Very or Extremely Concerned

<table>
<thead>
<tr>
<th></th>
<th>Mexico</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Privileged User Abuse/Threats</td>
<td>81%</td>
<td>53%</td>
</tr>
<tr>
<td>Security Breaches/Attacks at CSP</td>
<td>78%</td>
<td>59%</td>
</tr>
<tr>
<td>Custodianship of Encryption Keys</td>
<td>76%</td>
<td>51%</td>
</tr>
<tr>
<td>Shared Infrastructure Vulnerabilities</td>
<td>75%</td>
<td>57%</td>
</tr>
<tr>
<td>Lack of Data Privacy Policy/SLA</td>
<td>69%</td>
<td>52%</td>
</tr>
<tr>
<td>Meeting Compliance Requirements</td>
<td>66%</td>
<td>47%</td>
</tr>
<tr>
<td>Lack of Data Location Control</td>
<td>64%</td>
<td>55%</td>
</tr>
<tr>
<td>Lack of Visibility into Security Practices</td>
<td>63% (Japan)</td>
<td>50% (Global)</td>
</tr>
</tbody>
</table>

### Concerns with Sensitive Data in Cloud Environments

Are also high, with over half of respondents listing them as environments where they are concerned about using sensitive data.

- **PAAS**: 57%
- **SAAS**: 56%
- **IAAS**: 56%
WHAT CAN CSPS AND SAAS PROVIDERS DO TO INCREASE ENTERPRISE CLOUD ADOPTION IN MEXICO?

**Data Encryption in the Cloud with Enterprise Premise Key Control**
- **Mexico**: 64%
- **Global**: 61%

**SLA Agreements and Liability Terms for Data Breaches**
- **Mexico**: 56%
- **Global**: 49%

**Data Encryption in the Cloud with CSP Key Control**
- **Mexico**: 50%
- **Global**: 51%

**Support for Cloud HSMs**
- **Mexico**: 48%
- **Global**: 42%

**Consistently the first or second choice that would increase enterprise use of cloud worldwide is encryption with enterprise premise key control.**

<table>
<thead>
<tr>
<th>Country</th>
<th>Data Encryption</th>
<th>SLAs and Liability Terms</th>
<th>Data Encryption</th>
<th>Support for Cloud HSMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mexico</td>
<td>64%</td>
<td>56%</td>
<td>50%</td>
<td>48%</td>
</tr>
<tr>
<td>Global</td>
<td>61%</td>
<td>49%</td>
<td>51%</td>
<td>42%</td>
</tr>
</tbody>
</table>

**Additional Countries:**
- **U.S.**: 66%
- **Brazil**: 61%
- **U.K.**: 62%
- **Germany**: 50%
- **Japan**: 49%
BIG DATA - TOP DATA SECURITY CONCERNS AND STATS

**TOP 5 CONCERNS**

1. **47% MEXICO**  
   Security of reports that may include sensitive data

2. **44% GLOBAL**  
   Security of reports that may include sensitive data

3. **36% MEXICO**  
   Sensitive data may reside anywhere

4. **45% GLOBAL**  
   Sensitive data may reside anywhere

5. **42% MEXICO**  
   Privacy violations - data originates in many countries

6. **35% GLOBAL**  
   Privacy violations - data originates in many countries

7. **46% MEXICO**  
   Privileged user access to protected data

8. **36% GLOBAL**  
   Privileged user access to protected data

9. **34% MEXICO**  
   Lack of effective access controls

10. **31% GLOBAL**  
    Lack of effective access controls

- **40% MEXICO**  
  Using encryption to protect data in big data environments today

- **36% GLOBAL**  
  Using encryption to protect data in big data environments today

- **39% MEXICO**  
  Using sensitive information in big data environments

- **47% GLOBAL**  
  Using sensitive information in big data environments

- **49% MEXICO**  
  Very concerned about sensitive information in big data without data security controls

- **44% GLOBAL**  
  Very concerned about sensitive information in big data without data security controls

---

Research

THALES
ENTERPRISES IN MEXICO HAVE HIGH IOT ADOPTION
USE OF SENSITIVE DATA A CONCERN

95% ADOPTING IOT TECHNOLOGIES

27% USING SENSITIVE DATA IN IOT

32% VERY CONCERNED ABOUT SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

- 46% - PROTECTING SENSITIVE DATA GENERATED BY IOT
- 37% - PRIVILEGED USER ACCESS TO IOT DEVICES
- 32% - PRIVACY VIOLATIONS FROM IOT DATA
- 30% - IDENTIFYING WHICH DATA IS SENSITIVE
- 28% - IOT ATTACK OPS IMPACT

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

- 67% SECURE ID AND AUTHENTICATION
- 58% - IOT NETWORK ISOLATION
- 57% - ENCRYPTION OF DATA
- 52% - ANOMALY DETECTION/BEHAVIORAL ANALYSIS
- 51% - ANTI-MALWARE FOR DEVICES

95% ADOPTING IOT TECHNOLOGIES

27% USING SENSITIVE DATA IN IOT

32% VERY CONCERNED ABOUT SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

- 46% - PROTECTING SENSITIVE DATA GENERATED BY IOT
- 37% - PRIVILEGED USER ACCESS TO IOT DEVICES
- 32% - PRIVACY VIOLATIONS FROM IOT DATA
- 30% - IDENTIFYING WHICH DATA IS SENSITIVE
- 28% - IOT ATTACK OPS IMPACT

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

- 67% SECURE ID AND AUTHENTICATION
- 58% - IOT NETWORK ISOLATION
- 57% - ENCRYPTION OF DATA
- 52% - ANOMALY DETECTION/BEHAVIORAL ANALYSIS
- 51% - ANTI-MALWARE FOR DEVICES

95% ADOPTING IOT TECHNOLOGIES

27% USING SENSITIVE DATA IN IOT

32% VERY CONCERNED ABOUT SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

- 46% - PROTECTING SENSITIVE DATA GENERATED BY IOT
- 37% - PRIVILEGED USER ACCESS TO IOT DEVICES
- 32% - PRIVACY VIOLATIONS FROM IOT DATA
- 30% - IDENTIFYING WHICH DATA IS SENSITIVE
- 28% - IOT ATTACK OPS IMPACT

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

- 67% SECURE ID AND AUTHENTICATION
- 58% - IOT NETWORK ISOLATION
- 57% - ENCRYPTION OF DATA
- 52% - ANOMALY DETECTION/BEHAVIORAL ANALYSIS
- 51% - ANTI-MALWARE FOR DEVICES

95% ADOPTING IOT TECHNOLOGIES

27% USING SENSITIVE DATA IN IOT

32% VERY CONCERNED ABOUT SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

- 46% - PROTECTING SENSITIVE DATA GENERATED BY IOT
- 37% - PRIVILEGED USER ACCESS TO IOT DEVICES
- 32% - PRIVACY VIOLATIONS FROM IOT DATA
- 30% - IDENTIFYING WHICH DATA IS SENSITIVE
- 28% - IOT ATTACK OPS IMPACT

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

- 67% SECURE ID AND AUTHENTICATION
- 58% - IOT NETWORK ISOLATION
- 57% - ENCRYPTION OF DATA
- 52% - ANOMALY DETECTION/BEHAVIORAL ANALYSIS
- 51% - ANTI-MALWARE FOR DEVICES

95% ADOPTING IOT TECHNOLOGIES

27% USING SENSITIVE DATA IN IOT

32% VERY CONCERNED ABOUT SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

- 46% - PROTECTING SENSITIVE DATA GENERATED BY IOT
- 37% - PRIVILEGED USER ACCESS TO IOT DEVICES
- 32% - PRIVACY VIOLATIONS FROM IOT DATA
- 30% - IDENTIFYING WHICH DATA IS SENSITIVE
- 28% - IOT ATTACK OPS IMPACT

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

- 67% SECURE ID AND AUTHENTICATION
- 58% - IOT NETWORK ISOLATION
- 57% - ENCRYPTION OF DATA
- 52% - ANOMALY DETECTION/BEHAVIORAL ANALYSIS
- 51% - ANTI-MALWARE FOR DEVICES
## Top Security Controls Needed to Increase Container Adoption and Use in Mexico

**97%**

Plan to deploy container technology by end of 2017

Security the top barrier to container deployment

### Mexico

- **37%** Encryption
- **55%** Anti-Malware
- **46%** Vulnerability Scanning
- **38%** Monitoring tools for containers
- **37%** Digital Signature Image Validation

### Global

- **45%** Encryption
- **53%** Anti-Malware
- **42%** Vulnerability Scanning
- **36%** Monitoring tools for containers
- **31%** Digital Signature Image Validation

---

451 Research

Thales
<table>
<thead>
<tr>
<th>Category</th>
<th>Mexico</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud</strong></td>
<td>64%</td>
<td>61%</td>
</tr>
<tr>
<td><strong>Big Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption Enables Further Adoption of Cloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Encryption in the Cloud with Enterprise Premise Key Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IoT</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption Offsets Top Security Concerns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged User Access</td>
<td>46%</td>
<td>36%</td>
</tr>
<tr>
<td>Security of Reports</td>
<td>47%</td>
<td>44%</td>
</tr>
<tr>
<td>Sensitive Data Everywhere</td>
<td>36%</td>
<td>45%</td>
</tr>
<tr>
<td><strong>Containers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption a Top Control Needed to Enable Greater Adoption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Digital Identity (an Encryption Technology)</td>
<td>57%</td>
<td>56%</td>
</tr>
<tr>
<td>Secure Digital Identity (an Encryption Technology)</td>
<td>67%</td>
<td>55%</td>
</tr>
</tbody>
</table>

*Research*
## BEST PRACTICE RECOMMENDATIONS

**GARRETT BEEKER, 451 RESEARCH**

| Re-prioritize your IT security tool set | Cloud and SaaS break legacy IT Security models - Data security with encryption and access controls across environments is required. Service-based solutions and platforms that include automation are preferred for reduced costs and simplicity. |
| Discover and classify | Get a better handle on the location of sensitive data, particularly for Cloud, Big Data, Containers and IoT |
| Don’t just check off the compliance box | Global and industry regulations can be demanding, but agencies should consider moving beyond compliance to greater use of encryption and BYOK, especially for cloud and other advanced technology environments. |
| Encryption and access control | Encryption needs to move beyond laptops and desktops. **Data center:** File and application level encryption and access controls. **Cloud:** Encrypt and manage keys locally, BYOK enables safe SaaS, PaaS and IaaS. **Big Data:** Encryption and access control within the environment. **Containers:** Encrypt and control access to data both within containers and underlying data storage locations. **IoT:** Use secure device ID and authentication, as well as encryption of data at rest on devices, back end systems and in transit to limit data threats. |
**Instilling trust across the data landscape**
Our powerful technology platform provides advanced data security for more servers, applications, and environments than any other security alternative.

**What we do**
Thales e-Security provides companies everything they need to protect and manage their data and scale easily to new environments and requirements—encryption, advanced key management, tokenization, authorization, privileged user control, and HSMs.

**Our customers**
Our customers include 19 of the world’s 20 largest banks, four of the world’s five largest oil companies, 27 NATO country members and 15 of the Fortune 25.
Our solutions protect data while eliminating complexity, inefficiency and cost.

**Data Protection**
- **Hardware**
  - DB/ File Encryption
  - Application Encryption
  - Big Data
  - Code Signing
  - Tokenization
  - Transaction Security
  - Public Key Infra (PKI)
  - Cloud Security

**Software**
- **Customer Records**
  - PII
  - Secure Analytics
  - Script Development
  - PCI, PHI
  - Payment related apps
  - Internet of Things
  - Cloud Migration

**Use Cases**
- Cloud Migration
- Cloud Security
- Payment related apps
- Transaction Security
- Public Key Infra (PKI)
- Internet of Things
- Script Development
- Code Signing
- Tokenization
- Big Data
- Application Encryption
- DB/ File Encryption

**Data Protection Hardware**
- Transparent Encryption
- Application Encryption
- Tokenization
- Encryption Gateway
- Key Management
- Security Intelligence

**Data Protection Software**