2017 Thales Data Threat Report
Trends in Encryption and Data Protection

Respondents
Organizations (All)
- 73% - $500M or more
- 48% - $1B or more
- All US - $250M+
- All Global - $150M+

Copyright 2017 Thales
“The U.S. Federal Government is racing to boost data security against odds not faced in the private sector.... the U.S. government spent $14 billion last fiscal year on information and cyber security, and a Federal Cybersecurity Workforce Strategy published last year called for hiring of an additional 3500 ‘critical cyber security’ positions in 2017”

Garrett Bekker, 451 Research

* Global = Outside the U.S. results
STAFFING AND BUDGETS TOP BARRIERS TO DATA SECURITY

“U.S. FEDERAL ALSO HOLDS THE DUBIOUS TITLE OF LEADING OTHER VERTICAL AREAS AND COUNTRIES IN TERMS OF EXPERIENCING A SUCCESSFUL DATA BREACH IN THE PAST YEAR AT 34% ....”

“BUDGET CONSTRAINTS AND STAFFING SHORTAGES ARE BOTH CITED BY 53% OF U.S. FEDERAL RESPONDENTS AS THE CHIEF BARRIERS TO SECURITY INITIATIVES”
“U.S. federal also holds the dubious title of leading other vertical areas and countries in terms of experiencing a successful data breach in the past year at 34%, well above the global average of 26% and the average of all U.S. verticals of 24%.”

Garrett Bekker
Principal Analyst, Information Security, 451 Research

U.S. FEDERAL DATA BREACHES

IN THE LAST YEAR

2016: 22%
2017: 34%

AT ANOTHER TIME

2016: 44%
2017: 45%

DATA BREACHES BY U.S. VERTICAL

HEALTHCARE

EVER: 47%
IN THE LAST YEAR: 20%

RETAIL

EVER: 52%
IN THE LAST YEAR: 19%

FINANCIAL SERVICES

EVER: 42%
IN THE LAST YEAR: 24%

FEDERAL GOVERNMENT

EVER: 65%
IN THE LAST YEAR: 34%
96% of U.S. federal respondents report feeling vulnerable to threats to sensitive data, the highest of any other region or vertical surveyed. 

Garrett Bekker
Principal Analyst, Information Security, 451 Research

<table>
<thead>
<tr>
<th>Verticals</th>
<th>Healthcare</th>
<th>Retail</th>
<th>Financial Services</th>
<th>Federal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very or Extremely Vulnerable</td>
<td>29%</td>
<td>19%</td>
<td>27%</td>
<td>48%</td>
</tr>
<tr>
<td>Somewhat or More Vulnerable</td>
<td>90%</td>
<td>85%</td>
<td>86%</td>
<td>96%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verticals</th>
<th>Healthcare</th>
<th>Retail</th>
<th>Financial Services</th>
<th>Federal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very or Extremely Vulnerable</td>
<td>47%</td>
<td>37%</td>
<td>44%</td>
<td>31%</td>
</tr>
<tr>
<td>Somewhat or More Vulnerable</td>
<td>88%</td>
<td>88%</td>
<td>90%</td>
<td>88%</td>
</tr>
</tbody>
</table>
71% of U.S. federal respondents surveyed are deploying new technologies in advance of having appropriate levels of data security in place.

92% will use sensitive data in at least one of these advanced technology environments.

- **64%**: SAAS
- **62%**: IAAS
- **55%**: PAAS
- **41%**: MOBILE
- **59%**: BIG DATA
- **25%**: IOT
- **27%**: CONTAINERS
- **14%**: BLOCKCHAIN

*U.S. Results*
“While complexity is the main barrier to data security in most regions, for the U.S. Federal sector budget (53%, well ahead of global average of 33%), and lack of staff (also 53%) are the main challenges — though complexity remains the top barrier for Global Federal.”

Garrett Bekker
451 Research
“... the U.S. government spent $14 billion last fiscal year on information and cyber security”

“While most regions and verticals showed big year-over-year increases in spending plans, U.S. Federal showed a meager increase, to 61% from 58% in 2016.”

Garrett Bekker  
Principal Analyst, Information Security, 451 Research
“...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

“... 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.”

### IT Security Defense Spending Increases

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>62%</td>
</tr>
<tr>
<td>End Point and Mobile</td>
<td>52%</td>
</tr>
<tr>
<td>Analysis and Correlation</td>
<td>53%</td>
</tr>
<tr>
<td>Data in Motion</td>
<td>57%</td>
</tr>
<tr>
<td>Data at Rest</td>
<td>42%</td>
</tr>
</tbody>
</table>

### Rates of Effectiveness for Protecting Data

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>72%</td>
</tr>
<tr>
<td>End Point and Mobile</td>
<td>66%</td>
</tr>
<tr>
<td>Analysis and Correlation</td>
<td>72%</td>
</tr>
<tr>
<td>Data in Motion</td>
<td>68%</td>
</tr>
<tr>
<td>Data at Rest</td>
<td>71%</td>
</tr>
</tbody>
</table>

* U.S. Results
### DATA PRIVACY AND SOVEREIGNTY
**IMPACTING FEDERAL AGENCIES WORLDWIDE**

**73% - U.S. Federal**

**71% - Global Federal**

*Impacted by Data Privacy and Data Sovereignty*

### ADDRESSING REQUIREMENTS BY:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>U.S.</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypting Data</td>
<td>60%</td>
<td>58%</td>
</tr>
<tr>
<td>Tokenizing Data</td>
<td>53%</td>
<td>28%</td>
</tr>
<tr>
<td>Migrate Data</td>
<td>54%</td>
<td>23%</td>
</tr>
<tr>
<td>Local Hosting &amp; Cloud</td>
<td>40%</td>
<td>29%</td>
</tr>
</tbody>
</table>

*Garrett Bekker*
*Principal Analyst*
*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 the amended APPI in Japan.”*
“... external attackers frequently masquerade as insiders by using stolen or compromised credentials to access all types of valuable data, including PII, PHI, financial data and intellectual property.”

Garrett Bekker
Principal Analyst Information Security, 451 Research

### The Most Dangerous Insiders

<table>
<thead>
<tr>
<th>Role</th>
<th>U.S. Federal</th>
<th>Global Federal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged Users</td>
<td>59%</td>
<td>62%</td>
</tr>
<tr>
<td>Executive Management</td>
<td>55%</td>
<td>38%</td>
</tr>
<tr>
<td>Ordinary Employees</td>
<td>40%</td>
<td>50%</td>
</tr>
<tr>
<td>Contractors</td>
<td>39%</td>
<td>34%</td>
</tr>
</tbody>
</table>
In spite of all the furor around nation state hacking, cyber criminals top the list of concerns by a wide margin.

### Top External Threat Actor Selections

<table>
<thead>
<tr>
<th></th>
<th>U.S. Federal</th>
<th>Hacktivists</th>
<th>Nation States</th>
<th>Competitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Criminals</td>
<td>40%</td>
<td>29%</td>
<td>12%</td>
<td>2%</td>
</tr>
<tr>
<td>Competitors</td>
<td>17%</td>
<td>29%</td>
<td>40%</td>
<td>2%</td>
</tr>
<tr>
<td>Cyber-Terrorists</td>
<td>12%</td>
<td>16%</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>Nation States</td>
<td>17%</td>
<td>29%</td>
<td>40%</td>
<td>29%</td>
</tr>
</tbody>
</table>

### Global Federal

<table>
<thead>
<tr>
<th></th>
<th>Global Federal</th>
<th>Hacktivists</th>
<th>Nation States</th>
<th>Competitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Criminals</td>
<td>40%</td>
<td>16%</td>
<td>15%</td>
<td>9%</td>
</tr>
<tr>
<td>Competitors</td>
<td>9%</td>
<td>16%</td>
<td>15%</td>
<td>9%</td>
</tr>
<tr>
<td>Cyber-Terrorists</td>
<td>15%</td>
<td>15%</td>
<td>20%</td>
<td>20%</td>
</tr>
<tr>
<td>Nation States</td>
<td>20%</td>
<td>16%</td>
<td>40%</td>
<td>29%</td>
</tr>
</tbody>
</table>
While security breaches and attacks on public cloud providers was the top concern among the global average (58%), data residency and lack of visibility into the security practices of cloud service providers each elicited responses from 61% of U.S. federal respondents, putting them at the top of the list of public cloud concerns. For Global Federal, however, the top concern (58%) is the lack of a data privacy policy at public cloud providers.

Garrett Bekker
Principal Analyst, Information Security, 451 Research
**What Can CSPs and SaaS Providers Do to Increase Federal Cloud Adoption?**

<table>
<thead>
<tr>
<th>Category</th>
<th>U.S. Percentage</th>
<th>Global Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encryption in the Cloud with <strong>Agency Premise Key Control</strong></td>
<td>73%</td>
<td>65%</td>
</tr>
<tr>
<td>Data Encryption in the Cloud with <strong>CSP Key Control</strong></td>
<td>47%</td>
<td>38%</td>
</tr>
<tr>
<td>SLA Agreements and Liability Terms for Data Breaches</td>
<td>59%</td>
<td>44%</td>
</tr>
<tr>
<td>Detailed Physical and IT Security Implementation Information</td>
<td>55%</td>
<td>44%</td>
</tr>
</tbody>
</table>

“To guard against threats to sensitive data stored and processed in the public cloud, both U.S. Federal (73%) and Global Federal (65%) put encryption with the option for local key control (BYOK) at the top of the list - in fact encryption with BYOK was the top choice across virtually all categories surveyed.”

Garrett Bekker  
Principal Analyst, Information Security, 451 Research
BIG DATA - TOP FEDERAL DATA SECURITY CONCERNS AND STATS

TOP 5 CONCERNS

41% U.S.  
SECURITY OF REPORTS THAT MAY INCLUDE SENSITIVE DATA

52% GLOBAL

65% U.S.  
SENSITIVE DATA MAY RESIDE ANYWHERE

55% GLOBAL

38% U.S.  
PRIVACY VIOLATIONS - DATA ORIGINATES IN MANY COUNTRIES

24% GLOBAL

39% U.S.  
PRIVILEGED USER ACCESS TO PROTECTED DATA

35% GLOBAL

26% U.S.  
LACK OF EFFECTIVE ACCESS CONTROLS

34% GLOBAL

44% U.S.  
USING ENCRYPTION TO PROTECT DATA IN BIG DATA ENVIRONMENTS TODAY

29% GLOBAL

59% U.S.  
USING SENSITIVE INFORMATION IN BIG DATA ENVIRONMENTS

38% GLOBAL

59% U.S.  
VERY CONCERNED THAT THEY ARE USING SENSITIVE INFORMATION IN BIG DATA WITHOUT DATA SECURITY CONTROLS

30% GLOBAL
IOT ADOPTION IS HIGH FOR U.S. FEDERAL
USE OF SENSITIVE DATA A CONCERN

73% ADOPTING IOT
25% USING SENSITIVE DATA IN IOT
34% VERY CONCERNED ABOUT SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

34% - PROTECTING SENSITIVE DATA GENERATED BY IOT
33% - IDENTIFYING WHICH DATA IS SENSITIVE
25% - LACK OF SECURITY FRAMEWORKS & CONTROLS
23% - PRIVILEGED USER ACCESS TO DATA AND DEVICES
21% - IMPACT OF ATTACKS ON IOT DEVICES

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

65% SECURE ID AND AUTHENTICATION
63% ENCRYPTION OF DATA
42% - ANTI-MALWARE FOR DEVICES
59% - IOT NETWORK ISOLATION
45% - ANOMALY DETECTION/BEHAVIORAL ANALYSIS
"As is typical with any fast-emerging technology, security concerns abound, and security (60%) not surprisingly emerged as the top adoption barrier for U.S. Federal container deployments, as was the case with most other regions."

Garrett Bekker
451 Research
## Encryption Enables Digital Transformation

A Key Tool Required for Advanced Technology Adoption

<table>
<thead>
<tr>
<th>Technology</th>
<th>U.S.</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud</strong></td>
<td>73%</td>
<td>65%</td>
</tr>
<tr>
<td><strong>Big Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IOT</strong></td>
<td>63%</td>
<td></td>
</tr>
<tr>
<td><strong>Containers</strong></td>
<td>57%</td>
<td>55%</td>
</tr>
</tbody>
</table>

### Encryption Enabling Further Adoption of Cloud

- Data encryption in the cloud with agency premise key control
- U.S.: 73%
- Global: 65%

### Encryption Offsets Top Security Concerns

- Privileged user access
- Security of reports
- Sensitive data everywhere
- U.S.
  - Privileged user access: 39%
  - Security of reports: 41%
  - Sensitive data everywhere: 65%
- Global
  - Privileged user access: 35%
  - Security of reports: 52%
  - Sensitive data everywhere: 55%

### The Top Technologies Needed to Expand Usage

- Data encryption
- Secure digital identity (an encryption technology)
- U.S.
  - Data encryption: 63%
  - Secure digital identity: 65%
- Global
  - Data encryption: 51%
  - Secure digital identity: 47%

### Encryption the Top Control Needed to Enable Greater Adoption

- U.S. federal: 55%
- Global federal: 57%
<table>
<thead>
<tr>
<th><strong>BEST PRACTICE RECOMMENDATIONS</strong></th>
<th><strong>GARRETT BEKKER, 451 RESEARCH</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Re-prioritize your IT security tool set</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Discover and classify</strong></td>
<td>Get a better handle on the location of sensitive data, particularly for Cloud, Big Data, Containers and IoT</td>
</tr>
<tr>
<td><strong>Don’t just check off the compliance box</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Encryption and access control</strong></td>
<td>Encryption needs to move beyond laptops and desktops. <strong>Data center:</strong> File and application level encryption and access controls. <strong>Cloud:</strong> Encrypt and manage keys locally, BYOK enables safe SaaS, PaaS and IaaS. <strong>Big Data:</strong> Encryption and access control within the environment. <strong>Containers:</strong> Encrypt and control access to data both within containers and underlying data storage locations. <strong>IoT:</strong> 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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB/ File Encryption</td>
</tr>
<tr>
<td>Customer Records</td>
</tr>
</tbody>
</table>

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

**Data Protection Software**
2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

FEDERAL EDITION