THE GROWING STORM

Enterprises around the world are at the nexus of a growing need for data to power their businesses, regulatory requirements, and attacks aimed at this often sensitive information – and the U.K. is no exception.

In general, U.K. based enterprises seem to be doing a better job than their global counterparts at protecting this information.

But with data breaches and IT security spending increasing in parallel, and intense pressure to drive growth with cloud, big data and other advanced technologies …

There is clearly more to do.
OF U.K. RESPONDENTS FELT THEIR ORGANIZATIONS WERE VULNERABLE TO DATA THREATS

84%

WERE VERY OR EXTREMELY VULNERABLE

20%
VULNERABILITY TO DATA THREATS

GLOBAL

88% VULNERABLE
30% VERY/EXTREMELY VULNERABLE

REGIONAL

SO WHAT OR MORE VULNERABLE
90% UNITED STATES
84% UNITED KINGDOM
95% GERMANY
83% JAPAN
90% MEXICO
77% BRAZIL
91% AUSTRALIA

VERY OR EXTREMELY VULNERABLE
29% UNITED STATES
20% UNITED KINGDOM
45% GERMANY
23% JAPAN
31% MEXICO
19% BRAZIL
49% AUSTRALIA
THE STORM INTENSIFIES ...

43% have experienced a data breach
- 22% in the last year (up from 19% last year)
- 5% more than once (global average 12%)

63% expect their spending on data security to increase
- Up from 52% in 2016
- Global average 73%
THE GOOD NEWS ABOUT U.K. DATA SECURITY

SAFE OPERATION

50% – U.K.
33% – GLOBAL*

Highest “safe operation” rate we measured - 50% never had a data breach or compliance failure for data security violations

INCREASING SPENDING TO PROTECT DATA

U.K.

Global

<table>
<thead>
<tr>
<th>Year</th>
<th>U.K.</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>51%</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>54%</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>63%</td>
<td>73%</td>
</tr>
</tbody>
</table>

SAFE OPERATION RANKINGS

- U.K.
- Global*
## IT Security Spending Priorities (Rates of Top 3 Selection)

<table>
<thead>
<tr>
<th>Priority</th>
<th>2017</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Requirements</td>
<td>52%</td>
<td>47%</td>
</tr>
<tr>
<td>Reputation and Brand Protection</td>
<td>41%</td>
<td>50%</td>
</tr>
<tr>
<td>Data Breach Penalties</td>
<td>41%</td>
<td>38%</td>
</tr>
<tr>
<td>IT Security Best Practices</td>
<td>37%</td>
<td>41%</td>
</tr>
<tr>
<td>Executive Directive</td>
<td>35%</td>
<td>26%</td>
</tr>
<tr>
<td>Partner and Prospect Requirements</td>
<td>20%</td>
<td>34%</td>
</tr>
<tr>
<td>Data Breaches at Partners or Competitors</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>Previous Data Breach</td>
<td>15%</td>
<td>22%</td>
</tr>
<tr>
<td>Competitive/Strategic Concerns</td>
<td>15%</td>
<td>22%</td>
</tr>
</tbody>
</table>

*“Compliance is a minimum table stake for regulated enterprises ... but being compliant does not mean you won’t be breached.”*  
Garrett Bekker, Principal Analyst Information Security, 451 Research
“.. 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></th>
<th>U.K.</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Management</td>
<td>39%</td>
<td>43%</td>
</tr>
<tr>
<td>Ordinary Employees</td>
<td>36%</td>
<td>33%</td>
</tr>
<tr>
<td>Contractors</td>
<td>55%</td>
<td>58%</td>
</tr>
</tbody>
</table>

43% U.K.
36% GLOBAL
## Top External Threat Actor Selections

<table>
<thead>
<tr>
<th>Region</th>
<th>Cyber Criminals</th>
<th>Hacktivists</th>
<th>Cyber-Terrorists</th>
<th>Competitors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>U.K.</strong></td>
<td>44%</td>
<td>17%</td>
<td>13%</td>
<td>14%</td>
</tr>
<tr>
<td><strong>Global</strong></td>
<td>44%</td>
<td>17%</td>
<td>15%</td>
<td>12%</td>
</tr>
</tbody>
</table>
59% of U.K. IT security professionals surveyed are concerned that they are deploying new technologies in advance of having appropriate levels of data security in place.

91% 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>Technology</th>
<th>SAAS</th>
<th>IAAS</th>
<th>PAAS</th>
<th>MOBILE</th>
<th>BIG DATA</th>
<th>IOT</th>
<th>CONTAINERS</th>
<th>BLOCKCHAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>51%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Old Habits Die Hard - Investing Heavily in Network Security As It Becomes Less Relevant**

"... 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>Security Category</th>
<th>Increase</th>
<th>Spending Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td></td>
<td>48%</td>
</tr>
<tr>
<td>End Point and Mobile</td>
<td></td>
<td>41%</td>
</tr>
<tr>
<td>Analysis and Correlation Data in Motion</td>
<td></td>
<td>44%</td>
</tr>
<tr>
<td>Data at Rest</td>
<td></td>
<td>38%</td>
</tr>
</tbody>
</table>

### Rates of Effectiveness for Protecting Data

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Increase</th>
<th>Effectiveness Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td></td>
<td>74%</td>
</tr>
<tr>
<td>End Point and Mobile</td>
<td></td>
<td>58%</td>
</tr>
<tr>
<td>Analysis and Correlation Data in Motion</td>
<td></td>
<td>59%</td>
</tr>
<tr>
<td>Data at Rest</td>
<td></td>
<td>61%</td>
</tr>
</tbody>
</table>

**Good News - Data-at-rest security a priority**
With national regulations like GDPR coming worldwide, data privacy and sovereignty are making waves everywhere.

75% - U.K.
72% - Global

Impacted by data privacy and data sovereignty.

### Addressing Requirements by:

#### U.K.
- **57%** Encrypting Data
- **33%** Tokenizing Data
- **29%** Migrating Data
- **23%** Local Hosting & Cloud

#### Global
- **64%** Encrypting Data
- **40%** Tokenizing Data
- **36%** Migrating Data
- **26%** Local Hosting & Cloud

### Data Privacy/Sovereignty Beyond GDPR

- **U.S.A.**
  - AIPP Data Protection and Privacy Rules go live September 2017
  - 47 state laws plus federal regulations

- **Japan**
  - LFPDPPP Privacy Law with fines up to £1.5M

- **Mexico**
  - New privacy legislation pending for approval

- **Brazil**
**COMPLEXITY AND POTENTIAL PERFORMANCE IMPACTS**

**TOP BARRIERS TO DATA SECURITY DEPLOYMENT**

<table>
<thead>
<tr>
<th>Perception of Complexity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>44%</td>
</tr>
<tr>
<td>Potential Performance Impacts</td>
<td>35%</td>
</tr>
<tr>
<td>Lack of Staff to Manage</td>
<td>29%</td>
</tr>
<tr>
<td>Lack of Organizational Buy In</td>
<td>28%</td>
</tr>
<tr>
<td>Lack of Budget</td>
<td>22%</td>
</tr>
<tr>
<td>Lack of Perceived Need</td>
<td>17%</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
ENTERPRISE CONCERNS WITH CLOUD/SAAS ENVIRONMENTS

THREATS - RATES OF VERY OR EXTREMELY CONCERNED

- **SHARED INFRASTRUCTURE VULNERABILITIES**
  - 44% - U.K.
  - 57% - GLOBAL

- **LACK OF DATA PRIVACY POLICY / SLA**
  - 43% - U.K.
  - 52% - GLOBAL

- **SECURITY BREACHES/ATTACKS AT CSP**
  - 40% - U.K.
  - 59% - GLOBAL

- **LACK OF DATA LOCATION CONTROL**
  - 39% - U.K.
  - 55% - GLOBAL

- **LACK OF VISIBILITY INTO SECURITY PRACTICES**
  - 38% - U.K.
  - 50% - GLOBAL

- **CLOUD PRIVILEGED USER ABUSE/THREATS**
  - 37% - U.K.
  - 53% - GLOBAL

- **CUSTODIANSHIP OF ENCRYPTION KEYS**
  - 32% - U.K.
  - 51% - GLOBAL

- **MEETING COMPLIANCE REQUIREMENTS**
  - 30% - U.K.
  - 47% - GLOBAL

CONECRNS WITH SENSITIVE DATA IN CLOUD ENVIRONMENTS

ARE HIGH, WITH NEARLY HALF OF RESPONDENTS LISTING THEM AS ENVIRONMENTS WHERE THEY ARE CONCERNED ABOUT USING SENSITIVE DATA

- 48% - IAAS
- 47% - PAAS
- 44% - SAAS
WHAT CAN CSPS AND SAAS PROVIDERS DO TO INCREASE ENTERPRISE CLOUD ADOPTION IN THE U.K.?

- Data encryption in the cloud with enterprise key control: 62% UK, 61% Global
- Data encryption in the cloud with CSP premises key control: 39% UK, 51% Global
- Expose detailed security monitoring data to my enterprise: 44% UK, 41% Global
- SLA agreements and liability terms for data breaches: 46% UK, 49% Global

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

U.S. 66%  MEXICO 64%  U.K. 62%  GERMANY 50%  JAPAN 49%
### Big Data - Top Data Security Concerns and Stats

#### Top 5 Concerns

<table>
<thead>
<tr>
<th>Concern</th>
<th>UK (%)</th>
<th>Global (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Sensitive data may reside anywhere</td>
<td>44</td>
<td>45</td>
</tr>
<tr>
<td>2. Security of reports that may include sensitive data</td>
<td>41</td>
<td>44</td>
</tr>
<tr>
<td>3. Lack of effective access controls</td>
<td>29</td>
<td>31</td>
</tr>
<tr>
<td>4. Privileged user access to protected data</td>
<td>26</td>
<td>36</td>
</tr>
<tr>
<td>5. Privacy violations, data originating in multiple countries</td>
<td>23</td>
<td>35</td>
</tr>
</tbody>
</table>

#### Additional Stats

<table>
<thead>
<tr>
<th>Concern</th>
<th>UK (%)</th>
<th>Global (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Using encryption to protect data in big data environments today</td>
<td>34</td>
<td>36</td>
</tr>
<tr>
<td>2. Using sensitive information in big data environments</td>
<td>44</td>
<td>47</td>
</tr>
<tr>
<td>3. Very concerned about sensitive information in big data without data security controls</td>
<td>41</td>
<td>44</td>
</tr>
</tbody>
</table>
ENTERPRISES IN THE U.K. HAVE HIGH IOT ADOPTION
USE OF SENSITIVE DATA A CONCERN

75% ADOPTING IOT TECHNOLOGIES
19% USING SENSITIVE DATA IN IOT
24% VERY CONCERNED ABOUT SENSITIVE DATA IN IOT

TOP 5 DATA SECURITY CONCERNS FOR IOT

- 29% - Protecting sensitive data generated by IOT
- 22% - Lack of industry standards for securing IOT
- 18% - Privileged user access to IOT devices
- 18% - Loss or theft of IOT devices
- 17% - Operational impact of IOT attacks

TOP 5 CONTROLS NEEDED TO INCREASE IOT ADOPTION

- 49% - Encryption of data
- 50% - Secure ID and authentication
- 46% - Anti-malware for devices
- 42% - IOT network isolation
- 31% - Behavioral analytics / anomaly detection
TOP SECURITY CONTROLS NEEDED TO INCREASE CONTAINER ADOPTION AND USE IN THE U.K.

75% PLAN TO DEPLOY CONTAINER TECHNOLOGY BY END OF 2017

36% ALREADY IN PRODUCTION

40% BUDGET THE TOP BARRIER TO FURTHER CONTAINER DEPLOYMENT

U.K.

- 44% ADVANCED CONTINUED ALARMING
- 60% ENCRYPTION
- 33% VULNERABILITY SCANNING
- 39% MONITORING
- 27% DIGITAL SIGNATURE IMAGE VALIDATION

GLOBAL

- 45% ADVANCED CONTINUED ALARMING
- 53% ENCRYPTION
- 42% VULNERABILITY SCANNING
- 22% ROLE BASED ACCESS CONTROLS
- 31% DIGITAL SIGNATURE IMAGE VALIDATION
<table>
<thead>
<tr>
<th>Category</th>
<th>U.K.</th>
<th>Global</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>62%</td>
<td>61%</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables further adoption of Cloud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Big Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption offsets top security concerns</td>
<td>44%</td>
<td>45%</td>
<td></td>
</tr>
<tr>
<td>Sensitive data everywhere</td>
<td>41%</td>
<td>44%</td>
<td></td>
</tr>
<tr>
<td>Security of reports</td>
<td>29%</td>
<td>31%</td>
<td></td>
</tr>
<tr>
<td>Lack of access controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The top technology needed to expand usage</td>
<td>49%</td>
<td>56%</td>
<td></td>
</tr>
<tr>
<td>Data encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure digital identity (an encryption technology)</td>
<td>50%</td>
<td>55%</td>
<td></td>
</tr>
<tr>
<td>Containers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption the top control needed to enable greater adoption</td>
<td>60%</td>
<td>53%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BEST PRACTICE RECOMMENDATIONS</strong></td>
<td><strong>GARRETT BEKKER, 451 RESEARCH</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------</td>
<td></td>
<td></td>
</tr>
<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>
<td></td>
<td></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>
<td></td>
<td></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>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **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 |
ABOUT THALES E-SECURITY

- **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.

Use Cases

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

Use Cases Categories:

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

Data Protection Platforms:

- Hard Ware
- Software

Use Cases:

- Cloud Migration
- Cloud Security
- Payments
- Transaction Security
- Payment related apps
- Internet of Things
- Script Development
- Code Signing
- Tokenization
- Encryption Gateway
- Key Management
- Security Intelligence