PART 1. EXECUTIVE SUMMARY ................................................. 3

PART 2. KEY FINDINGS ...................................................... 8

  Strategy and adoption of encryption ............................................. 9
  Trends in encryption adoption .................................................. 11
  Threats, main drivers and priorities .......................................... 11
  Deployment choices ............................................................. 13
  Encryption features considered most important ...................... 14
  Attitudes about key management .......................................... 15
  Importance of hardware security modules (HSMs) .................. 18
  Cloud encryption .............................................................. 22

APPENDIX 1. METHODS & LIMITATIONS ................................. 24

APPENDIX 2. CONSOLIDATED FINDINGS ................................. 29
EXECUTIVE SUMMARY
We surveyed 5,856 individuals across multiple industry sectors in 14 countries/regions: Australia, Brazil, France, Germany, India, Japan, Mexico, the Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), the Russian Federation, South Korea, the United Kingdom, the United States and, two new regions in Asia for the first time, Southeast Asia (Indonesia, Malaysia, Philippines, Thailand and Vietnam) and Hong Kong and Taiwan.

The purpose of this research is to examine how the use of encryption has evolved over the past 14 years and the impact of this technology on the security posture of organizations.

The first encryption trends study was conducted in 2005 for a US sample of respondents. Since then we have expanded the scope of the research to include respondents in all regions of the world.

As shown in Figure 1, since 2015 the deployment of an overall encryption strategy has steadily increased. This year, 45 percent of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise and 42 percent say they have a limited encryption plan or strategy that is applied to certain applications and data types.

The following pages contain the 2019 findings.

---

1 This year’s data collection was completed in December 2018. Throughout the report we present trend data based on the fiscal year (FY) the survey commenced rather than the year the report is finalized. Hence, our most current findings are presented as FY18. The same dating convention is used in prior years.

2 Country-level results are abbreviated as follows: Australia (AU), Brazil (BZ), France (FR), Germany (DE), Hong Kong and Taiwan (HKT), India (IN), Japan (JP), Korea (KO), Mexico (MX), Middle East (ME), Russia (RF), Southeast Asia (SA), United Kingdom (UK), and United States (US).

3 The trend analysis shown in this study was performed on a combined country samples spanning 14 years (since 2005).
STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase.
Since first conducting this study 14 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise. In turn, there has been a steady decline in organizations not having an encryption plan or strategy. The results have essentially reversed over the years of the study.

Certain countries have more mature encryption strategies.
The prevalence of an enterprise encryption strategy varies among the countries represented in this research. The highest prevalence of an enterprise encryption strategy is reported in Germany followed by the United States, Australia and the United Kingdom. Respondents in the Russian Federation and Brazil report the lowest adoption of an enterprise encryption strategy. The global average of adoption is 45 percent.

The IT operations function is the most influential in framing the organization’s encryption strategy over the past 14 years.
However, in some countries lines of business are more influential. These are the United States and Brazil. IT security and IT operations have a similar level of influence in Australia, India, Mexico and the Russian Federation.

TRENDS IN ADOPTION OF ENCRYPTION

The use of encryption increases in all industries.
Results suggest a steady increase in all industry sectors. The most significant increases in extensive encryption usage occur in manufacturing, hospitality and consumer products.

The extensive use of encryption technologies increases.
Since we began tracking the enterprise-wide use of encryption in 2005, there has been a steady increase in the encryption solutions extensively used by organizations.

“Since first conducting this study 14 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise.”

THREATS, MAIN DRIVERS AND PRIORITIES

Employee mistakes continue to be the most significant threats to sensitive data.
The most significant threats to the exposure of sensitive or confidential data are employee mistakes. In contrast, the least significant threats to the exposure of sensitive or confidential data include government eavesdropping and lawful data requests. Concerns over inadvertent exposure (employee mistakes and system malfunction) significantly outweigh concerns over actual attacks by temporary or contract workers and malicious insiders. It is interesting to note that the employee mistake threat exceeds the combined threat by both hackers and insiders.

The main driver for encryption is protection of sensitive information.
Organizations are using encryption to protect the enterprise’s intellectual property and the personal information of customers (both 54 percent of respondents).

A barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization.
Sixty-nine percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. In addition, 42 percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-two percent cite classifying which data to encrypt as difficult.
DEPLOYMENT CHOICES

No single encryption technology dominates in organizations. Organizations have very diverse needs. Internet communications, databases and laptop hard drives are the most likely to be encrypted and correspond to mature use cases. For the second year, the study tracked the deployment of encryption of IoT devices and platforms. As shown, 52 percent of respondents say encryption of IoT devices and 50 percent of respondents say encryption on IoT platforms have been at least partially deployed.

ENCcryPTION FEATURES CONSIDERED MOST IMPORTANT

Certain encryption features are considered more critical than others. According to consolidated findings, enforcement of policy, system performance and latency and support for both cloud and on-premise deployment are the three most important features. Support for both cloud and on-premise deployment has risen in importance as organizations have increasingly embraced cloud computing and look for consistency across computing styles. In fact, the top findings in this area all correspond to features considered important for cloud solutions. System performance and latency and system scalability remain at high levels but declined in importance in this year’s survey.

Which data types are most often encrypted?
Payment-related data and financial records are most likely to be encrypted as a result of high-profile data breaches in financial services. Employee/HR data and intellectual property remain high on the list of data being encrypted. The least likely data type to be encrypted is health-related information and non-financial information, which is a surprising result given the sensitivity of health information and the recent high-profile healthcare data breaches. Financial records had the largest increase on this list over last year.

ATTITUDES ABOUT KEY MANAGEMENT

How painful is key management?
Sixty-one percent of respondents rate key management as very painful, which suggests respondents view managing keys as a very challenging activity. The highest percentage pain threshold of 70 percent occurs in the UK. At 38 percent, the lowest pain level occurs in France.

Companies continue to use a variety of key management systems.
Companies continue to use a variety of key management systems. The most commonly deployed systems include: (1) formal key management policy (KMP), (2) formal key management infrastructure (KMI) and (3) manual process.

IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)

Germany, United States and India organizations are more likely to deploy HSMs. Germany, United States and India are more likely to deploy HSMs than other countries. The overall average deployment rate for HSMs is 47 percent.

How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months.
Almost half (48 percent of respondents) own and operate HSMs on-premise for cloud-based applications, and 37 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. In the next 12 months, both figures will increase, by 5 and 7 percent respectively. Interestingly, the use of HSMs with Cloud Access Security Brokers is expected to double in the next 12 months.

The overall average importance rating for HSMs, as part of an encryption and key management strategy in the current year is 60 percent.
The pattern of responses suggests Japan, Germany and Australia are most likely to assign importance to HSMs as part of their organization’s encryption or key management activities.
What best describes an organization’s use of HSMs?
Sixty percent of respondents say their organization has a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within their organization (i.e., private cloud model). Forty percent say each individual application owner/team is responsible for their own cryptographic services (including HSMs), indicative of the more traditional siloed application-specific data center deployment approach.

What are the primary purposes or uses for HSMs?
The top uses are application-level encryption, TLS/SSL, and database encryption. There is projected to be a significant (10%) increase in the use of database encryption 12 months from now. It is also significant to note that HSM use for application-level encryption will soon be deployed in 50 percent of the organizations represented in this study.

CLOUD ENCRYPTION

60 percent of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted or made unreadable via some other mechanism such as tokenization or data masking.

Another 22 percent of respondents expect to do so in the next one to two years. These findings indicate the benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.

How do organizations protect data at rest in the cloud?
Forty-four percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 35 percent of respondents perform encryption in the cloud, with cloud provider generated/managed keys. Twenty-one percent of respondents are using some form of Bring Your Own Key (BYOK) approach.

What are the top three encryption features specifically for the cloud?
The top three features are support for the KMIP standard for key management (73 percent of respondents), SIEM integration, visualization and analysis of logs (60 percent of respondents) and granular access controls (58 percent of respondents).

“Payment-related data and financial records are most likely to be encrypted as a result of high-profile data breaches in financial services. Employee/HR data and intellectual property remain high on the list of data being encrypted.”
02 KEY FINDINGS
IN THIS SECTION, WE PROVIDE A DEEPER ANALYSIS OF THE KEY FINDINGS. THE COMPLETE AUDITED FINDINGS ARE PRESENTED IN THE APPENDIX OF THE REPORT.

We have organized the report according to the following themes:

- Strategy and adoption of encryption
- Trends in adoption of encryption
- Threats, main drivers and priorities
- Deployment choices
- Encryption features considered most important
- Attitudes about key management
- Importance of hardware security modules (HSMs) 4

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase. Since first conducting this study 14 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise. In turn, there has been a steady decline in organizations not having an encryption plan or strategy. The results have essentially reversed over the years of the study. Figure 2 shows these changes over time.

![Figure 2. Trends in encryption strategy](image)

*Company has an encryption strategy applied consistently across the entire enterprise
*Company does not have an encryption strategy

---

4 HSMs are devices specifically built to create a tamper-resistant environment in which to perform cryptographic processes (e.g., encryption or digital signing) and to manage the keys associated with those processes. These devices are used to protect critical data processing activities and can be used to strongly enforce security policies and access controls. HSMs are typically validated to formal security standards such as FIPS 140-2.
Certain countries have more mature encryption strategies. According to Figure 3, the prevalence of an enterprise encryption strategy varies among the countries represented in this research. The highest prevalence of an enterprise encryption strategy is reported in Germany followed by the United States, Australia and the United Kingdom. Respondents in the Russian Federation and Brazil report the lowest adoption of an enterprise encryption strategy. The global average of adoption is 45 percent.

However, in some countries lines of business are more influential. These are the United States and Brazil. IT security and IT operations have a similar level of influence in Australia, India, Mexico and the Russian Federation.

A possible reason why the lines of business are more influential than IT security is because of the growing adoption of Internet of Things (IoT) devices in the workplace, proliferation of employee-owned devices or BYOD and the general consumerization of IT. A consequence is that lines of business are required to be more accountable for the security of these technologies.

Figure 4 shows that the IT operations function is the most influential in framing the organization’s encryption strategy over the past 14 years.
**TRENDS IN ADOPTION OF ENCRYPTION**

The use of encryption increases in all industries. Figure 5 shows the current year and the seven-year average in the use of encryption solutions for 10 industry sectors. Results suggest a steady increase in all industry sectors. The most significant increases in extensive encryption usage occur in manufacturing, hospitality and consumer products.

**THREATS, MAIN DRIVERS AND PRIORITIES**

Employee mistakes continue to be the most significant threats to sensitive data.

Figure 6 shows that the most significant threats to the exposure of sensitive or confidential data are employee mistakes.

In contrast, the least significant threats to the exposure of sensitive or confidential data include government eavesdropping and lawful data requests. Concerns over inadvertent exposure (employee mistakes and system malfunction) significantly outweigh concerns over actual attacks by temporary or contract workers and malicious insiders. It is interesting to note that the employee mistake threat exceeds the combined threat by both hackers and insiders.
The main driver for encryption is protection of information against identified threats.

Eight drivers for deploying encryption are presented in Figure 7. Organizations use an average of 8 different products to perform encryption.

Organizations are using encryption to protect the enterprise’s intellectual property and the personal information of customers (both 54 percent of respondents).

This marks the second year that compliance with regulations has not been the top driver for encryption indicating that encryption is less of a “checkbox” exercise and is now used to safeguard targeted critical information.

To protect enterprise intellectual property
To protect customer personal information
To protect information against specific, identified threats
To comply with external privacy or data security regulations and requirement
To reduce the scope of compliance audits
To limit liability from breaches or inadvertent disclosure
To comply with internal policies
To avoid public disclosure after a data breach occurs

A barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization.

Figure 8 provides a list of six aspects that present challenges to an organization’s effective execution of its data encryption strategy in descending order of importance. Sixty-nine percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. In addition, 42 percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-two percent cite classifying which data to encrypt as difficult.

Figure 7. The main drivers for using encryption technology solutions
Country samples are consolidated. Three responses permitted

<table>
<thead>
<tr>
<th>Driver</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>To protect enterprise intellectual property</td>
<td>54%</td>
</tr>
<tr>
<td>To protect customer personal information</td>
<td>54%</td>
</tr>
<tr>
<td>To protect information against specific, identified threats</td>
<td>51%</td>
</tr>
<tr>
<td>To comply with external privacy or data security regulations and requirement</td>
<td>46%</td>
</tr>
<tr>
<td>To reduce the scope of compliance audits</td>
<td>31%</td>
</tr>
<tr>
<td>To limit liability from breaches or inadvertent disclosure</td>
<td>29%</td>
</tr>
<tr>
<td>To comply with internal policies</td>
<td>21%</td>
</tr>
<tr>
<td>To avoid public disclosure after a data breach occurs</td>
<td>14%</td>
</tr>
</tbody>
</table>

Figure 8. Biggest challenges in planning and executing a data encryption strategy
Country samples are consolidated. More than one choice permitted

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovering where sensitive data resides in the organization</td>
<td>69%</td>
</tr>
<tr>
<td>Initially deploying the encryption technology</td>
<td>42%</td>
</tr>
<tr>
<td>Classifying which data to encrypt</td>
<td>32%</td>
</tr>
<tr>
<td>Ongoing management of encryption and keys</td>
<td>28%</td>
</tr>
<tr>
<td>Determining which encryption technologies are most effective</td>
<td>16%</td>
</tr>
<tr>
<td>Training users to use encryption appropriately</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>
DEPLOYMENT CHOICES

No single encryption technology dominates in organizations.

We asked respondents to indicate if specific encryption technologies are widely or only partially deployed within their organizations. “Extensive deployment” means that the encryption technology is deployed enterprise-wide. “Partial deployment” means the encryption technology is confined or limited to a specific purpose (i.e., point solution).

As shown in Figure 9, no single technology dominates because organizations have very diverse needs. Internet communications, databases and laptop hard drives are the most likely to be deployed and correspond to mature use cases.

For the second year, the study tracked the deployment of encryption of IoT devices and platforms. As shown, 52 percent of respondents say encryption of IoT devices and 50 percent of respondents say encryption on IoT platforms have been at least partially deployed.
ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

Certain encryption features are considered more critical than others. Figure 10 lists 12 encryption technology features. Each percentage defines the very important response (on a four-point scale). Respondents were asked to rate encryption technology features considered most important to their organization’s security posture.

According to consolidated findings, enforcement of policy, system performance and latency and support for both cloud and on-premise deployment are the three most important features. The performance finding is not surprising given that encryption in networking is a prominent use case, as well as the often-emphasized requirement for transparency of encryption solutions.

Support for both cloud and on-premise deployment has risen in importance as organizations have increasingly embraced cloud computing and look for consistency across computing styles.

In fact, the top findings in this area all correspond to features considered important for cloud solutions. System performance and latency and system scalability remain at high levels but declined in importance in this year’s survey.
Which data types are most often encrypted?  
Figure 11 provides a list of seven data types that are routinely encrypted by respondents’ organizations. As can be seen, payment-related data and financial records are most likely to be encrypted as a result of high-profile data breaches in financial services.

The least likely data type to be encrypted is health-related information and non-financial information, which is a surprising result given the sensitivity of health information and the recent high-profile healthcare data breaches. Financial records had the largest increase on this list over last year.

ATTITUDES ABOUT KEY MANAGEMENT

How painful is key management?  
Using a 10-point scale, respondents were asked to rate the overall “pain” associated with managing keys within their organization, where 1 = minimal impact to 10 = severe impact. Figure 12 clearly shows that 61 percent of respondents in this year’s survey chose ratings at or above 7; thus, suggesting a fairly high pain threshold.
Figure 13 shows the 7+ ratings on a 10-point scale for each country. As can be seen, the average percentage in all country samples is 61 percent, which suggests respondents view managing keys as a very challenging activity. The highest percentage pain threshold of 70 percent occurs in the UK. At 38 percent, the lowest pain level occurs in France.

**Why is key management painful?**

Figure 14 shows the reasons why the management of keys is so difficult. The top three reasons are: (1) no clear ownership of the key management function, (2) lack of skilled personnel and (3) isolated or fragmented key management systems.
Which keys are most difficult to manage?
For the second year in a row, keys for external cloud or hosted services rank as the most difficult keys to manage. As shown in Figure 15, they are followed by SSH keys, signing keys, and keys for TLS/SSL. The least difficult include: (1) encryption keys for archived data, (2) encryption keys for backups and storage, and (3) embedded device keys.

As shown in Figure 16, respondents’ companies continue to use a variety of key management systems. The most commonly deployed systems include: (1) formal key management policy (KMP) and (3) formal key management infrastructure (KMI) and manual process.

Figure 15. Types of keys most difficult to manage
Country samples are consolidated. Very painful and painful responses combined

- Keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys: 60%
- SSH keys: 57%
- Signing keys (e.g., code signing, digital signatures): 51%
- Keys associated with TLS/SSL: 42%
- End user encryption keys (e.g., email, full disk encryption): 41%
- Payments-related keys (e.g., ATM, POS, etc.): 35%
- Encryption keys for archived data: 34%
- Encryption keys for backups and storage: 30%
- Keys to embed into devices (e.g., at the time of manufacture in device production environments, or for IoT devices you use): 27%

Figure 16. What key management systems does your organization presently use?
Country samples are consolidated. More than one choice permitted

- Formal key management policy (KMP): 56%
- Formal key management infrastructure (KMI): 44%
- Manual process (e.g., spreadsheet, paper-based): 41%
- Central key management system/server: 34%
- Removable media (e.g., thumb drive, CDROM): 31%
- Software-based key stores and wallets: 30%
- Hardware security modules: 24%
- Smart cards: 24%
IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)

Germany, United States and India organizations are more likely to deploy HSMs.

Figure 17 summarizes the percentage of respondents that deploy HSMs. Germany, United States and India are more likely to deploy HSMs than other countries. The overall average deployment rate for HSMs is 47 percent.

Deployment of HSMs increases steadily.

Figure 18 shows a seven-year trend for HSMs. As can be seen, the rate of global HSM deployment has steadily increased.

---

5 HSMs are devices specifically built to create a tamper-resistant environment in which to perform cryptographic processes (e.g. encryption or digital signing) and to manage the keys associated with those processes. These devices are used to protect critical data processing activities and can be used to strongly enforce security policies and access controls. HSMs are typically validated to formal security standards such as FIPS 140-2.
How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months.

As shown in Figure 19, almost half (48 percent of respondents) own and operate HSMs on-premise for cloud-based applications, and 37 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. In the next 12 months, both figures will increase, by 5 and 7 percent respectively. Interestingly, the use of HSMs with Cloud Access Security Brokers is expected to double in the next 12 months.

Figure 20 summarizes the percentage of respondents in 14 countries that rate HSMs as either very important or important to their organization’s encryption or key management program or activities. The overall average importance rating in the current year is 60 percent. The pattern of responses suggests Japan, Germany and Australia are most likely to assign importance to HSMs as part of their organization’s encryption or key management activities.
Figure 21 shows a seven-year trend in the importance of HSMs for encryption or key management, which has steadily increased over time.

**What best describes an organization’s use of HSMs?**

As shown in Figure 22, 60 percent of respondents say their organization has a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within their organization (i.e., private cloud model). Forty percent say each individual application owner/team is responsible for their own cryptographic services (including HSMs), indicative of the more traditional siloed application-specific data center deployment approach.

---

**Figure 21. Perceived importance of HSMs as part of encryption or key management over seven years**

Country samples are consolidated

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY12</td>
<td>33%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY13</td>
<td>39%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY14</td>
<td>48%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY15</td>
<td>49%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY16</td>
<td>55%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY17</td>
<td>57%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY18</td>
<td>60%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Figure 22. Which statement best describes how your organization uses HSMs?**

- **60 percent** of respondents say their organization has a **centralized team that provides cryptography as a service** (including HSMs) to multiple applications/teams within their organization (i.e., private cloud model).

- **40 percent** say each individual application owner/team is responsible for their own cryptographic services (including HSMs) (i.e., traditional siloed, application-specific data center deployment).
What are the primary purposes or uses for HSMs? Figure 23 summarizes the primary purpose or use cases for deploying HSMs. As can be seen, the top choices are application-level encryption, TLS/SSL, and database encryption. This chart shows a significant increase in the use of database encryption projected for 12 months from now.

It is significant to note that HSM use for application-level encryption will soon be deployed in 50 percent of the organizations represented in this study.
CLOUD ENCRYPTION

According to Figure 24, 60 percent of respondents say their organizations transfer sensitive or confidential data to the cloud whether or not it is encrypted or made unreadable via some other mechanism such as tokenization or data masking. Another 22 percent of respondents expect to do so in the next one to two years.

These findings indicate the benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.

According to Figure 25, with respect to the transfer of sensitive or confidential data to the cloud, the United States, Germany, Korea and India are more frequently transferring sensitive data to the cloud.
How do organizations protect data at rest in the cloud? As shown in Figure 26, 44 percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 35 percent of respondents perform encryption in the cloud, with cloud provider generated/managed keys. Twenty-one percent of respondents are using some form of Bring Your Own Key (BYOK) approach.

What are the top three encryption features specifically for the cloud? The top three features are support for the KMIP standard for key management (73 percent of respondents), SIEM integration, visualization and analysis of logs (60 percent of respondents) and granular access controls (58 percent of respondents).
APPENDIX 1
METHODS & LIMITATIONS
Table 1 reports the sample response for 14 separate country samples. Data collection was completed in December 2018. Our consolidated sampling frame of practitioners in all countries consisted of 150,066 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 6,502 returns of which 646 were rejected for reliability issues. Our final consolidated 2018 sample was 5,856, thus resulting in an overall 3.9% response rate.

The first encryption trends study was conducted in the United States in 2005. Since then we have expanded the scope of the research to include 14 separate country samples. Trend analysis was performed on combined country samples. As noted previously, we added Southeast Asia and also Hong Kong & Taiwan to this year’s study.

Table 1. Survey response in 14 countries

<table>
<thead>
<tr>
<th>Legend</th>
<th>Survey response</th>
<th>Sampling frame</th>
<th>Final sample</th>
<th>Response rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU</td>
<td>Australia</td>
<td>7,077</td>
<td>327</td>
<td>4.6%</td>
</tr>
<tr>
<td>BZ</td>
<td>Brazil</td>
<td>12,550</td>
<td>517</td>
<td>4.1%</td>
</tr>
<tr>
<td>DE</td>
<td>Germany</td>
<td>11,938</td>
<td>531</td>
<td>4.4%</td>
</tr>
<tr>
<td>FR</td>
<td>France</td>
<td>10,356</td>
<td>332</td>
<td>3.2%</td>
</tr>
<tr>
<td>HKT</td>
<td>Hong Kong &amp; Taiwan</td>
<td>8,360</td>
<td>317</td>
<td>3.8%</td>
</tr>
<tr>
<td>IN</td>
<td>India</td>
<td>15,053</td>
<td>587</td>
<td>3.9%</td>
</tr>
<tr>
<td>JP</td>
<td>Japan</td>
<td>11,030</td>
<td>502</td>
<td>4.6%</td>
</tr>
<tr>
<td>KO</td>
<td>Korea</td>
<td>10,349</td>
<td>325</td>
<td>3.1%</td>
</tr>
<tr>
<td>ME</td>
<td>Middle East</td>
<td>9,842</td>
<td>340</td>
<td>3.5%</td>
</tr>
<tr>
<td>MX</td>
<td>Mexico</td>
<td>10,961</td>
<td>499</td>
<td>4.6%</td>
</tr>
<tr>
<td>RF</td>
<td>Russian Federation</td>
<td>5,959</td>
<td>226</td>
<td>3.8%</td>
</tr>
<tr>
<td>SA</td>
<td>Southeast Asia</td>
<td>7,693</td>
<td>268</td>
<td>3.5%</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
<td>10,984</td>
<td>402</td>
<td>3.7%</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
<td>17,914</td>
<td>683</td>
<td>3.8%</td>
</tr>
<tr>
<td></td>
<td>Consolidated</td>
<td>150,066</td>
<td>5,856</td>
<td>3.9%</td>
</tr>
</tbody>
</table>

The purpose of this research is to examine how the use of encryption has evolved over the past 14 years and the impact of this technology on the security posture of organizations.
Table 2 summarizes our survey samples for 14 countries over the history of the study.

Figure 28 reports the respondent’s organizational level within participating organizations. By design, 56 percent of respondents are at or above the supervisory levels.

Respondents have on average 10 years of security experience with approximately 7 years of experience in their current position.

Table 2. Sample history over 13 years

<table>
<thead>
<tr>
<th>Legend</th>
<th>FY18</th>
<th>FY17</th>
<th>FY16</th>
<th>FY15</th>
<th>FY14</th>
<th>FY13</th>
<th>FY12</th>
<th>FY11</th>
<th>FY10</th>
<th>FY09</th>
<th>FY08</th>
<th>FY07</th>
<th>FY06</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU</td>
<td>327</td>
<td>315</td>
<td>331</td>
<td>334</td>
<td>359</td>
<td>414</td>
<td>938</td>
<td>471</td>
<td>477</td>
<td>482</td>
<td>405</td>
<td>449</td>
<td></td>
</tr>
<tr>
<td>BZ</td>
<td>517</td>
<td>507</td>
<td>463</td>
<td>460</td>
<td>472</td>
<td>530</td>
<td>637</td>
<td>525</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>531</td>
<td>543</td>
<td>531</td>
<td>563</td>
<td>564</td>
<td>602</td>
<td>499</td>
<td>526</td>
<td>465</td>
<td>490</td>
<td>453</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FR</td>
<td>332</td>
<td>370</td>
<td>345</td>
<td>344</td>
<td>375</td>
<td>478</td>
<td>584</td>
<td>511</td>
<td>419</td>
<td>414</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKT</td>
<td>317</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IN</td>
<td>587</td>
<td>582</td>
<td>548</td>
<td>578</td>
<td>532</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JP</td>
<td>502</td>
<td>468</td>
<td>450</td>
<td>487</td>
<td>476</td>
<td>521</td>
<td>466</td>
<td>544</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KO</td>
<td>325</td>
<td>317</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ME</td>
<td>340</td>
<td>308</td>
<td>316</td>
<td>368</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MX</td>
<td>499</td>
<td>468</td>
<td>451</td>
<td>429</td>
<td>445</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RF</td>
<td>226</td>
<td>196</td>
<td>206</td>
<td>201</td>
<td>193</td>
<td>201</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SA</td>
<td>268</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>402</td>
<td>468</td>
<td>460</td>
<td>487</td>
<td>509</td>
<td>637</td>
<td>550</td>
<td>651</td>
<td>622</td>
<td>615</td>
<td>638</td>
<td>541</td>
<td>489</td>
</tr>
<tr>
<td>US</td>
<td>683</td>
<td>710</td>
<td>701</td>
<td>758</td>
<td>789</td>
<td>892</td>
<td>531</td>
<td>912</td>
<td>964</td>
<td>997</td>
<td>975</td>
<td>768</td>
<td>918</td>
</tr>
<tr>
<td>Total</td>
<td>5,856</td>
<td>5,252</td>
<td>4,802</td>
<td>5,009</td>
<td>4,714</td>
<td>4,275</td>
<td>4,205</td>
<td>4,140</td>
<td>2,947</td>
<td>2,998</td>
<td>2,471</td>
<td>1,758</td>
<td>1,407</td>
</tr>
</tbody>
</table>

Figure 28. Distribution of respondents according to position level
Country samples are consolidated
Figure 29 identifies the organizational location of respondents in our study. Over half of respondents (55 percent) are located within IT operations, followed by security at 19 percent of respondents and 12 percent of respondents are located within the lines of business.

Figure 30 reports the industry classification of respondents’ organizations. Fifteen percent of respondents are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards. Eleven percent of respondents are located in manufacturing and industrial organizations and 11 percent of respondents are in service organizations. Another nine percent are located in the public sector, including central and local government.
According to Figure 31 the majority of respondents (60 percent) are located in larger-sized organizations with a global headcount of more than 1,000 employees.

**LIMITATIONS**

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from the presented findings. The following items are specific limitations that are germane to most survey-based research studies.

- **Non-response bias:**
  The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners in 14 countries, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.

- **Sampling-frame bias:**
  The accuracy of survey results is dependent upon the degree to which our sampling frames are representative of individuals who are IT or IT security practitioners within the sample of 14 countries selected.

- **Self-reported results:**
  The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process including sanity checks, there is always the possibility that some respondents did not provide truthful responses.

![Figure 31: Distribution of respondents according to organizational headcount](image)
The following tables provide the consolidated results for 14 country samples.

<table>
<thead>
<tr>
<th>Survey response</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>150,066</td>
</tr>
<tr>
<td>Total returns</td>
<td>6,502</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>646</td>
</tr>
<tr>
<td>Final sample</td>
<td>5,856</td>
</tr>
<tr>
<td>Response rate</td>
<td>3.9%</td>
</tr>
</tbody>
</table>

**PART 1. ENCRYPTION POSTURE**

**Q1. Please select one statement that best describes your organization’s approach to encryption implementation across the enterprise.**

<table>
<thead>
<tr>
<th></th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have an overall encryption plan or strategy that is applied consistently across the entire enterprise</td>
<td>45%</td>
</tr>
<tr>
<td>We have a limited encryption plan or strategy that is applied to certain applications and data types</td>
<td>42%</td>
</tr>
<tr>
<td>We don’t have an encryption plan or strategy</td>
<td>13%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Q2. Following are areas where encryption technologies can be deployed. Please check those areas where encryption is extensively deployed, partially deployed or not as yet deployed by your organization.**

<table>
<thead>
<tr>
<th>Q2a-1 Backup and archives</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensively deployed</td>
<td>50%</td>
</tr>
<tr>
<td>Partially deployed</td>
<td>32%</td>
</tr>
<tr>
<td>Not deployed</td>
<td>18%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q2b-1 Big data repositories</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensively deployed</td>
<td>30%</td>
</tr>
<tr>
<td>Partially deployed</td>
<td>24%</td>
</tr>
<tr>
<td>Not deployed</td>
<td>47%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q2c-1 Cloud gateway</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensively deployed</td>
<td>44%</td>
</tr>
<tr>
<td>Partially deployed</td>
<td>31%</td>
</tr>
<tr>
<td>Not deployed</td>
<td>25%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q2d-1 Data center storage</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensively deployed</td>
<td>40%</td>
</tr>
<tr>
<td>Partially deployed</td>
<td>34%</td>
</tr>
<tr>
<td>Not deployed</td>
<td>26%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
<tr>
<td>Table</td>
<td>FY2018</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| Q2e-1. Databases | Extensively deployed: 58%  
Partially deployed: 28%  
Not deployed: 15%  
Total: 100% |
| Q2f-1. Docker containers | Extensively deployed: 26%  
Partially deployed: 32%  
Not deployed: 42%  
Total: 100% |
| Q2g-1. Email | Extensively deployed: 40%  
Partially deployed: 34%  
Not deployed: 27%  
Total: 100% |
| Q2h-1. Public cloud services | Extensively deployed: 40%  
Partially deployed: 29%  
Not deployed: 31%  
Total: 100% |
| Q2i-1. File systems | Extensively deployed: 38%  
Partially deployed: 32%  
Not deployed: 29%  
Total: 100% |
| Q2j-1. Internet communications (e.g., SSL) | Extensively deployed: 62%  
Partially deployed: 26%  
Not deployed: 12%  
Total: 100% |
| Q2k-1. Internal networks (e.g., VPN/LPN) | Extensively deployed: 47%  
Partially deployed: 34%  
Not deployed: 19%  
Total: 100% |
| Q2l-1. Laptop hard drives | Extensively deployed: 55%  
Partially deployed: 25%  
Not deployed: 21%  
Total: 100% |
| Q2m-1 Private cloud infrastructure | Extensively deployed: 35%  
Partially deployed: 31%  
Not deployed: 35%  
Total: 100% |
| Q2n-1 Internet of things (IoT) devices | Extensively deployed: 28%  
Partially deployed: 24%  
Not deployed: 48%  
Total: 100% |
| Q2o-1 Internet of things (IoT) platforms | Extensively deployed: 25%  
Partially deployed: 25%  
Not deployed: 49%  
Total: 100% |
Q3. How many different products does your organization use that perform encryption?  

<table>
<thead>
<tr>
<th>Number of Products</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 3</td>
<td>14%</td>
</tr>
<tr>
<td>4 to 6</td>
<td>23%</td>
</tr>
<tr>
<td>7 to 9</td>
<td>31%</td>
</tr>
<tr>
<td>10 to 12</td>
<td>20%</td>
</tr>
<tr>
<td>13 or more</td>
<td>12%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q4. Who is most influential in directing your organization's encryption strategy? Please select one best choice.  

<table>
<thead>
<tr>
<th>Influential Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT operations</td>
<td>33%</td>
</tr>
<tr>
<td>Security</td>
<td>17%</td>
</tr>
<tr>
<td>Compliance</td>
<td>2%</td>
</tr>
<tr>
<td>Lines of business (LOB) or general management</td>
<td>25%</td>
</tr>
<tr>
<td>No single function has responsibility</td>
<td>22%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q5. What are the reasons why your organization encrypts sensitive and confidential data? Please select the top three reasons.  

<table>
<thead>
<tr>
<th>Reason for Encryption</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>To protect enterprise intellectual property</td>
<td>54%</td>
</tr>
<tr>
<td>To protect customer personal information</td>
<td>54%</td>
</tr>
<tr>
<td>To limit liability from breaches or inadvertent disclosure</td>
<td>29%</td>
</tr>
<tr>
<td>To avoid public disclosure after a data breach occurs</td>
<td>14%</td>
</tr>
<tr>
<td>To protect information against specific, identified threats</td>
<td>51%</td>
</tr>
<tr>
<td>To comply with internal policies</td>
<td>21%</td>
</tr>
<tr>
<td>To comply with external privacy or data security regulations and requirement</td>
<td>46%</td>
</tr>
<tr>
<td>To reduce the scope of compliance audits</td>
<td>31%</td>
</tr>
<tr>
<td>Unsure</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>300%</td>
</tr>
</tbody>
</table>

Q6. What are the biggest challenges in planning and executing a data encryption strategy? Please select the top two reasons.  

<table>
<thead>
<tr>
<th>Challenge for Encryption</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovering where sensitive data resides in the organization</td>
<td>69%</td>
</tr>
<tr>
<td>Classifying which data to encrypt</td>
<td>32%</td>
</tr>
<tr>
<td>Determining which encryption technologies are most effective</td>
<td>16%</td>
</tr>
<tr>
<td>Initially deploying the encryption technology</td>
<td>42%</td>
</tr>
<tr>
<td>Ongoing management of encryption and keys</td>
<td>28%</td>
</tr>
<tr>
<td>Training users to use encryption appropriately</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>200%</td>
</tr>
</tbody>
</table>
### Q7. How important are the following features associated with encryption solutions that may be used by your organization? Very important and important response combined.

<table>
<thead>
<tr>
<th>Feature</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforcement of policy</td>
<td>73%</td>
</tr>
<tr>
<td>Management of keys</td>
<td>66%</td>
</tr>
<tr>
<td>Support for multiple applications or environments</td>
<td>51%</td>
</tr>
<tr>
<td>Separation of duties and role-based controls</td>
<td>54%</td>
</tr>
<tr>
<td>System scalability</td>
<td>59%</td>
</tr>
<tr>
<td>Tamper resistance by dedicated hardware (e.g., HSM)</td>
<td>50%</td>
</tr>
<tr>
<td>Integration with other security tools (e.g., SIEM and ID management)</td>
<td>63%</td>
</tr>
<tr>
<td>Support for regional segregation (e.g., data residency)</td>
<td>43%</td>
</tr>
<tr>
<td>System performance and latency</td>
<td>70%</td>
</tr>
<tr>
<td>Support for emerging algorithms (e.g., ECC)</td>
<td>57%</td>
</tr>
<tr>
<td>Support for cloud and on-premise deployment</td>
<td>68%</td>
</tr>
<tr>
<td>Formal product security certifications (e.g., FIPS 140)</td>
<td>56%</td>
</tr>
</tbody>
</table>

### Q8. What types of data does your organization encrypt? Please select all that apply.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer information</td>
<td>44%</td>
</tr>
<tr>
<td>Non-financial business information</td>
<td>25%</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>51%</td>
</tr>
<tr>
<td>Financial records</td>
<td>54%</td>
</tr>
<tr>
<td>Employee/HR data</td>
<td>51%</td>
</tr>
<tr>
<td>Payment related data</td>
<td>55%</td>
</tr>
<tr>
<td>Healthcare information</td>
<td>24%</td>
</tr>
</tbody>
</table>

### Q9. What are the main threats that might result in the exposure of sensitive or confidential data? Please select the top two choices.

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hackers</td>
<td>30%</td>
</tr>
<tr>
<td>Malicious insiders</td>
<td>21%</td>
</tr>
<tr>
<td>System or process malfunction</td>
<td>30%</td>
</tr>
<tr>
<td>Employee mistakes</td>
<td>54%</td>
</tr>
<tr>
<td>Temporary or contract workers</td>
<td>22%</td>
</tr>
<tr>
<td>Third party service providers</td>
<td>19%</td>
</tr>
<tr>
<td>Lawful data request (e.g., by police)</td>
<td>11%</td>
</tr>
<tr>
<td>Government eavesdropping</td>
<td>12%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>200%</td>
</tr>
</tbody>
</table>
## Q10. Please rate the overall “pain” associated with managing keys or certificates within your organization, where 1 = minimal impact to 10 = severe impact?

<table>
<thead>
<tr>
<th>Pain Rating</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>8%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>12%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>20%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>25%</td>
</tr>
<tr>
<td>9 or 10</td>
<td>36%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

## Q11. What makes the management of keys so painful? Please select the top three reasons.

<table>
<thead>
<tr>
<th>Reason</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>No clear ownership</td>
<td>64%</td>
</tr>
<tr>
<td>Insufficient resources (time/money)</td>
<td>33%</td>
</tr>
<tr>
<td>Lack of skilled personnel</td>
<td>62%</td>
</tr>
<tr>
<td>No clear understanding of requirements</td>
<td>25%</td>
</tr>
<tr>
<td>Key management tools are inadequate</td>
<td>45%</td>
</tr>
<tr>
<td>Systems are isolated and fragmented</td>
<td>50%</td>
</tr>
<tr>
<td>Technology and standards are immature</td>
<td>12%</td>
</tr>
<tr>
<td>Manual processes are prone to errors and unreliable</td>
<td>9%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>300%</td>
</tr>
</tbody>
</table>

## Q12. Following are a wide variety of keys that may be managed by your organization. Please rate the overall “pain” associated with managing each type of key. Very painful and painful response combined.

<table>
<thead>
<tr>
<th>Key Type</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption keys for backups and storage</td>
<td>30%</td>
</tr>
<tr>
<td>Encryption keys for archived data</td>
<td>34%</td>
</tr>
<tr>
<td>Keys associated with SSL/TLS</td>
<td>42%</td>
</tr>
<tr>
<td>SSH keys</td>
<td>57%</td>
</tr>
<tr>
<td>End user encryption keys (e.g., email, full disk encryption)</td>
<td>41%</td>
</tr>
<tr>
<td>Signing keys (e.g., code signing, digital signatures)</td>
<td>51%</td>
</tr>
<tr>
<td>Payments-related keys (e.g., ATM, POS, etc.)</td>
<td>35%</td>
</tr>
<tr>
<td>Keys to embed into devices (e.g., at the time of manufacture in device production environments, or for IoT devices you use)</td>
<td>25%</td>
</tr>
<tr>
<td>Keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys</td>
<td>60%</td>
</tr>
</tbody>
</table>
**PART 3. HARDWARE SECURITY MODULES**

### Q13a. What key management systems does your organization presently use?

<table>
<thead>
<tr>
<th>System</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal key management policy (KMP)</td>
<td>56%</td>
</tr>
<tr>
<td>Formal key management infrastructure (KMI)</td>
<td>44%</td>
</tr>
<tr>
<td>Manual process (e.g., spreadsheet, paper-based)</td>
<td>41%</td>
</tr>
<tr>
<td>Central key management system/server</td>
<td>34%</td>
</tr>
<tr>
<td>Hardware security modules</td>
<td>24%</td>
</tr>
<tr>
<td>Removable media (e.g., thumb drive, CDROM)</td>
<td>31%</td>
</tr>
<tr>
<td>Software-based key stores and wallets</td>
<td>30%</td>
</tr>
<tr>
<td>Smart cards</td>
<td>24%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>283%</td>
</tr>
</tbody>
</table>

### Q13b. What key management systems does your organization presently not used or not aware of use?

<table>
<thead>
<tr>
<th>System</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal key management policy (KMP)</td>
<td>27%</td>
</tr>
<tr>
<td>Formal key management infrastructure (KMI)</td>
<td>29%</td>
</tr>
<tr>
<td>Manual process (e.g., spreadsheet, paper-based)</td>
<td>34%</td>
</tr>
<tr>
<td>Central key management system/server</td>
<td>45%</td>
</tr>
<tr>
<td>Hardware security modules</td>
<td>51%</td>
</tr>
<tr>
<td>Removable media (e.g., thumb drive, CDROM)</td>
<td>50%</td>
</tr>
<tr>
<td>Software-based key stores and wallets</td>
<td>45%</td>
</tr>
<tr>
<td>Smart cards</td>
<td>58%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>339%</td>
</tr>
</tbody>
</table>

### Q14. What best describes your level of knowledge about HSMs?

<table>
<thead>
<tr>
<th>Knowledge Level</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very knowledgeable</td>
<td>36%</td>
</tr>
<tr>
<td>Knowledgeable</td>
<td>28%</td>
</tr>
<tr>
<td>Somewhat knowledgeable</td>
<td>19%</td>
</tr>
<tr>
<td>No knowledge (skip to Q18)</td>
<td>17%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q15a. Does your organization use HSMs?

<table>
<thead>
<tr>
<th>Use of HSMs</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>47%</td>
</tr>
<tr>
<td>No (skip to Q18)</td>
<td>53%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>
Q15b. For what purpose does your organization presently deploy or plan to use HSMs? Please select all that apply.

<table>
<thead>
<tr>
<th>Q15b-1. HSMs used today</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application level encryption</td>
<td>48%</td>
</tr>
<tr>
<td>Database encryption</td>
<td>36%</td>
</tr>
<tr>
<td>Big data encryption</td>
<td>24%</td>
</tr>
<tr>
<td>Public cloud encryption including for Bring Your Own Key (BYOK)</td>
<td>32%</td>
</tr>
<tr>
<td>Private cloud encryption</td>
<td>24%</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>45%</td>
</tr>
<tr>
<td>PKI or credential management</td>
<td>29%</td>
</tr>
<tr>
<td>Internet of Things (IoT) root of trust</td>
<td>22%</td>
</tr>
<tr>
<td>Document signing (e.g. electronic invoicing)</td>
<td>20%</td>
</tr>
<tr>
<td>Code signing</td>
<td>20%</td>
</tr>
<tr>
<td>Payment transaction processing including P2PE</td>
<td>27%</td>
</tr>
<tr>
<td>Payment credential issuing (e.g., mobile, EMV)</td>
<td>24%</td>
</tr>
<tr>
<td>Payment credential provisioning (e.g., mobile, IoT)</td>
<td>30%</td>
</tr>
<tr>
<td>Payment service provider interface (e.g., TSP, real-time payments, Open API)</td>
<td>25%</td>
</tr>
<tr>
<td>With Cloud Access Security Brokers (CASBs) for encryption key management</td>
<td>26%</td>
</tr>
<tr>
<td>With Privileged Access Management (PAM) solutions to protect administrative access</td>
<td>28%</td>
</tr>
<tr>
<td>Blockchain applications (e.g., cryptocurrency, financial transfer)</td>
<td>19%</td>
</tr>
<tr>
<td>Not planning to use</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>487%</td>
</tr>
</tbody>
</table>
## Q15b-2. HSMs planned to be deployed in the next 12 months

<table>
<thead>
<tr>
<th>Technology</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application level encryption</td>
<td>50%</td>
</tr>
<tr>
<td>Database encryption</td>
<td>46%</td>
</tr>
<tr>
<td>Big data encryption</td>
<td>25%</td>
</tr>
<tr>
<td>Public cloud encryption including for Bring Your Own Key (BYOK)</td>
<td>33%</td>
</tr>
<tr>
<td>Private cloud encryption</td>
<td>24%</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>47%</td>
</tr>
<tr>
<td>PKI or credential management</td>
<td>33%</td>
</tr>
<tr>
<td>Internet of Things (IoT) root of trust</td>
<td>24%</td>
</tr>
<tr>
<td>Document signing (e.g. electronic invoicing)</td>
<td>23%</td>
</tr>
<tr>
<td>Code signing</td>
<td>22%</td>
</tr>
<tr>
<td>Payment transaction processing including P2PE</td>
<td>30%</td>
</tr>
<tr>
<td>Payment credential issuing (e.g., mobile, EMV)</td>
<td>28%</td>
</tr>
<tr>
<td>Payment credential provisioning (e.g., mobile, IoT)</td>
<td>27%</td>
</tr>
<tr>
<td>Payment service provider interface (e.g., TSP, real-time payments, Open API)</td>
<td>26%</td>
</tr>
<tr>
<td>With Cloud Access Security Brokers (CASBs) for encryption key management</td>
<td>28%</td>
</tr>
<tr>
<td>With Privileged Access Management (PAM) solutions to protect administrative access</td>
<td>27%</td>
</tr>
<tr>
<td>Blockchain applications (e.g., cryptocurrency, financial transfer)</td>
<td>22%</td>
</tr>
<tr>
<td>Not planning to use</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>529%</strong></td>
</tr>
</tbody>
</table>

## Q15c-1. If you use HSMs in conjunction with public cloud based applications, what models do you use today? Please select all that apply.

<table>
<thead>
<tr>
<th>Model</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rent/use HSMs from public cloud provider, hosted in the cloud</td>
<td>36%</td>
</tr>
<tr>
<td>Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications</td>
<td>47%</td>
</tr>
<tr>
<td>Own and operate HSMs for the purpose of generating and managing BYOK (Bring Your Own Key) keys to send to the cloud for use by the cloud provider</td>
<td>17%</td>
</tr>
<tr>
<td>Own and operate HSMs that integrate with a Cloud Access Security Broker to manage keys and cryptographic operations (e.g., encrypting data on the way to the cloud, managing keys for cloud applications)</td>
<td>12%</td>
</tr>
<tr>
<td>Not using HSMs with public cloud applications</td>
<td>1%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>113%</strong></td>
</tr>
<tr>
<td>Q15c-2. If you use HSMs in conjunction with public cloud based applications, what models do you plan to use in the next 12 months. Please select all that apply.</td>
<td>FY2018</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Rent/use HSMs from public cloud provider, hosted in the cloud</td>
<td>44%</td>
</tr>
<tr>
<td>Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications</td>
<td>53%</td>
</tr>
<tr>
<td>Own and operate HSMs for the purpose of generating and managing BYOK (Bring Your Own Key) keys to send to the cloud for use by the cloud provider</td>
<td>24%</td>
</tr>
<tr>
<td>Own and operate HSMs that integrate with a Cloud Access Security Broker to manage keys and cryptographic operations (e.g., encrypting data on the way to the cloud, managing keys for cloud applications)</td>
<td>24%</td>
</tr>
<tr>
<td>Not using HSMs with public cloud applications</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>145%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q16. In your opinion, how important are HSMs to your encryption or key management strategy? Very important and important response combined</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q16a. Importance today</td>
<td>60%</td>
</tr>
<tr>
<td>Q16b. Importance in the next 12 months</td>
<td>69%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q17. Which statement best describes how your organization uses HSMs?</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have a centralized team that provides cryptography as a service (including HSMs) to multiple applications/teams within our organization (i.e. private cloud model).</td>
<td>60%</td>
</tr>
<tr>
<td>Each individual application owner/team is responsible for their own cryptographic services (including HSMs) (i.e. traditional siloed, application-specific data center deployment).</td>
<td>40%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

**PART 6: CLOUD ENCRYPTION:** WHEN RESPONDING TO THE FOLLOWING QUESTIONS, PLEASE ASSUME THEY REFER ONLY TO PUBLIC CLOUD SERVICES

<table>
<thead>
<tr>
<th>Q37. Does your organization currently use cloud computing services for any class of data or application – both sensitive and non-sensitive?</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, we are presently doing so</td>
<td>67%</td>
</tr>
<tr>
<td>No, but we are likely to do so in the next 12 to 24 months</td>
<td>16%</td>
</tr>
<tr>
<td>No (Go to Part 7 if you do not use cloud services for any class of data or application)</td>
<td>16%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
### Q38. Do you currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism)?

<table>
<thead>
<tr>
<th>Option</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, we are presently doing so</td>
<td>60%</td>
</tr>
<tr>
<td>No, but we are likely to do so in the next 12 to 24 months</td>
<td>22%</td>
</tr>
<tr>
<td>No (Go to Part 7 if you do not use or plan to use any cloud services for sensitive or confidential data)</td>
<td>17%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q39. In your opinion, who is most responsible for protecting sensitive or confidential data transferred to the cloud?

<table>
<thead>
<tr>
<th>Option</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cloud provider</td>
<td>44%</td>
</tr>
<tr>
<td>The cloud user</td>
<td>23%</td>
</tr>
<tr>
<td>Shared responsibility</td>
<td>33%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q40. How does your organization protect data at rest in the cloud?

<table>
<thead>
<tr>
<th>Option</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption performed in the cloud using keys generated/managed by the cloud provider</td>
<td>35%</td>
</tr>
<tr>
<td>Encryption performed in the cloud using keys my organization generates and manages on-premise</td>
<td>21%</td>
</tr>
<tr>
<td>Encryption performed on-premise prior to sending data to the cloud using keys my organization generates and manages</td>
<td>44%</td>
</tr>
<tr>
<td>Tokenization performed by the cloud provider</td>
<td>13%</td>
</tr>
<tr>
<td>Tokenization performed on-premise prior to sending data to the cloud</td>
<td>12%</td>
</tr>
<tr>
<td>None of the above</td>
<td>6%</td>
</tr>
<tr>
<td>Total</td>
<td>130%</td>
</tr>
</tbody>
</table>

### Q41. For encryption of data at rest in the cloud, my organization's strategy is to...

<table>
<thead>
<tr>
<th>Option</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only use keys controlled by my organization</td>
<td>41%</td>
</tr>
<tr>
<td>Only use keys controlled by the cloud provider</td>
<td>18%</td>
</tr>
<tr>
<td>Use a combination of keys controlled by my organization and the cloud provider, with a preference for keys controlled by my organization</td>
<td>19%</td>
</tr>
<tr>
<td>Use a combination of keys controlled by my organization and the cloud provider, with a preference for keys controlled by the cloud provider</td>
<td>22%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
### Q42. How important are the following features associated with cloud encryption to your organization?

<table>
<thead>
<tr>
<th>Feature</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bring Your Own Key (BYOK) management support</td>
<td>47%</td>
</tr>
<tr>
<td>Privileged user access control</td>
<td>49%</td>
</tr>
<tr>
<td>Granular access controls</td>
<td>58%</td>
</tr>
<tr>
<td>Audit logs identifying key usage</td>
<td>56%</td>
</tr>
<tr>
<td>Audit logs identifying data access attempts</td>
<td>41%</td>
</tr>
<tr>
<td>SIEM integration, visualization and analysis of logs</td>
<td>60%</td>
</tr>
<tr>
<td>Support for FIPS 140-2 compliant key management</td>
<td>35%</td>
</tr>
<tr>
<td>Support for the KMIP standard for key management</td>
<td>73%</td>
</tr>
<tr>
<td>Ability to encrypt and rekey data while in use without downtime</td>
<td>47%</td>
</tr>
</tbody>
</table>

### Q43-1. How many public cloud providers does your organization in use today?

<table>
<thead>
<tr>
<th>Quantity</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>36%</td>
</tr>
<tr>
<td>2</td>
<td>26%</td>
</tr>
<tr>
<td>3</td>
<td>16%</td>
</tr>
<tr>
<td>4 or more</td>
<td>21%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q43-2. How many public cloud providers does your organization plan to use in the next 12 to 24 months?

<table>
<thead>
<tr>
<th>Quantity</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>26%</td>
</tr>
<tr>
<td>2</td>
<td>21%</td>
</tr>
<tr>
<td>3</td>
<td>18%</td>
</tr>
<tr>
<td>4 or more</td>
<td>34%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

### PART 7: ROLE AND ORGANIZATIONAL CHARACTERISTICS

#### D1. What organizational level best describes your current position?

<table>
<thead>
<tr>
<th>Position</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Executive</td>
<td>3%</td>
</tr>
<tr>
<td>Vice President</td>
<td>3%</td>
</tr>
<tr>
<td>Director</td>
<td>17%</td>
</tr>
<tr>
<td>Manager/Supervisor</td>
<td>33%</td>
</tr>
<tr>
<td>Associate/Staff/Technician</td>
<td>42%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
### D2. Select the functional area that best describes your organizational location.

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT operations</td>
<td>55%</td>
</tr>
<tr>
<td>Security</td>
<td>19%</td>
</tr>
<tr>
<td>Compliance</td>
<td>7%</td>
</tr>
<tr>
<td>Finance</td>
<td>4%</td>
</tr>
<tr>
<td>Lines of business (LOB)</td>
<td>12%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

### D4. What industry best describes your organization’s industry focus?

<table>
<thead>
<tr>
<th>Industry</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture &amp; food services</td>
<td>1%</td>
</tr>
<tr>
<td>Communications</td>
<td>3%</td>
</tr>
<tr>
<td>Consumer products</td>
<td>4%</td>
</tr>
<tr>
<td>Defense &amp; aerospace</td>
<td>0%</td>
</tr>
<tr>
<td>Education &amp; research</td>
<td>3%</td>
</tr>
<tr>
<td>Energy &amp; utilities</td>
<td>7%</td>
</tr>
<tr>
<td>Entertainment &amp; media</td>
<td>2%</td>
</tr>
<tr>
<td>Financial services</td>
<td>15%</td>
</tr>
<tr>
<td>Health &amp; pharmaceutical</td>
<td>8%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>3%</td>
</tr>
<tr>
<td>Manufacturing &amp; industrial</td>
<td>11%</td>
</tr>
<tr>
<td>Pharmaceuticals</td>
<td>1%</td>
</tr>
<tr>
<td>Public sector</td>
<td>9%</td>
</tr>
<tr>
<td>Retailing</td>
<td>7%</td>
</tr>
<tr>
<td>Services</td>
<td>11%</td>
</tr>
<tr>
<td>Technology &amp; software</td>
<td>8%</td>
</tr>
<tr>
<td>Transportation</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

### D5. What is the worldwide headcount of your organization?

<table>
<thead>
<tr>
<th>Headcount Range</th>
<th>FY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 500</td>
<td>15%</td>
</tr>
<tr>
<td>500 to 1,000</td>
<td>26%</td>
</tr>
<tr>
<td>1,001 to 5,000</td>
<td>32%</td>
</tr>
<tr>
<td>5,001 to 25,000</td>
<td>19%</td>
</tr>
<tr>
<td>25,001 to 75,000</td>
<td>6%</td>
</tr>
<tr>
<td>More than 75,000</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
ABOUT PONEMON INSTITUTE

The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries.

ABOUT NCIPHER SECURITY

Today’s fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks. nCipher Security, a leader in the general purpose hardware security module (HSM) market, empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies – cloud, IoT, blockchain, digital payments – and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times. www.ncipher.com
Today’s fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks.