THALES

Ponemon INSTITUTE

BRAZIL ENCRYPTION TRENDS STUDY

July 2018

TABLE OF CONTENTS

OUR SPONSORS

VENAFI

GEOBRIDGE

CSA cloud security alliance

GuidePoint SECURITY

CRITICALSTART

OASIS

Sponsored by Thales eSecurity

INDEPENDENTLY CONDUCTED BY PONEMON INSTITUTE LLC

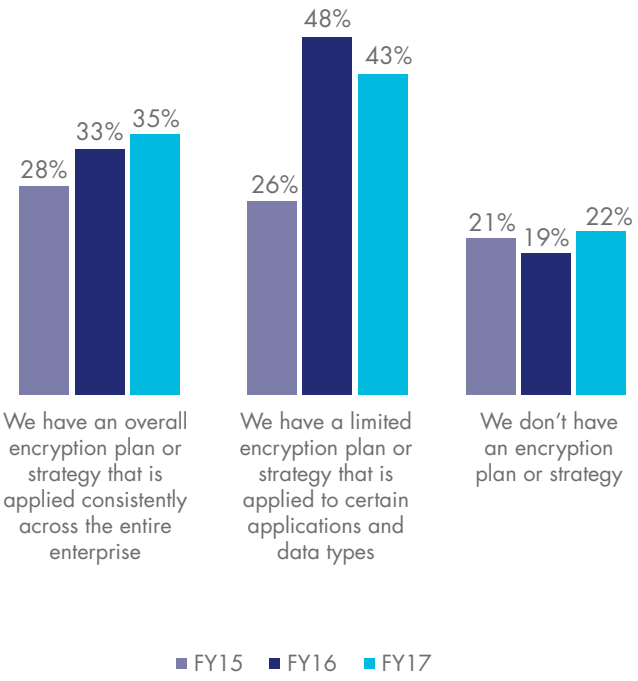
PART 1. EXECUTIVE SUMMARY

Ponemon Institute is pleased to present the findings of the *2018 Brazil Encryption Trends Study,* sponsored by Thales eSecurity. We surveyed 507 individuals in Brazil to examine the use of encryption and the impact of this technology on the security posture of organizations in this region.

The first encryption study trends study was conducted in 2005 for a U.S. sample of respondents. Since then we have expanded the scope of the research to include respondents in 11 countries plus Brazil. The 11 countries include: Australia, France, Germany, India, Japan, Mexico, the Middle East, the Russian Federation, the United Kingdom, the United States and, for the first time, South Korea.

As shown in Figure 1, more organizations represented in this research continue to recognize the importance of having an encryption strategy, either an enterprise-wide (35 percent of respondents) or a limited strategy that targets certain applications and data types (43 percent of respondents).

Figure 1. What best describes your organization's encryption strategy?



Following is a summary of our key findings. More details are provided for each key finding listed below in the next section of this report.

IT operations continue to have the most influence in directing encryption strategies. While responsibility for the encryption strategy is dispersed throughout the organization, IT operations (33 percent of respondents) has the most influence. Twenty-eight percent of respondents say no one single function is responsible for encryption strategy.

Which data types are most often encrypted? More companies are encrypting financial records and payment-related data. Fewer companies are encrypting employee/HR data and non-financial business information in this year's research.

Employee mistakes are the most significant threats to sensitive data. The most significant threats to the exposure of sensitive or confidential data are employee mistakes, according to 43 percent of respondents. Thirty-three percent of respondents say government eavesdropping and 30 percent of respondents say malicious insiders pose the most significant threat to sensitive or confidential data.

Protection of customers' personal information is the main driver for using encryption technologies. The importance of protecting customers' personal information has increased significantly in the past three years (50 percent of respondents vs. 61 percent of respondents in this year's research). The protection of information against specific, identified threats has also increased significantly from 37 percent of respondents in 2015 to 59 percent of respondents in this year's research. In contrast, compliance with external privacy or data security regulations and requirements (42 percent of respondents) and to reduce the scope of compliance audits (29 percent of respondents) have declined as drivers for using encryption technologies.

The initial deployment of encryption technology continues to be the biggest challenge. Fifty-two percent of respondents say initially deploying the encryption technology is the biggest challenge in planning and executing a data encryption strategy. In the past three years, the challenge of classifying which data to encrypt has increased from 42 percent of respondents to 50 percent of respondents in this year's research.

No single encryption technology dominates because organizations have very diverse needs. Internet communications, encryption of databases and internal networks are most likely to be extensively deployed. In contrast, Internet of Things (IoT) platforms and devices, a nascent but emerging use case, and docker containers are the least likely to be deployed.

Certain encryption features are considered more critical than others. In the past three years, enforcement of policy and system scalability features have increased the most in importance. Management of keys, support for cloud and on-premises deployment and support for multiple applications or environments have decreased but remain at high levels.

How painful is key management? Fifty-nine percent (24 + 35) of respondents report the management of keys is painful. The top reasons for the pain are: lack of skilled personnel, no clear ownership, systems are isolated and fragmented, and key management tools are inadequate. Respondents' companies continue to use a variety of key management systems. The most commonly deployed systems are manual process (e.g., spreadsheet, paper-based) and formal key management policy (KMP).

Which keys are most difficult to manage? The keys most difficult to manage are keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys, signing keys, and SSH keys. These keys have demonstrated modest decreases in management difficulty but still remain at significant levels.

The importance of HSMs to an encryption or key management strategy will grow in the next 12 months. Forty-four percent of respondents say they are important today and 51 percent of respondents say they will be important in the next 12 months. SSL/TLS, payment transaction processing including P2PE, application level encryption, database encryption, payment service provider interface and payment credential provisioning are growing use cases for HSMs.

How organizations are using HSMs. Fifty-five percent of respondents say they have a centralized team that provides cryptography as a service and 45 percent of respondents say each individual application owner/team is responsible for their own cryptographic services. The global average for the use of a centralized team is 61 percent of respondents.

Most organizations transfer sensitive or confidential data to the cloud. Forty-six percent of respondents say their organizations currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism) and 39 percent of respondents plan to in the next 12 to 24 months. Thirty-seven percent of respondents say it is the cloud provider who is most responsible for protecting sensitive or confidential data transferred to the cloud.

How is data at rest in the cloud protected? Forty-three percent of respondents say encryption is performed in the cloud using keys the cloud provider generates and manages and 40 percent of respondents say encryption is performed on-premises prior to sending data to the cloud using keys their organization generates and manages.

35%

of organizations now have a consistent, enterprise-wide **encryption strategy**

PART 2. KEY FINDINGS

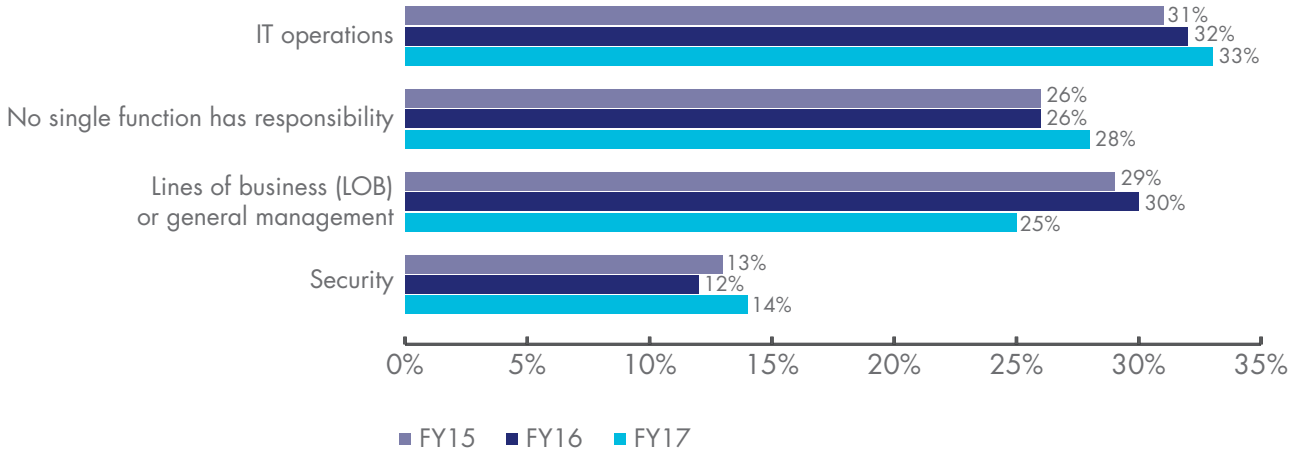
In this section, we present an analysis of the key findings. The complete audited findings are presented in the appendix of the report. We have organized the report according to the following themes:

- Strategy and adoption of encryption
- Threats, main drivers and priorities
- Deployment choices
- Encryption features considered most important
- Attitudes about key management
- Importance of hardware security modules (HSMs)[1]
- Cloud encryption

Strategy and adoption of encryption

IT operations continue to have the most influence in directing encryption strategies. As shown in Figure 2, while responsibility for the encryption strategy is dispersed throughout the organization, IT operations (33 percent of respondents) has the most influence. Twenty-eight percent of respondents say no one single function is responsible for encryption strategy.

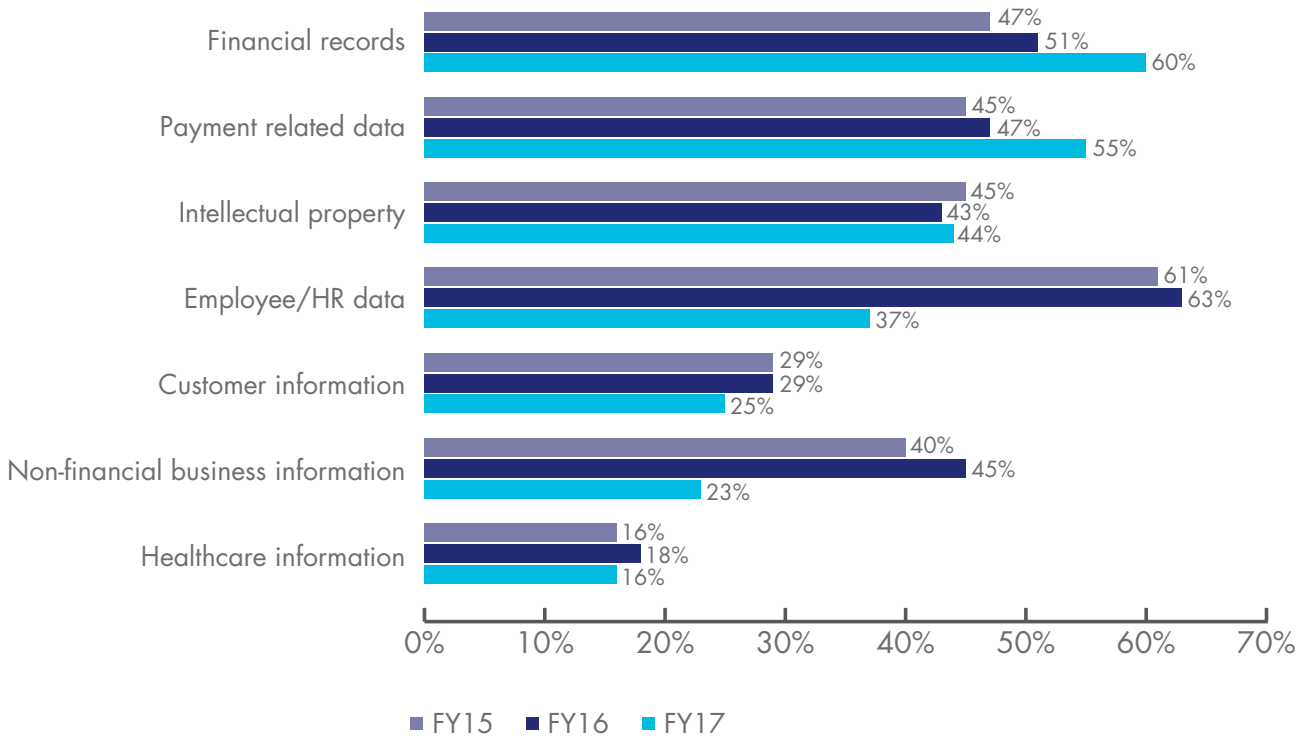
Figure 2. Influence of IT operations, lines of business and security



[1] 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.

Which data types are most often encrypted? Figure 3 provides a list of seven data types that are routinely encrypted by respondents' organizations. As shown, more companies are encrypting financial records and payment-related data. Fewer companies are encrypting employee/HR data and non-financial business information in this year's research.

Figure 3. Data types routinely encrypted
More than one response permitted

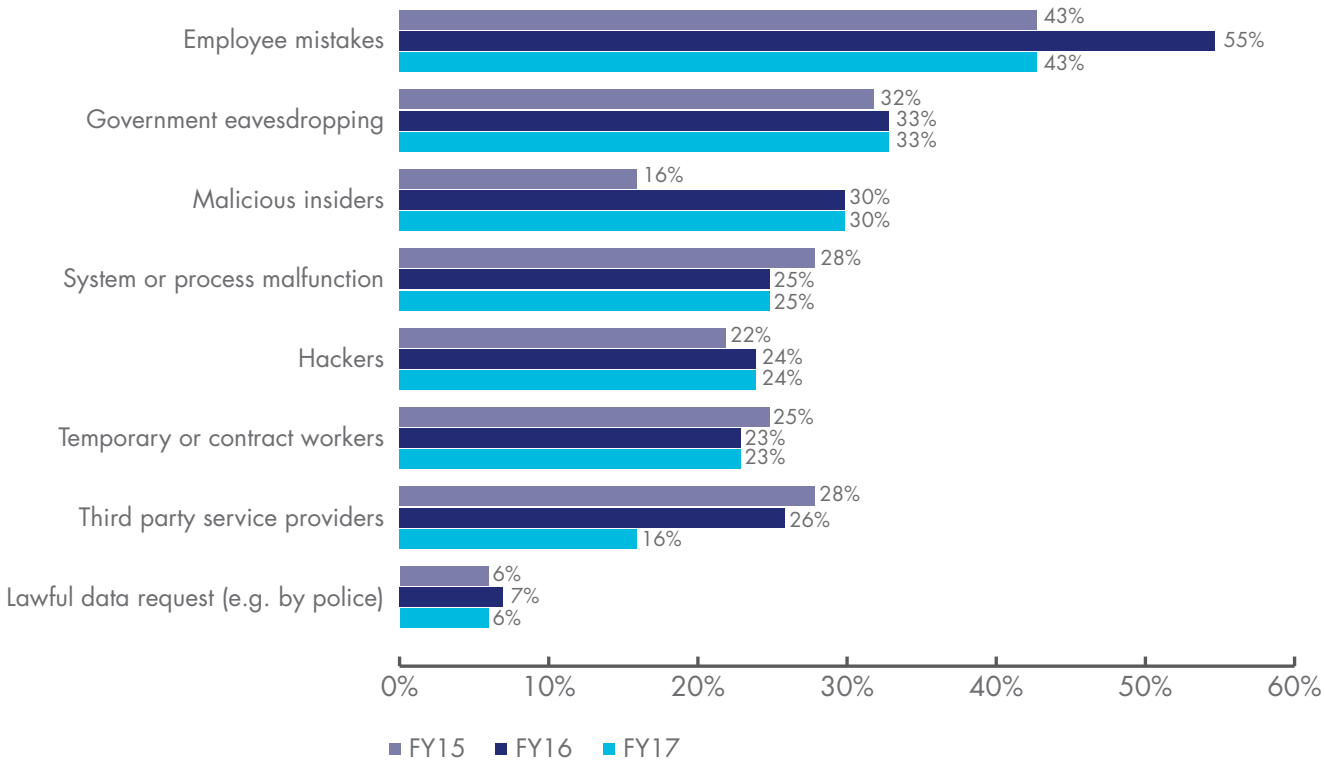


"MORE COMPANIES ARE ENCRYPTING FINANCIAL RECORDS AND PAYMENT-RELATED DATA. FEWER COMPANIES ARE ENCRYPTING EMPLOYEE/HR DATA AND NON-FINANCIAL BUSINESS INFORMATION IN THIS YEAR'S RESEARCH."

Threats, main drivers and priorities

Employee mistakes are the most significant threats to sensitive data. Figure 4 reveals the most significant threats to the exposure of sensitive or confidential data are employee mistakes, according to 43 percent of respondents. Thirty-three percent of respondents say government eavesdropping and 30 percent of respondents say malicious insiders pose the most significant threat to sensitive or confidential data.

Figure 4. The main threats that might expose of sensitive or confidential data
Two responses permitted

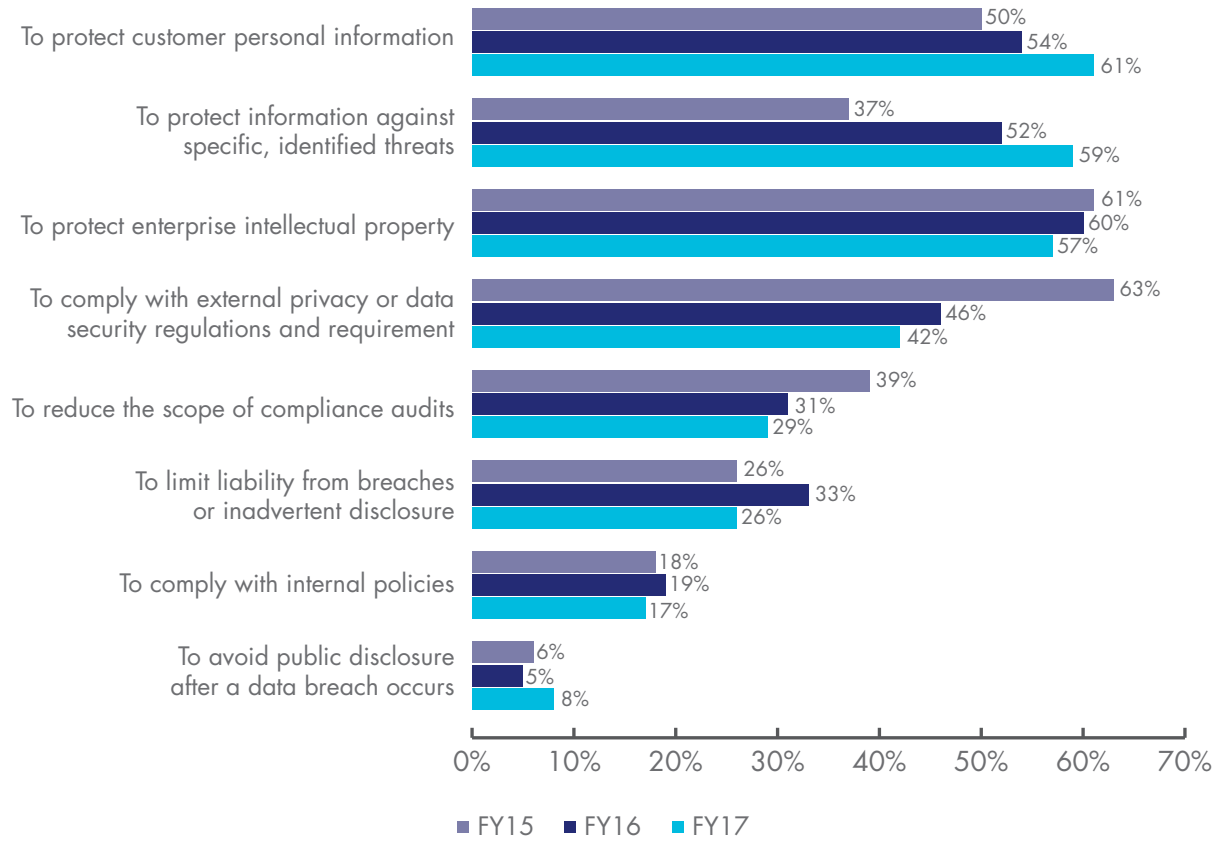


"THIRTY-THREE PERCENT OF RESPONDENTS SAY GOVERNMENT EAVESDROPPING AND 30 PERCENT OF RESPONDENTS SAY MALICIOUS INSIDERS POSE THE MOST SIGNIFICANT THREAT TO SENSITIVE OR CONFIDENTIAL DATA."

Protection of customers' personal information is the main driver to using encryption technologies. Eight drivers for deploying encryption are presented in Figure 5. The importance of protecting customers' personal information has increased significantly in the past three years (50 percent of respondents vs. 61 percent of respondents in this year's research). The protection of information against specific, identified threats has also increased significantly from 37 percent of respondents in 2015 to 59 percent of respondents in this year's research.

In contrast, compliance with external privacy or data security regulations and requirements (42 percent of respondents) and to reduce the scope of compliance audits (29 percent of respondents) have declined as drivers in using encryption technologies.

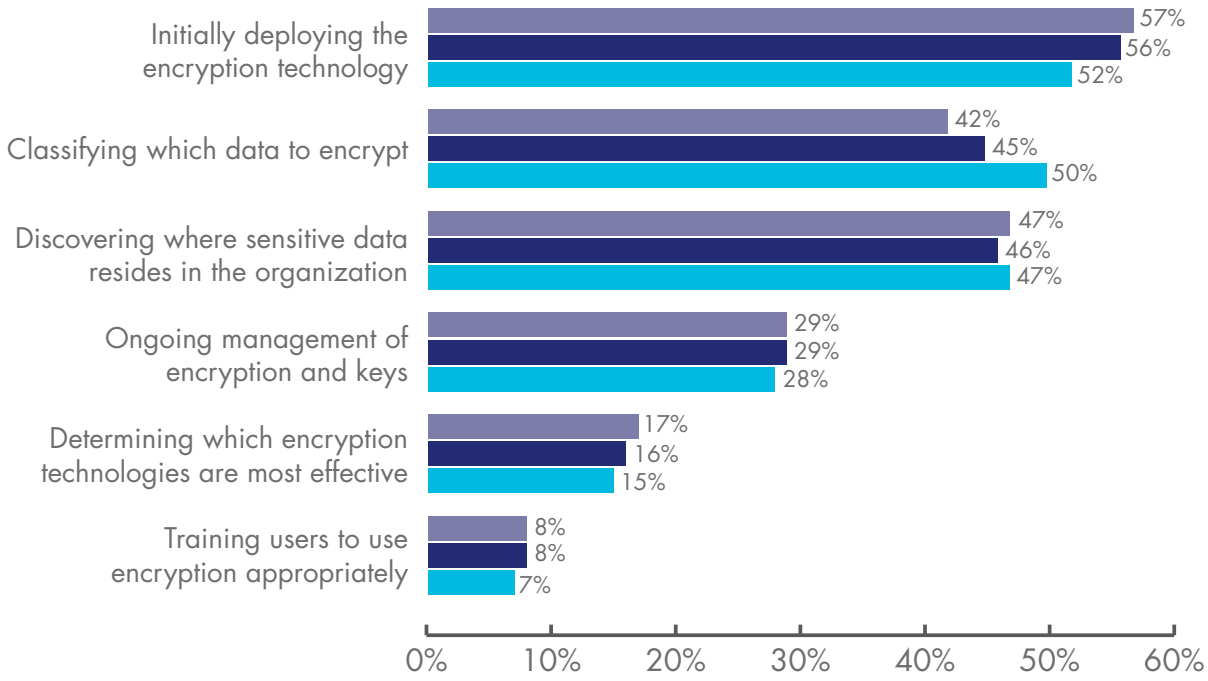
Figure 5. The main drivers for using encryption technology solutions
Three responses permitted



"THE IMPORTANCE OF PROTECTING CUSTOMERS' PERSONAL INFORMATION HAS INCREASED SIGNIFICANTLY IN THE PAST THREE YEARS (50 PERCENT OF RESPONDENTS VS. 61 PERCENT OF RESPONDENTS IN THIS YEAR'S RESEARCH)."

The initial deployment of encryption technology continues to be the biggest challenge in planning and executing a data encryption strategy. Figure 6 provides a list of six challenges to an organization's effective execution of its data encryption strategy in descending order of importance. In the past three years, the challenge of classifying which data to encrypt has increased from 42 percent of respondents to 50 percent of respondents in this year's research.

Figure 6. Biggest challenges in planning and executing a data encryption strategy
Two responses permitted



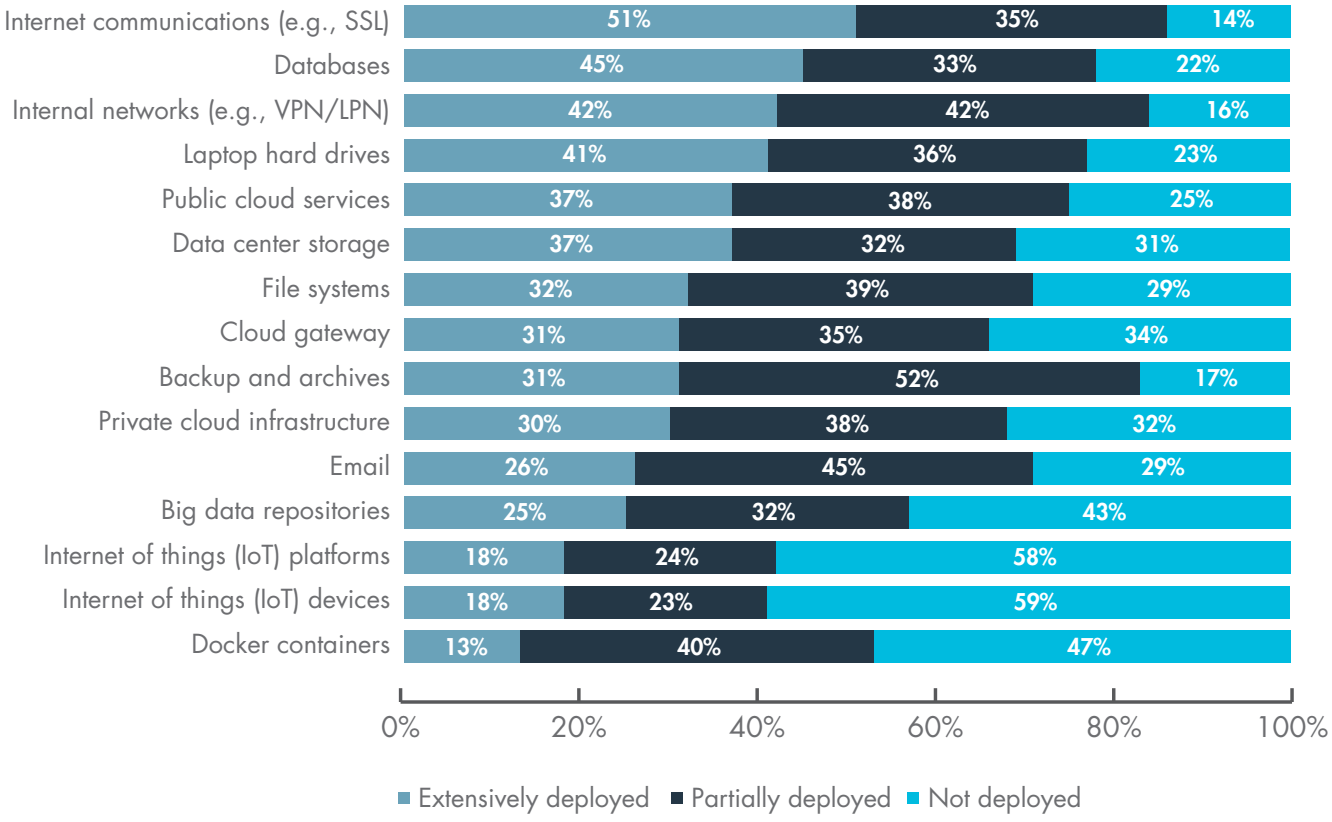
"IN THE PAST THREE YEARS, THE CHALLENGE OF CLASSIFYING WHICH DATA TO ENCRYPT HAS INCREASED FROM 42 PERCENT OF RESPONDENTS TO 50 PERCENT OF RESPONDENTS IN THIS YEAR'S RESEARCH."

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 (a.k.a. point solution).

As shown in Figure 7, no single technology dominates because organizations have very diverse needs. Encryption of Internet communications, databases, internal networks and laptop hard drives are most likely to be extensively deployed. In contrast, Internet of Things (IoT) platforms and devices, a nascent but emerging use case, and docker containers are less likely to be fully or partially deployed.

Figure 7. The use of encryption technologies

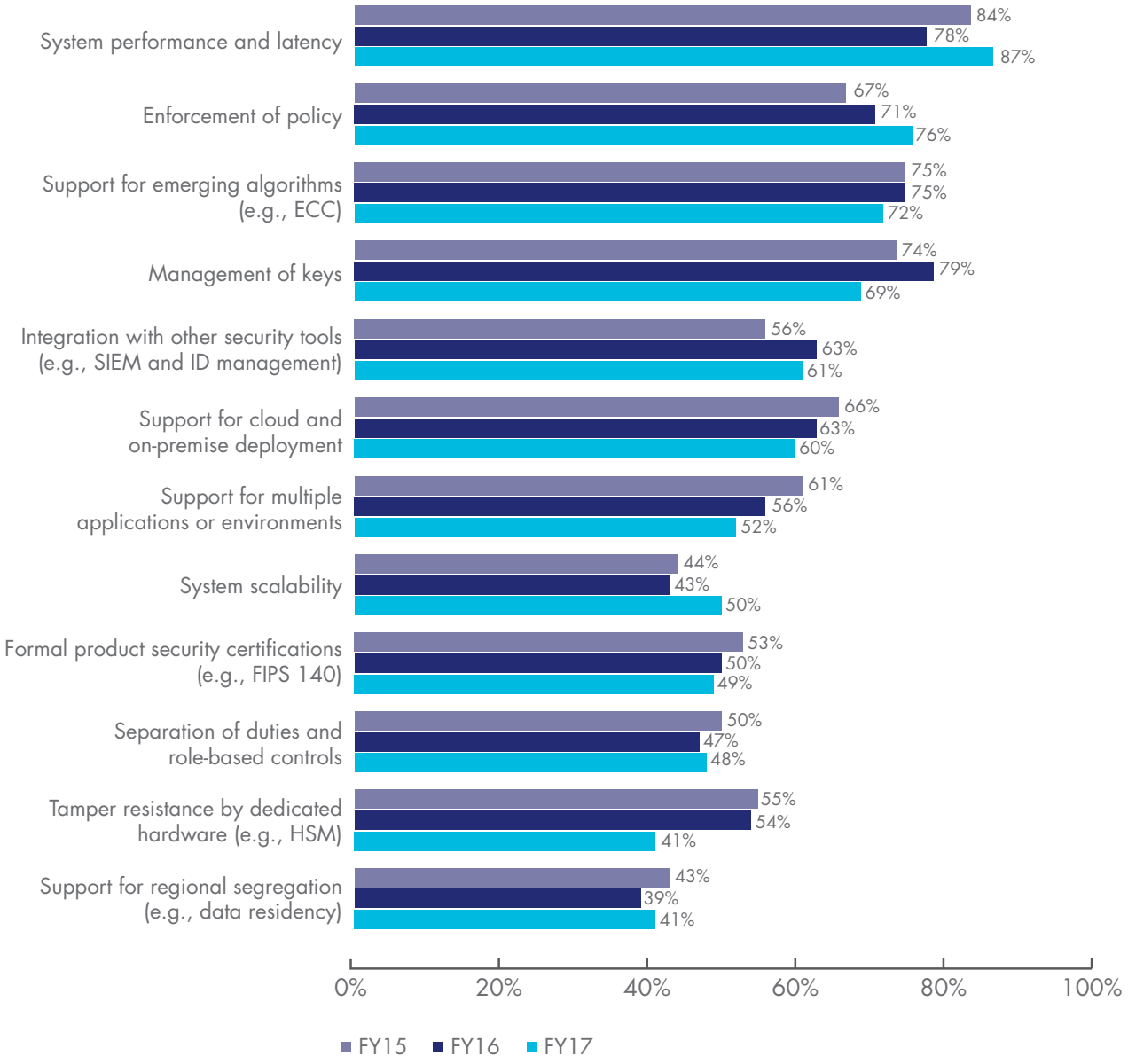


Encryption features considered most important

Certain encryption features are considered more critical than others. Figure 8 lists 12 encryption technology features. Each percentage defines the very important and important responses (on a four point scale). Respondents were asked to rate encryption technology features considered most important to their organization's security posture.

In the past three years, enforcement of policy and system scalability features have increased the most in importance. Management of keys, support for cloud and on-premises deployment and support for multiple applications or environments have decreased but remain at high levels.

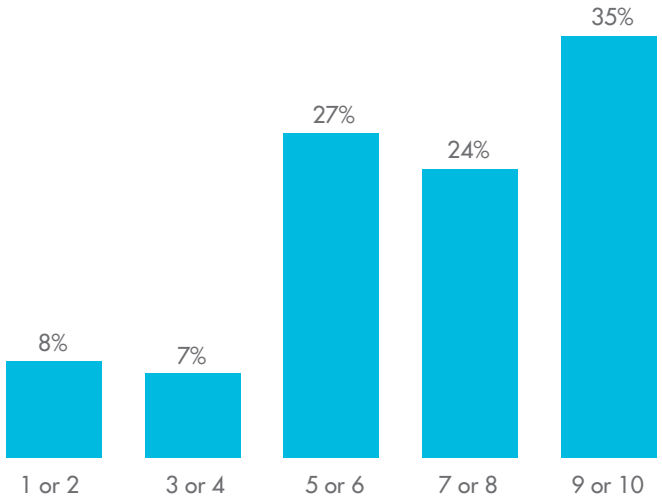
Figure 8. Most important features of encryption technology solutions
Very important and Important response combined



Attitudes about key management

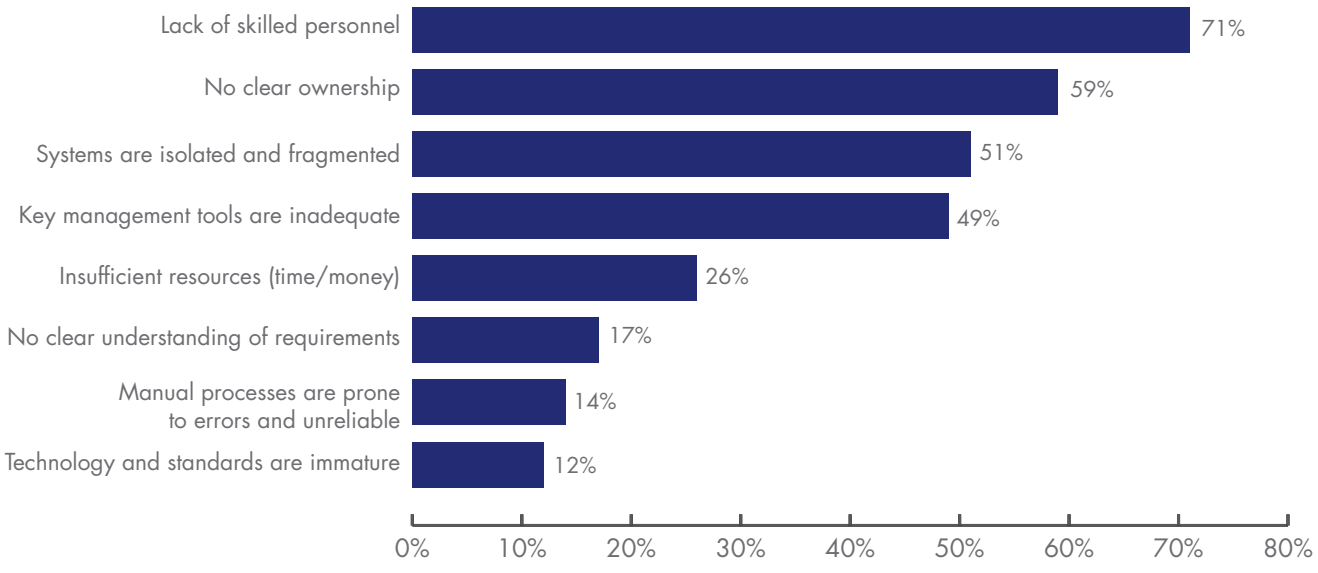
How painful is key management? Using a 10-point scale, respondents were asked to rate the overall "pain" associated with managing keys within their organization, where 1 = minimal impact to 10 = severe impact. Figure 9 shows that 59 percent (24 + 35) of respondents chose ratings at 7 or above, thus suggesting a fairly high pain threshold.

Figure 9. How painful is key management?
1 = minimal impact to 10 = severe impact



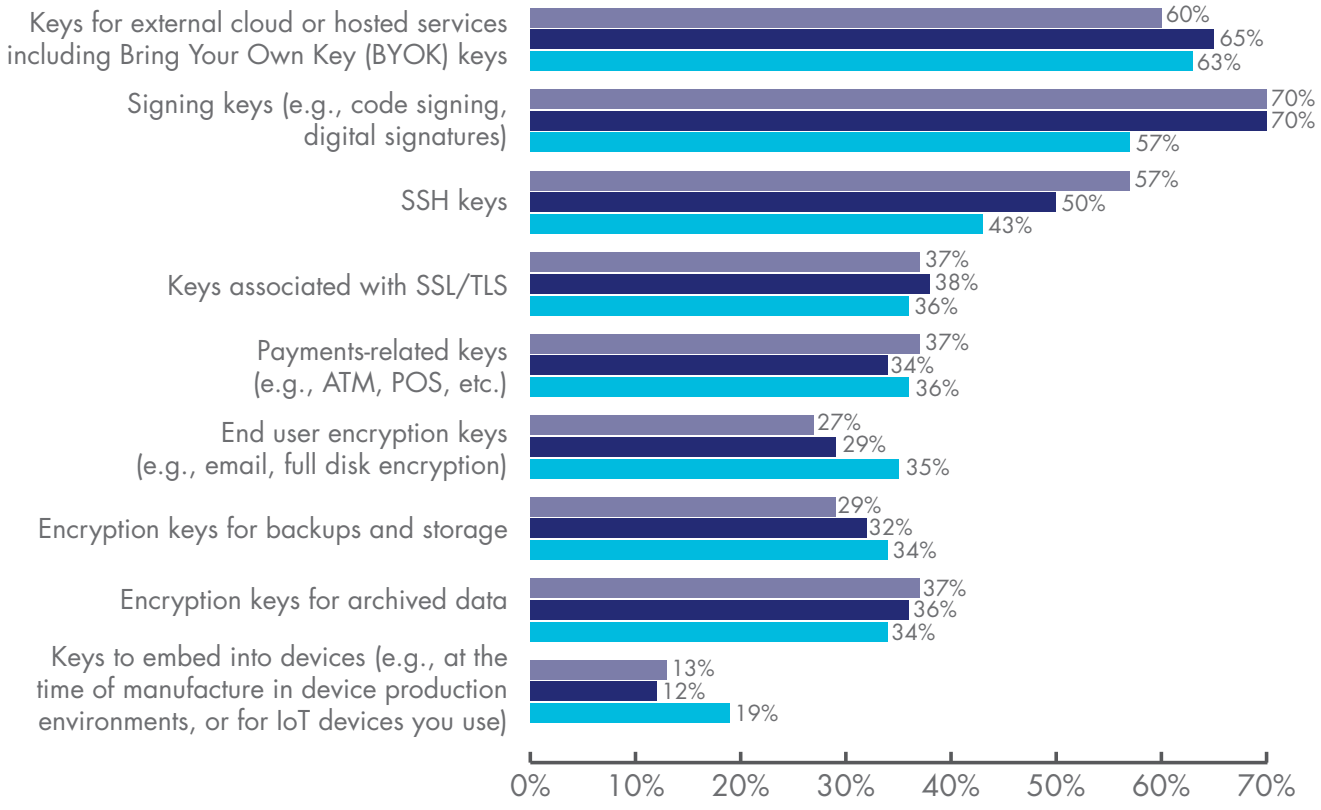
Why is key management painful? Figure 10 shows the reasons why the management of keys is so difficult. The top reasons are: lack of skilled personnel, no clear ownership and systems are isolated and fragmented.

Figure 10. What makes the management of keys so painful?
Three responses permitted



Which keys are most difficult to manage? According to Figure 11, companies continue to experience the pain of managing certain keys. These are: keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys, signing keys (e.g., code signing, digital signatures) and SSH keys. These keys have decreased in management difficulty but still remain at significant levels.

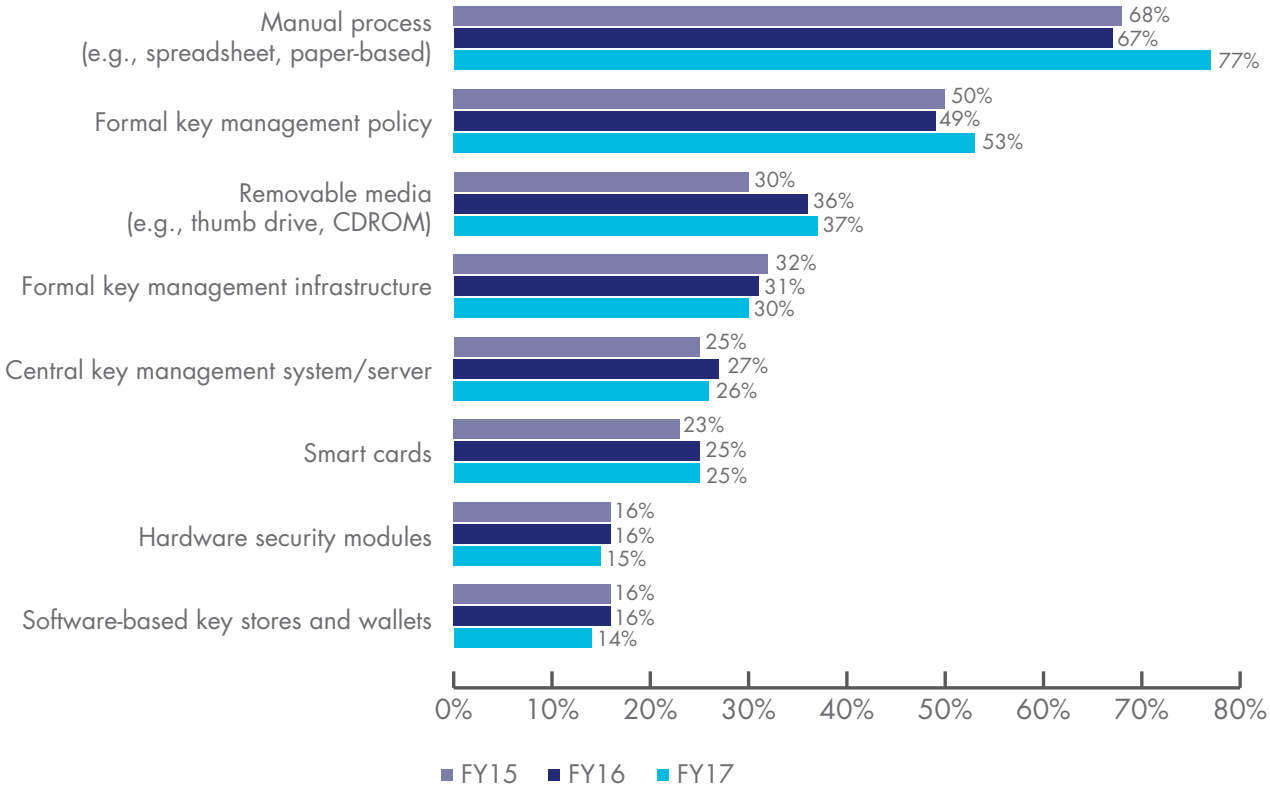
Figure 11. Types of keys most difficult to manage
Very painful and Painful response combined



"COMPANIES CONTINUE TO EXPERIENCE THE PAIN OF MANAGING CERTAIN KEYS. THESE ARE: KEYS FOR EXTERNAL CLOUD OR HOSTED SERVICES INCLUDING BRING YOUR OWN KEY (BYOK) KEYS, SIGNING KEYS (E.G., CODE SIGNING, DIGITAL SIGNATURES) AND SSH KEYS. THESE KEYS HAVE DECREASED IN MANAGEMENT DIFFICULTY BUT STILL REMAIN AT SIGNIFICANT LEVELS."

As shown in Figure 12, respondents' companies continue to use a variety of key management systems. The most commonly deployed systems are: manual process (e.g., spreadsheet, paper-based) and formal key management policy (KMP).

Figure 12. What key management systems does your organization presently use?
More than one response permitted

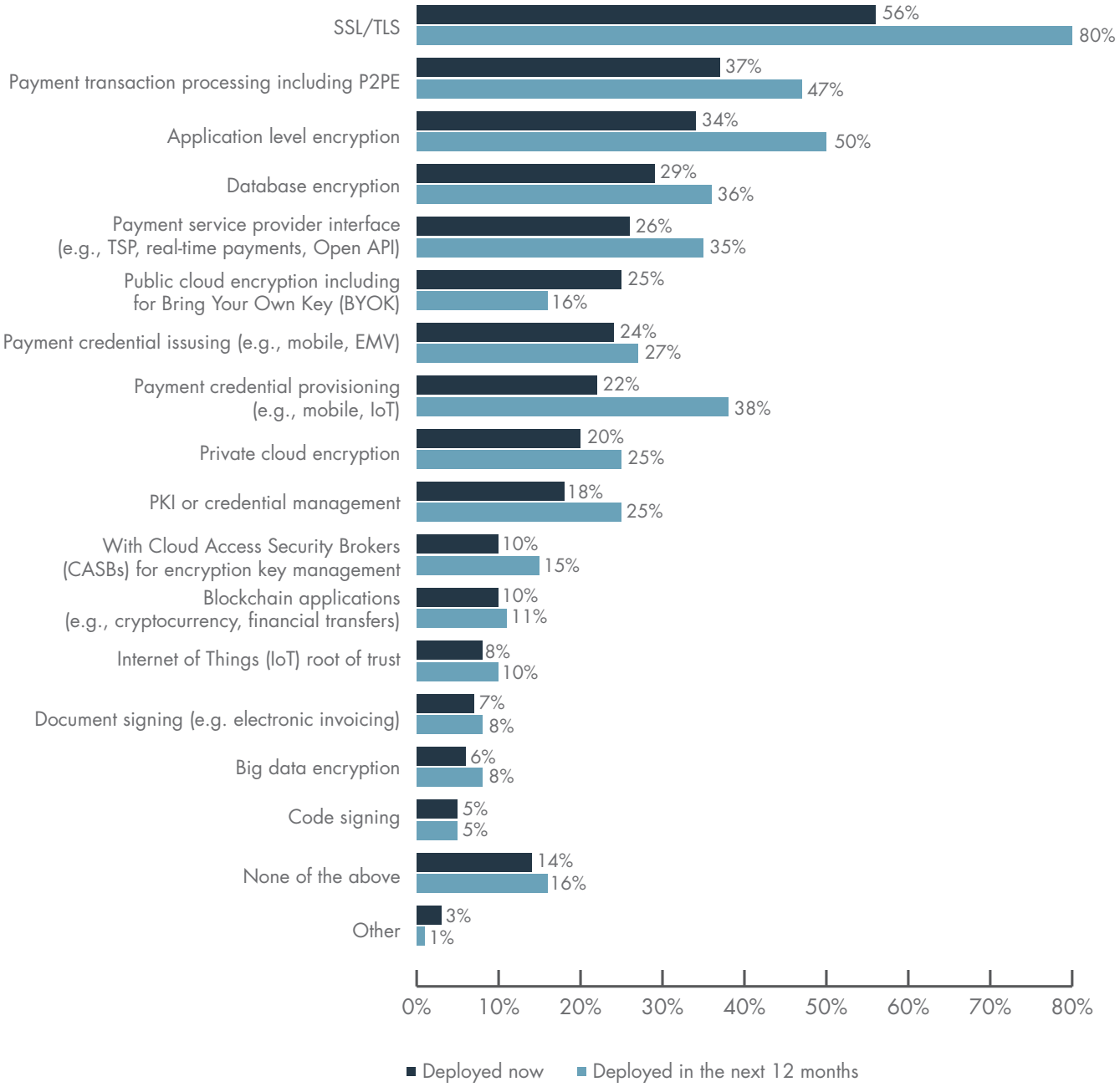


"COMPANIES CONTINUE TO USE A VARIETY OF KEY MANAGEMENT SYSTEMS. THE MOST COMMONLY DEPLOYED SYSTEMS ARE: MANUAL PROCESS (E.G., SPREADSHEET, PAPER-BASED) AND FORMAL KEY MANAGEMENT POLICY (KMP)."

Importance of hardware security modules (HSMs)

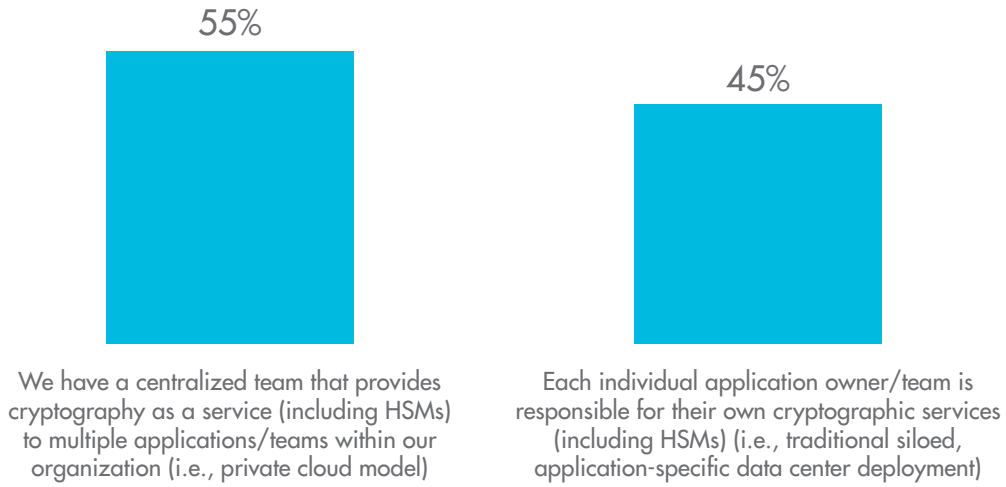
The importance of HSMs to an encryption or key management strategy will grow in the next 12 months. We asked respondents in organizations that currently deploy HSMs how important they are to their encryption or key management strategy. Forty-four percent of respondents say they are important today and 51 percent of respondents say they will be important in the next 12 months. Figure 13 summarizes the primary purposes or use cases for deploying HSMs. SSL/TLS, payment transaction processing including P2PE, application level encryption, database encryption, payment service provider interface and payment credential provisioning are growing use cases for HSMs.

Figure 13. How HSMs are deployed or will be deployed in the next 12 months
More than one response permitted



How organizations are using HSMs. According to Figure 14, 55 percent of respondents say they have a centralized team that provides cryptography as a service and 45 percent of respondents say each individual application owner/team is responsible for their own cryptographic services. The global average in the use of a centralized team is 61 percent of respondents.

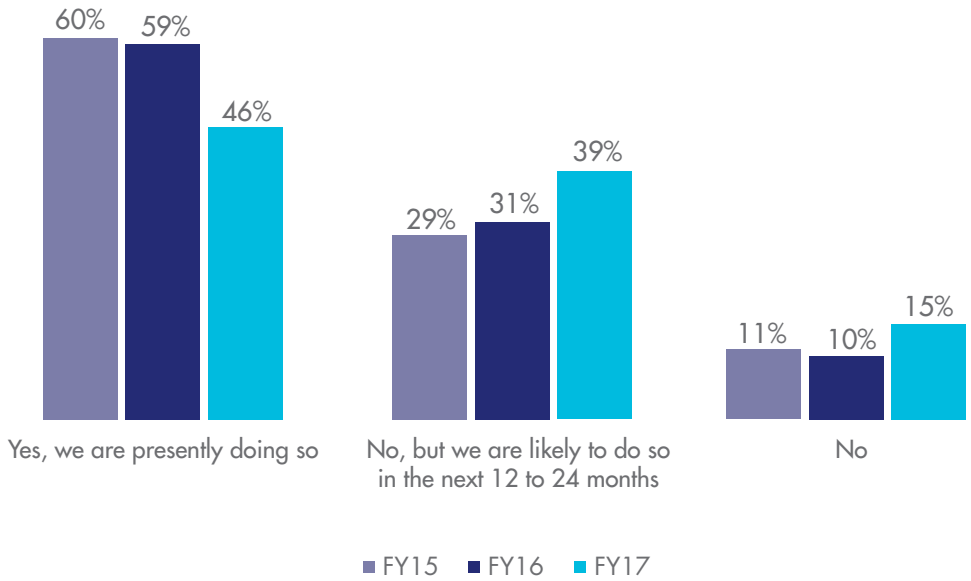
Figure 14. Which statement best describes how your organization uses HSMs?



Cloud encryption

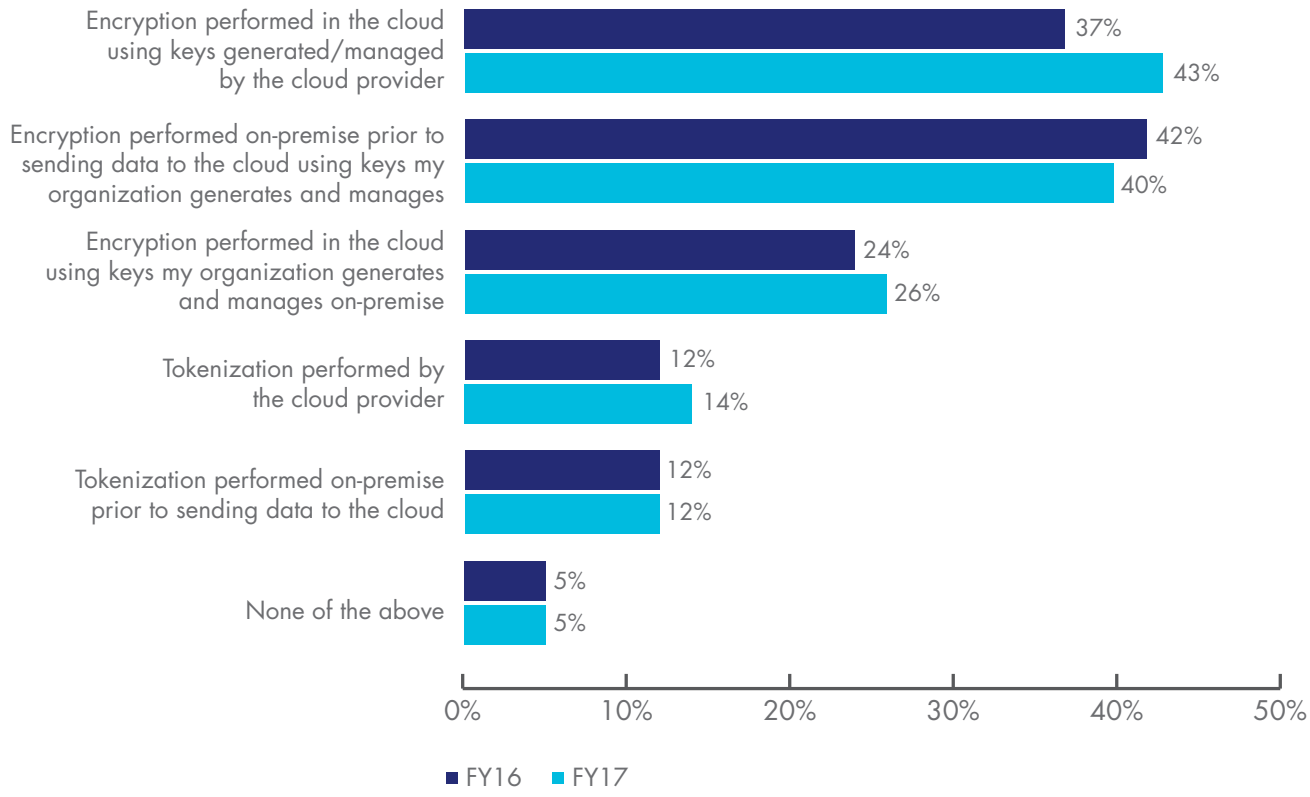
Most organizations transfer sensitive or confidential data to the cloud. As shown in Figure 15, 46 percent of respondents say their organizations currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism) and 39 percent of respondents plan to in the next 12 to 24 months. Thirty-seven percent of respondents say it is the cloud provider who is most responsible for protecting sensitive or confidential data transferred to the cloud.

Figure 15. Do you currently transfer sensitive or confidential data to the cloud?



How is data at rest in the cloud protected? As shown in Figure 16, 43 percent of respondents say encryption is performed in the cloud using keys generated/managed by the cloud provider and 40 percent say encryption is performed on-premises prior to sending data to the cloud using keys their organization generates and manages.

Figure 16. How does your organization protect data at rest in the cloud?



"43 PERCENT OF RESPONDENTS SAY ENCRYPTION IS PERFORMED IN THE CLOUD USING KEYS GENERATED/MANAGED BY THE CLOUD PROVIDER AND 40 PERCENT SAY ENCRYPTION IS PERFORMED ON-PREMISES PRIOR TO SENDING DATA TO THE CLOUD USING KEYS THEIR ORGANIZATION GENERATES AND MANAGES."

APPENDIX 1. METHODS & LIMITATIONS

Table 1 reports the sample response for Brazil. The sample response for this study was conducted over a 49-day period ending in January 2018. Our sampling frame of practitioners in Brazil consisted of 13,200 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 563 returns of which 56 were rejected for reliability issues. Our final sample for Brazil was 507, thus resulting in an overall 3.8% response rate.

Table 1. Sample response	Frequency	Pct%
Total sampling frame	13,200	100%
Total returns	563	4.2%
Rejected or screened surveys	56	0.4%
Final sample	507	3.8%

Figure 17 summarizes the approximate position levels of respondents in our study. As can be seen, more than half of the respondents (64 percent) are at or above the supervisory level.

Figure 17. Distribution of respondents according to position level

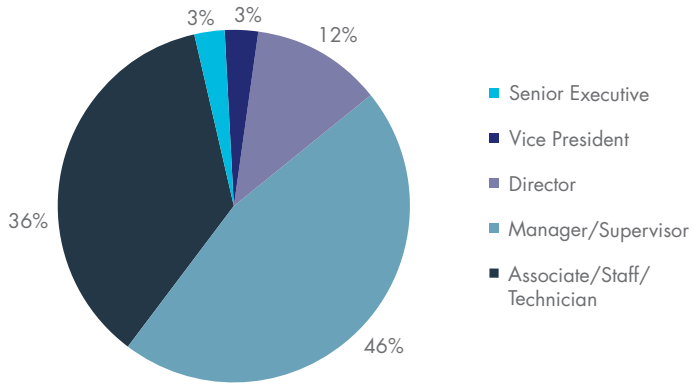


Figure 18 reports the respondents' functional area. As shown, 59 percent of respondents are located in IT operations, 16 percent are in security and 14 percent of respondents are in lines of business.

Figure 18. Distribution of respondents according to functional area

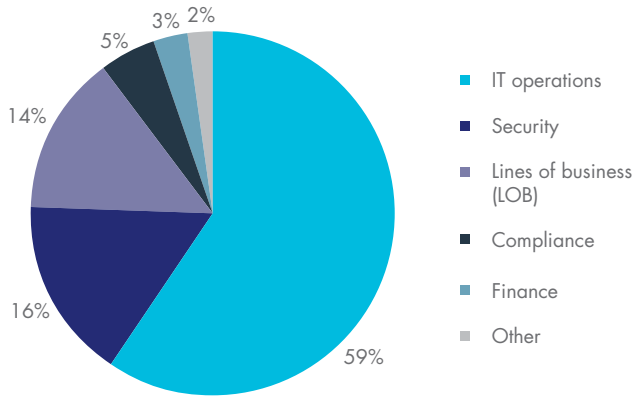
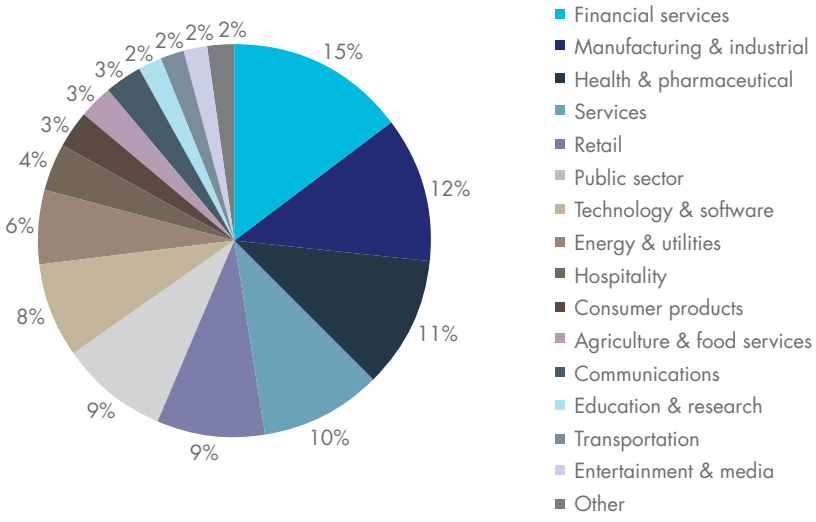


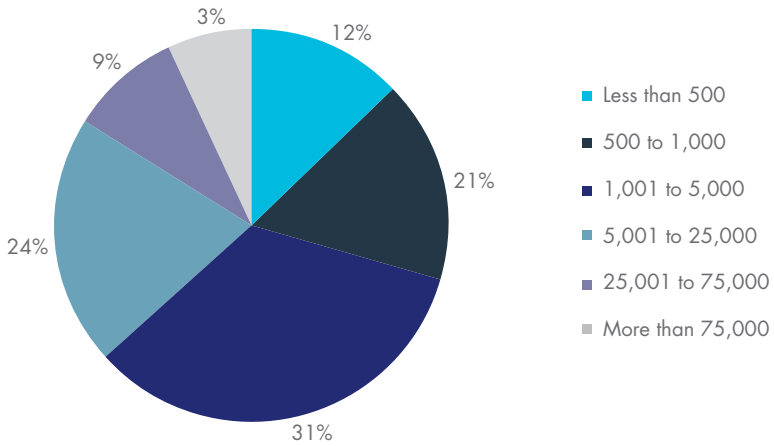
Figure 19 reports the respondents' organizations primary industry segments. As shown, 15 percent of respondents are located in financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Twelve percent of respondents are located in manufacturing and industrial, 11 percent of respondents are located in health and pharmaceuticals and 10 percent of respondents are in the services industry.

Figure 19. Distribution of respondents according to primary industry classification



According to Figure 20, more than half (67 percent) of respondents are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Figure 20. Distribution of respondents according to organizational headcount



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 Brazil, 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 from Brazil.

- **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.

APPENDIX 2. SURVEY DATA TABLES

The following tables provide the results for the Brazil country sample.

Survey response	BZ
Sampling frame	13,200
Total returns	563
Rejected or screened surveys	56
Final sample	507
Response rate	3.8%
Sample weights	10%

Part 1. Encryption Posture

Q1. Please select one statement that best describes your organization's approach to encryption implementation across the enterprise.	BZ
We have an overall encryption plan or strategy that is applied consistently across the entire enterprise	35%
We have a limited encryption plan or strategy that is applied to certain applications and data types	43%
We don't have an encryption plan or strategy	22%
Total	100%

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.

Q2a-1 Backup and archives	BZ
Extensively deployed	31%
Partially deployed	52%
Not deployed	17%
Total	100%

Q2b-1. Big data repositories	BZ
Extensively deployed	25%
Partially deployed	32%
Not deployed	43%
Total	100%

Q2c-1 Cloud gateway	BZ
Extensively deployed	31%
Partially deployed	35%
Not deployed	34%
Total	100%

Q2d-1. Data center storage	BZ
Extensively deployed	37%
Partially deployed	32%
Not deployed	31%
Total	100%

Q2e-1. Databases	BZ
Extensively deployed	45%
Partially deployed	33%
Not deployed	22%
Total	100%

Q2f-1. Docker containers	BZ
Extensively deployed	13%
Partially deployed	40%
Not deployed	47%
Total	100%

Q2g-1. Email	BZ
Extensively deployed	26%
Partially deployed	45%
Not deployed	29%
Total	100%

Q2h-1. Public cloud services	BZ
Extensively deployed	37%
Partially deployed	38%
Not deployed	25%
Total	100%

Q2i-1. File systems	BZ
Extensively deployed	32%
Partially deployed	39%
Not deployed	29%
Total	100%

Q2j-1. Internet communications (e.g., SSL)	BZ
Extensively deployed	51%
Partially deployed	35%
Not deployed	14%
Total	100%

Q2k-1. Internal networks (e.g., VPN/LPN)	BZ
Extensively deployed	42%
Partially deployed	42%
Not deployed	16%
Total	100%

Q2l-1. Laptop hard drives	BZ
Extensively deployed	41%
Partially deployed	36%
Not deployed	23%
Total	100%

Q2m-1 Private cloud infrastructure	BZ
Extensively deployed	30%
Partially deployed	38%
Not deployed	32%
Total	100%

Q2n-1 Internet of things (IoT) devices	BZ
Extensively deployed	18%
Partially deployed	23%
Not deployed	59%
Total	100%

Q2o-1 Internet of things (IoT) platforms	BZ
Extensively deployed	18%
Partially deployed	24%
Not deployed	58%
Total	100%

Q3. Who is most influential in directing your organization's encryption strategy? Please select one best choice.	BZ
IT operations	33%
Security	14%
Compliance	0%
Lines of business (LOB) or general management	25%
No single function has responsibility	28%
Total	100%

Q4. What are the reasons why your organization encrypts sensitive and confidential data? Please select the top three reasons.	BZ
To protect enterprise intellectual property	57%
To protect customer personal information	61%
To limit liability from breaches or inadvertent disclosure	26%
To avoid public disclosure after a data breach occurs	8%
To protect information against specific, identified threats	59%
To comply with internal policies	17%
To comply with external privacy or data security regulations and requirement	42%
To reduce the scope of compliance audits	29%
Total	300%

Q5. What are the biggest challenges in planning and executing a data encryption strategy? Please select the top two reasons.	BZ
Discovering where sensitive data resides in the organization	47%
Classifying which data to encrypt	50%
Determining which encryption technologies are most effective	15%
Initially deploying the encryption technology	52%
Ongoing management of encryption and keys	28%
Training users to use encryption appropriately	7%
Total	200%

Q6. How important are the following features associated with encryption solutions that may be used by your organization? Very important and important response combined.	**BZ**
Enforcement of policy	76%
Management of keys	69%
Support for multiple applications or environments	52%
Separation of duties and role-based controls	48%
System scalability	50%
Tamper resistance by dedicated hardware (e.g., HSM)	41%
Integration with other security tools (e.g., SIEM and ID management)	61%
Support for regional segregation (e.g., data residency)	41%
System performance and Latency	87%
Support for emerging algorithms (e.g., ECC)	72%
Support for cloud and on-premise deployment	60%
Formal product security certifications (e.g., FIPS 140)	49%

Q7. What types of data does your organization encrypt? Please select all that apply.	**BZ**
Customer information	25%
Non-financial business information	23%
Intellectual property	44%
Financial records	60%
Employee/HR data	37%
Payment related data	55%
Healthcare information	16%

Q8. What are the main threats that might result in the exposure of sensitive or confidential data? Please select the top two choices.	**BZ**
Hackers	24%
Malicious insiders	30%
System or process malfunction	25%
Employee mistakes	43%
Temporary or contract workers	23%
Third party service providers	16%
Lawful data request (e.g. by police)	6%
Government eavesdropping	33%
Total	200%

Part 2. Key Management

Q9. Please rate the overall "pain" associated with managing keys or certificates within your organization, where 1 = minimal impact to 10 = severe impact?	**BZ**
1 or 2	8%
3 or 4	7%
5 or 6	27%
7 or 8	24%
9 or 10	35%
Total	100%

Q10. What makes the management of keys so painful? Please select the top three reasons.	**BZ**
No clear ownership	59%
Insufficient resources (time/money)	26%
Lack of skilled personnel	71%
No clear understanding of requirements	17%
Key management tools are inadequate	49%
Systems are isolated and fragmented	51%
Technology and standards are immature	12%
Manual processes are prone to errors and unreliable	14%
Total	300%

Q11. 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.	**BZ**
Encryption keys for backups and storage	34%
Encryption keys for archived data	34%
Keys associated with SSL/TLS	36%
SSH keys	43%
End user encryption keys (e.g., email, full disk encryption)	35%
Signing keys (e.g., code signing, digital signatures)	57%
Payments-related keys (e.g., ATM, POS, etc.)	36%
Keys to embed into devices (e.g. at the time of manufacture in device production environments, or for IoT devices you use)	19%
Keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys	63%

Q12a. What key management systems does your organization presently use?	BZ
Formal key management policy (KMP)	53%
Formal key management infrastructure (KMI)	30%
Manual process (e.g., spreadsheet, paper-based)	77%
Central key management system/server	26%
Hardware security modules	15%
Removable media (e.g., thumb drive, CDROM)	37%
Software-based key stores and wallets	14%
Smart cards	25%
Total	276%

Q12b. What key management systems does your organization presently not used or not aware of use?	BZ
Formal key management policy (KMP)	36%
Formal key management infrastructure (KMI)	40%
Manual process (e.g., spreadsheet, paper-based)	15%
Central key management system/server	43%
Hardware security modules	63%
Removable media (e.g., thumb drive, CDROM)	53%
Software-based key stores and wallets	59%
Smart cards	46%
Total	355%

Part 3. Hardware Security Modules

Q13. What best describes your level of knowledge about HSMs?	BZ
Very knowledgeable	29%
Knowledgeable	20%
Somewhat knowledgeable	25%
No knowledge (skip to Q17a)	26%
Total	100%

Q14a. Does your organization use HSMs?	BZ
Yes	34%
No (skip to Q17a)	66%
Total	100%

Q14b. For what purpose does your organization presently deploy or plan to use HSMs? Please select all that apply.

Q14b-1. HSMs used today	BZ
Application level encryption	34%
Database encryption	29%
Big data encryption	6%
Public cloud encryption including for Bring Your Own Key (BYOK)	25%
Private cloud encryption	20%
SSL/TLS	56%
PKI or credential management	18%
Internet of Things (IoT) root of trust	8%
Document signing (e.g. electronic invoicing)	7%
Code signing	5%
Payment transaction processing including P2PE	37%
Payment credential issuing (e.g., mobile, EMV)	24%
Payment credential provisioning (e.g., mobile, IoT)	22%
Payment service provider interface (e.g., TSP, real-time payments, Open API	26%
With Cloud Access Security Brokers (CASBs) for encryption key management	10%
Blockchain applications (e.g., cryptocurrency, financial transfer)	10%
None of the above	14%
Other	3%
Total	354%

Q14b-2. HSMs planned to be deployed in the next 12 months	BZ
Application level encryption	50%
Database encryption	36%
Big data encryption	8%
Public cloud encryption including for Bring Your Own Key (BYOK)	16%
Private cloud encryption	25%
SSL/TLS	80%
PKI or credential management	25%
Internet of Things (IoT) root of trust	10%
Document signing (e.g. electronic invoicing)	8%
Code signing	5%
Payment transaction processing	47%
Payment credential issuing (e.g., mobile, EMV)	27%
Payment credential provisioning (e.g., mobile, IoT)	38%
Payment service provider interface (e.g., TSP, real-time payments, Open API	35%
With Cloud Access Security Brokers (CASBs) for encryption key management	15%
Blockchain applications (e.g., cryptocurrency, financial transfer)	11%
None of the above	16%
Other	1%
Total	453%

Q14c-1. If you use HSMs in conjunction with public cloud based applications, what models do you use today? Please select all that apply.	BZ
Rent/use HSMs from public cloud provider, hosted in the cloud	46%
Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications	46%
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	15%
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)	9%
None of the above	0%
Total	116%

Q14c-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.	**BZ**
Rent/use HSMs from public cloud provider, hosted in the cloud	41%
Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications	52%
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	21%
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)	25%
None of the above	0%
Total	139%

Q15. In your opinion, how important are HSMs to your encryption or key management strategy? Very important and important response combined	**BZ**
Q15a. Importance today	44%
Q15b. Importance in the next 12 months	51%

Q16. Which statement best describes how your organization uses HSMs?	**BZ**
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).	55%
Each individual application owner/team is responsible for their own cryptographic services (including HSMs) (i.e. traditional siloed, application-specific data center deployment).	45%
Total	100%

Part 4. Budget Questions

Q17a. Are you responsible for managing all or part of your organization's IT budget this year?	BZ
Yes	52%
No (skip to Q18)	48%
Total	100%

Q17b. Approximately, what percentage of the 2018 IT budget will go to IT security activities?	BZ
	9.7%

Q17c. Approximately, what percentage of the 2018 IT security budget will go to encryption activities?	BZ
	8.9%

Part 6: Cloud encryption: When responding to the following questions, please assume they refer only to public cloud services

Q35a. Does your organization currently use cloud computing services for any class of data or application – both sensitive and non-sensitive?	BZ
Yes, we are presently doing so	54%
No, but we are likely to do so in the next 12 to 24 months	25%
No (Go to Part 7 if you do not use cloud services for any class of data or application)	21%
Total	100%

Q35b. Do you currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism)?	BZ
Yes, we are presently doing so	46%
No, but we are likely to do so in the next 12 to 24 months	39%
No (Go to Part 7 if you do not use or plan to use any cloud services for sensitive or confidential data)	15%
Total	100%

Q35c. In your opinion, who is most responsible for protecting sensitive or confidential data transferred to the cloud?	BZ
The cloud provider	37%
The cloud user	26%
Shared responsibility	37%
Total	100%

Q35d. How does your organization protect data at rest in the cloud?	BZ
Encryption performed in the cloud using keys generated/managed by the cloud provider	43%
Encryption performed in the cloud using keys my organization generates and manages on-premise	26%
Encryption performed on-premise prior to sending data to the cloud using keys my organization generates and manages	40%
Tokenization performed by the cloud provider	14%
Tokenization performed on-premise prior to sending data to the cloud	12%
None of the above	5%
Total	140%

Q35e. For encryption of data at rest in the cloud, my organization's strategy is to…	BZ
Only use keys controlled by my organization	34%
Only use keys controlled by the cloud provider	12%
Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by my organization	28%
Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by the cloud provider	27%
Total	100%

Q35f. How important are the following features associated with cloud encryption to your organization? Very important and Important response provided.	**BZ**
Bring Your Own Key (BYOK) management support	44%
Privileged user access control	46%
Granular access controls	53%
Audit logs identifying key usage	71%
Audit logs identifying data access attempts	41%
SIEM integration, visualization and analysis of logs	57%
Support for FIPS 140-2 compliant key management	30%
Support for the KMIP standard for key management	70%
Ability to encrypt and rekey data while in use without downtime	36%
Average	50%

Q35g-1. How many public cloud providers does your organization in use today?	**BZ**
1	55%
2	21%
3	9%
4 or more	15%
Total	100%

Q35g-2. How many public cloud providers does your organization plan to use in the next 12 to 24 months?	**BZ**
1	44%
2	21%
3	10%
4 or more	25%
Total	100%

Part 7: Role and organizational characteristics

D1. What organizational level best describes your current position?	BZ
Senior Executive	3%
Vice President	3%
Director	12%
Manager/Supervisor	46%
Associate/Staff/Technician	36%
Other	0%
Total	100%

D2. Select the functional area that best describes your organizational location.	BZ
IT operations	59%
Security	16%
Compliance	5%
Finance	3%
Lines of business (LOB)	14%
Other	2%
Total	100%

D3. What industry best describes your organization's industry focus?	BZ
Agriculture & food services	3%
Communications	3%
Consumer products	3%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	2%
Financial services	15%
Health & pharmaceutical	11%
Hospitality	4%
Manufacturing & industrial	12%
Public sector	9%
Retail	9%
Services	10%
Technology & software	8%
Transportation	2%
Other	1%
Total	100%

D4. What is the worldwide headcount of your organization?	BZ
Less than 500	12%
500 to 1,000	21%
1,001 to 5,000	31%
5,001 to 25,000	24%
25,001 to 75,000	9%
More than 75,000	3%
Total	100%

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 Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and, with the internet of things (IoT), even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property, and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged-user control and high-assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

About Thales

The people we all rely on to make the world go round – they rely on Thales. Our customers come to us with big ambitions: to make life better, to keep us safer. Combining a unique diversity of expertise, talents and cultures, our architects design and deliver extraordinary high technology solutions. Solutions that make tomorrow possible, today. From the bottom of the oceans to the depth of space and cyberspace, we help our customers think smarter and act faster – mastering ever greater complexity and every decisive moment along the way. With 65,000 employees in 56 countries, Thales reported sales of €15.8 billion in 2017.

Platinum partner – Geobridge

Established in 1997, GEOBRIDGE emerged as one of the first information security solutions providers to support cryptography and payment applications for payment processors, financial institutions and retail organizations. Today, GEOBRIDGE is a leading information security solutions and compliance provider that provides Cryptography and Key Management, Payment Security, Compliance, and HSM Virtualization solutions and services to our clients. Our client list includes Fortune 500 companies, financial institutions, healthcare organizations and government clients across North America and around the globe. GEOBRIDGE leverages our team's expertise in data protection, program development, enforcement and governance to help architect solutions to help mitigate risk for our clients.

Platinum partner – Venafi

Venafi is the cyber security market leader in machine identity protection, securing machine-to-machine connections and communications. Venafi protects machine identity types by orchestrating cryptographic keys and digital certificates for SSL/TLS, IoT, mobile and SSH. Venafi provides global visibility of machine identities and the risks associated with them for the extended enterprise – on premises, mobile, virtual, cloud and IoT – at machine speed and scale. Venafi puts this intelligence into action with automated remediation that reduces the security and availability risks connected with weak or compromised machine identities while safeguarding the flow of information to trusted machines and preventing communication with machines that are not trusted.

With 31 patents currently in its portfolio, Venafi delivers innovative solutions for the world's most demanding, security-conscious Global 2000 organizations. Venafi is backed by top-tier investors, including Foundation Capital, Intel Capital, Origin Partners, Pelion Venture Partners, QuestMark Partners, Mercato Partners and NextEquity. For more information, visit: www.venafi.com.

THALES

www.thalesesecurity.com

©2018 Thales