Entrust Datacard®

NCIPHER
AN ENTRUST DATACARD COMPANY

2020
GLOBAL ENCRYPTION TRENDS STUDY

Ponemon INSTITUTE

Sponsored by nCipher Security
and Entrust Datacard

Independently conducted by
Ponemon Institute LLC

01 EXECUTIVE SUMMARY

PONEMON INSTITUTE PRESENTS THE FINDINGS OF THE 2020 GLOBAL ENCRYPTION TRENDS STUDY[1]

We surveyed 6,457 individuals across multiple industry sectors in 17 countries - Australia, Brazil, France, Germany, Hong Kong, India, Japan, Mexico, the Middle East (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates), Netherlands, the Russian Federation, Southeast Asia, South Korea, Sweden, Taiwan, the United Kingdom, and the United States.[2]

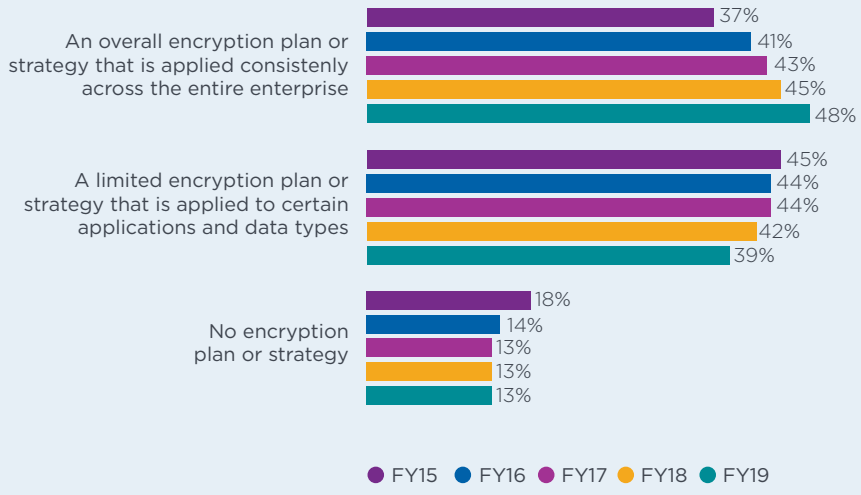
The purpose of this research is to examine how the use of encryption has evolved over the past 15 years and the impact of this technology on the security posture of organizations. The first encryption trends study was conducted in 2005 for a US sample of respondents.[3]

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, 48 percent of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise and 39 percent say they have a limited encryption plan or strategy that is applied to certain applications and data types, a slight decrease from last year.

Following are the findings from this year's research.

Figure 1. **Does your company have an encryption strategy?**
Country samples are consolidated



[1] This year's data collection was started in December 2019 and completed in January 2020. Throughout the report we present trend data based on the fiscal year the survey commenced rather than the year the report is finalized. Hence, we present the current findings as fiscal year 2019.

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

[3] The trend analysis shown in this study was performed on combined country samples spanning 15 years (since 2005).

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase. Since conducting this study 15 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, the United States, Sweden and Hong Kong. Respondents in the Russian Federation and Brazil report the lowest adoption of an enterprise encryption strategy. The global average of adoption is 48 percent.

The IT operations function is the most influential in framing the organization's encryption strategy over the past 14 years. However, in the United States, lines of business are more influential (30 percent of respondents). IT operations and IT security have a similar level of influence in the United States and Mexico.

TRENDS IN ADOPTION OF ENCRYPTION

The use of encryption increases in all industries. Results suggest a steady increase in all industry sectors, with the exception of healthcare and pharma. 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.

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.

The main driver for encryption is the protection of customer's personal information. Organizations are using encryption for protection of customers' personal information (54 percent of respondents), the protection of enterprise intellectual property (52 percent of respondents) and protection against specific, identified threats (51 percent of respondents).

A barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization. Sixty-seven percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. Forty-four percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-one percent cite classifying which data to encrypt as difficult.

> **48%** of respondents say their organizations have an overall encryption plan that is applied consistently across the entire enterprise.

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 deployed and correspond to mature use cases. For the third year, the study tracked the deployment of encryption of IoT devices and platforms/data repositories. Sixty percent of respondents say encryption is at least partially deployed for IoT devices, and 61 percent of respondents say encryption of IoT platforms/data repositories is at least partially deployed.

ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

Certain encryption features are considered more critical than others. According to the consolidated findings, system performance and latency, enforcement of policy and support for both cloud and on-premise deployment are the three most important encryption features.

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. The least likely data types to be encrypted are non-financial business information and health-related information, which is a surprising result given the sensitivity of health information.

Most companies plan to use blockchain. Sixty percent of respondents say their organizations will use blockchain. The two primary use cases are for cryptocurrency/wallets and asset transactions/management.

Newer encryption technologies are at least 5 years from mainstream adoption. Respondents were asked when they believe homomorphic encryption, multi-party computation, and quantum algorithms will achieve mainstream enterprise adoption. The solution expected to achieve adoption the soonest is multi-party computation.

ATTITUDES ABOUT KEY MANAGEMENT

How painful is key management? Sixty 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 67 percent occurs in Germany. At 38 percent, the lowest pain level occurs in France. No clear ownership and lack of skilled personnel are the primary reasons why key management is painful.

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

IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)

Germany, the United States and Middle East organizations are more likely to deploy HSMs. Germany, the United States and the Middle East are more likely to deploy HSMs than other countries. The overall average deployment rate for HSMs is 48 percent.

How HSMs in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months. Fifty percent of respondents say their organizations own and operate HSMs on-premise, accessed real-time by cloud-hosted applications and 39 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. In the next 12 months, both figures will increase. The use of HSMs with Cloud Access Security Brokers and the ownership and operation of HSMs for the purpose of generating and managing keys to send to the cloud for use by the cloud provider are expected to increase significantly.

The overall average importance rating for HSMs as part of an encryption and key management strategy in the current year is 64 percent. The pattern of responses suggests Australia, Germany and the United States 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? Fifty-nine 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-one 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 two top uses are application-level encryption and TLS/SSL, followed by public cloud encryption, including for BYOK (Bring Your Own Key). There is a significant increase forecast in the use of database encryption 12 months from now. It is significant to note that HSM use for application-level encryption will soon be deployed in 51 percent of the organizations represented in this study.

CLOUD ENCRYPTION

Fifty-eight 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 25 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-five percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 36 percent of respondents perform encryption in the cloud, with cloud provider generated/managed keys. Twenty percent of respondents are using some form of BYOK approach.

What are the top three cloud encryption features? The top three features are support for the KMIP standard for key management (67 percent of respondents), SIEM integration, visualization and analysis of logs (62 percent of respondents) and granular access controls (60 percent of respondents).

> Since conducting this study 15 years ago, there has been a steady increase in organizations with an encryption strategy applied consistently across the entire enterprise.

02 KEY FINDINGS

IN THIS SECTION, WE PROVIDE A DEEPER ANALYSIS OF THE KEY FINDINGS.

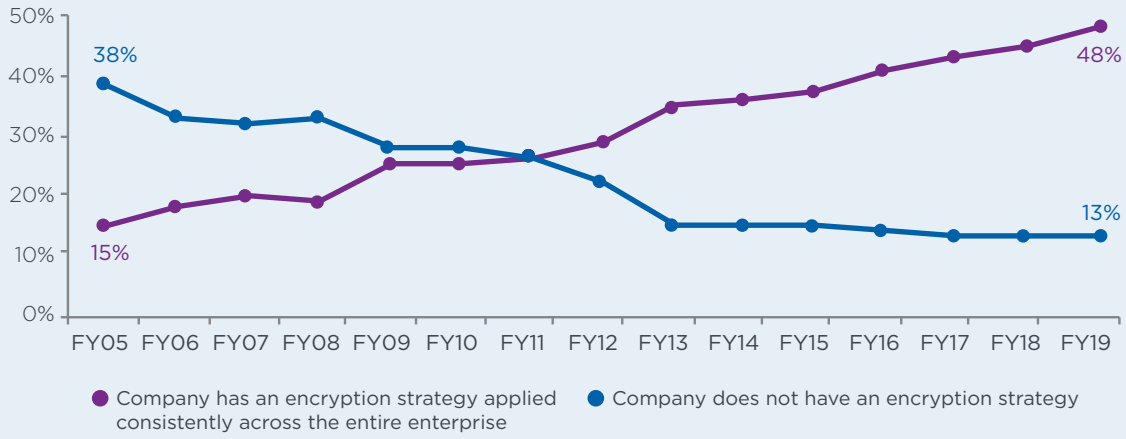
We have organized the report according to the following themes:

- 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]
- Cloud encryption

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase. Since conducting this study 15 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**
Country samples are consolidated



[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, the United States, Sweden and Hong Kong. Respondents in the Russian Federation and Brazil report the lowest adoption of an enterprise encryption strategy. The global average of adoption is 48 percent.

Figure 4 shows that the IT operations function is the most influential in framing the organization's encryption strategy since the research commenced.

However, in the United States, lines of business are more influential than IT operations. IT operations and IT security have a similar level of influence in the United States and Mexico.

A possible reason why the lines of business are more influential than IT security in many countries 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 3. **Differences in enterprise encryption strategies by country**

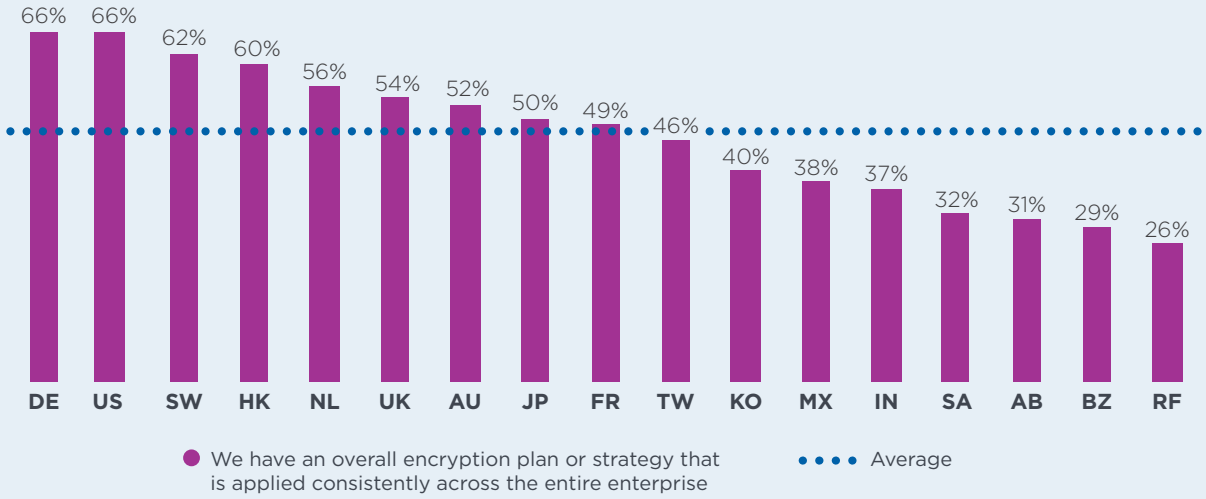
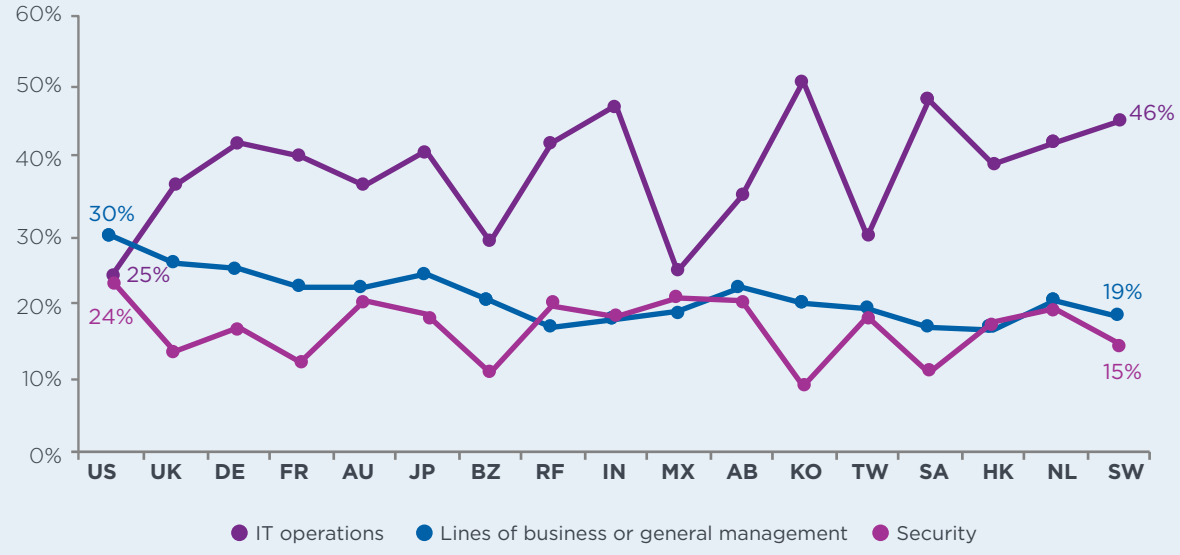


Figure 4. **Influence of IT operations, lines of business and security**
Country samples are consolidated



TRENDS IN ADOPTION OF ENCRYPTION

The use of encryption increases in most industries. Figure 5 shows the current year and the eight-year average in the use of encryption solutions for 10 industry sectors. Results suggest a steady increase in all industry sectors, with the exception of healthcare and pharmaceutical. 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.

Figure 5. **The extensive use of encryption by industry: Current year versus 8-year average**
Country samples are consolidated. Average of 15 encryption categories

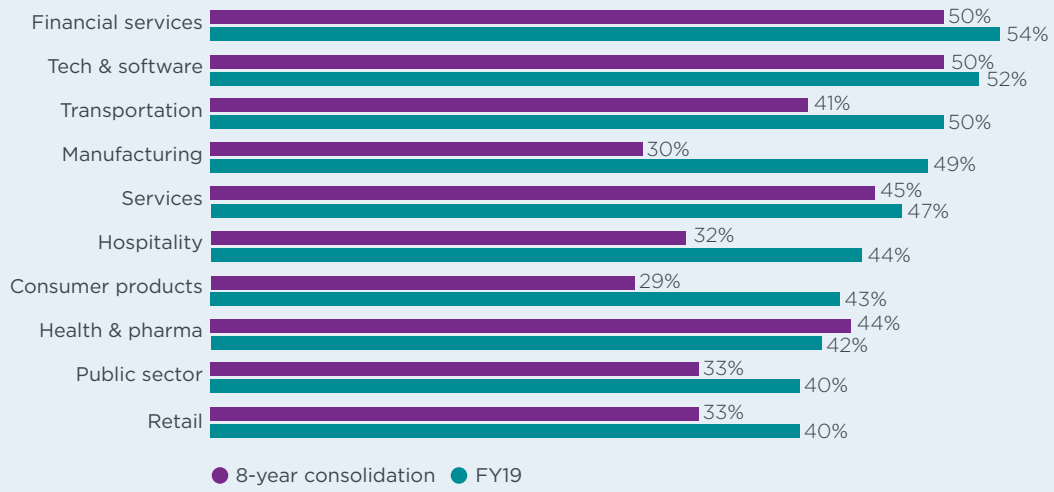
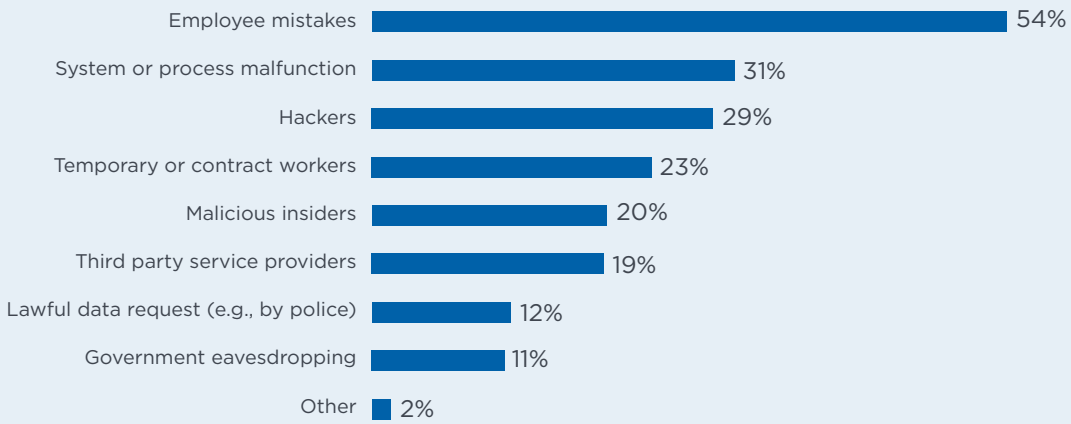


Figure 6. **The most salient threats to sensitive or confidential data**
Consolidated country samples. Two choices permitted



The main driver for encryption is protection of customers' personal information. 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 for protection of customer personal information followed by the protection of enterprise intellectual property and protection of information against specific, identified threats (54 percent, 52 percent and 51 percent of respondents, respectively).

This marks the third 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.

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 the organization's effective execution of its data encryption strategy in descending order of importance. Sixty-seven percent of respondents say discovering where sensitive data resides in the organization is the number one challenge. In addition, 44 percent of all respondents cite initially deploying encryption technology as a significant challenge. Thirty-one 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

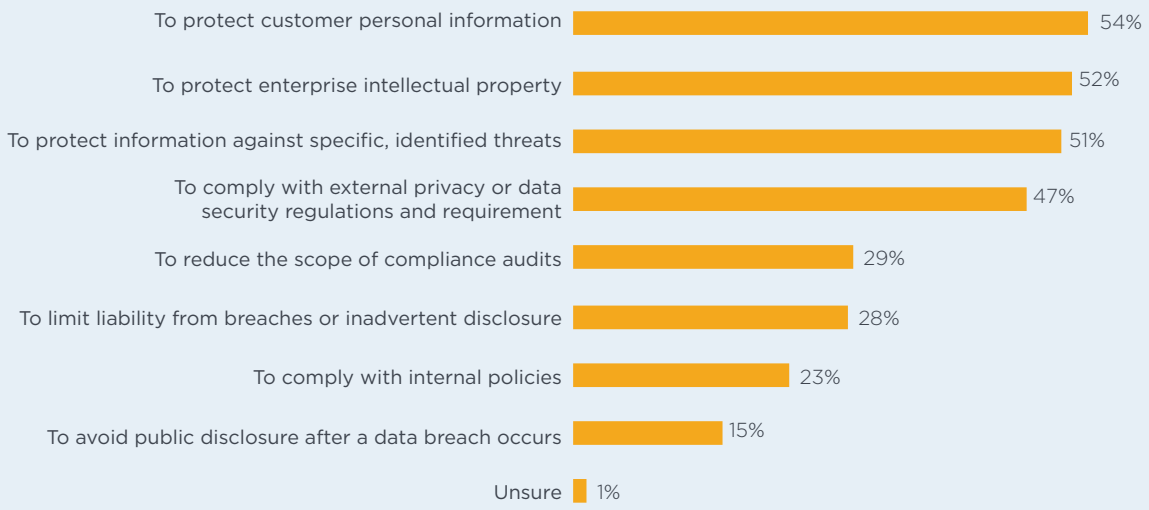
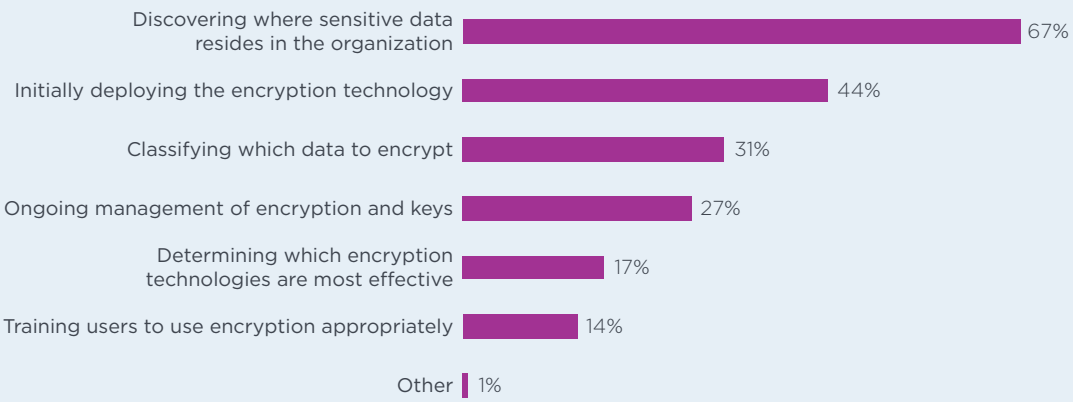


Figure 8. **Biggest challenges in planning and executing a data encryption strategy**
Country samples are consolidated. More than one choice permitted



DEPLOYMENT CHOICES

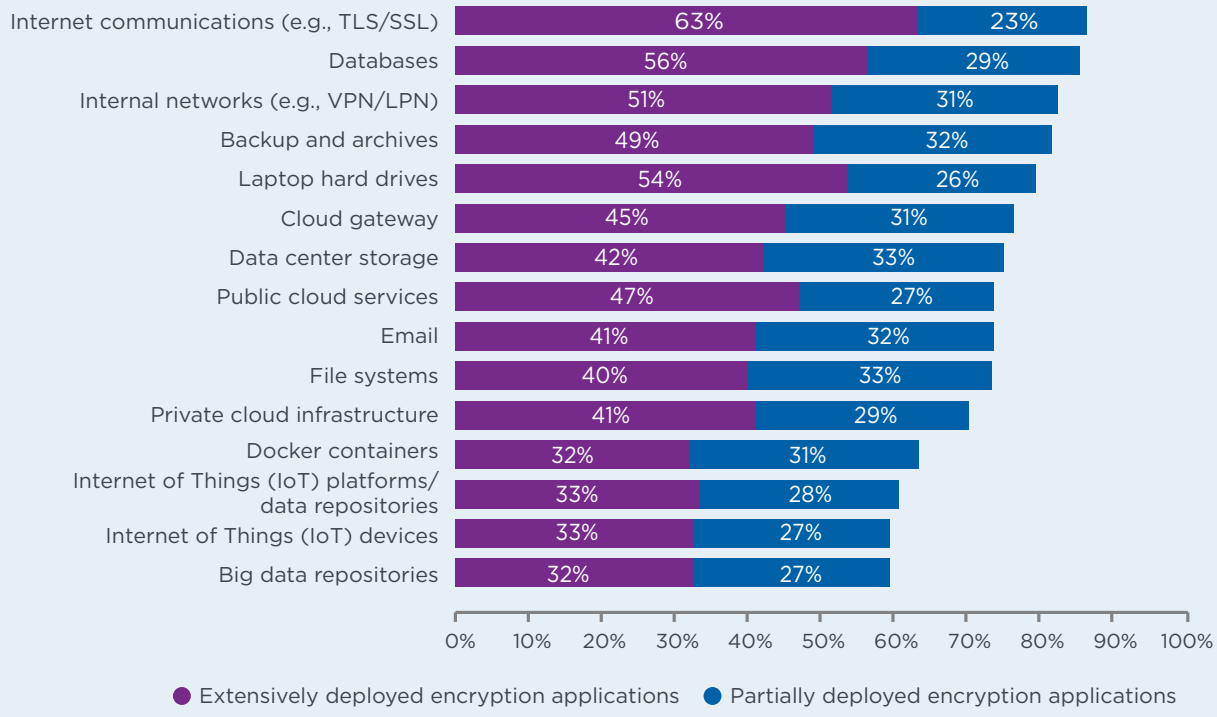
No single encryption technology dominates in organizations. We asked respondents to indicate if specific encryption technologies are widely or only partially deployed within their organizations. "Extensive deployment" means that the encryption technology is deployed enterprise-wide. "Partial deployment" means the encryption technology is confined or limited to a specific purpose (a.k.a. point solution).

As shown in Figure 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 third year, the study tracked the deployment of encryption of IoT devices and platforms/data repositories. As shown, 61 percent of respondents say encryption for IoT platforms/data repositories has been at least partially deployed, and 60 percent of respondents say encryption for IoT devices has been at least partially deployed.

> **#1** The number one barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization.

Figure 9. **Consolidated view on the use of 15 encryption technologies**
Country samples are consolidated

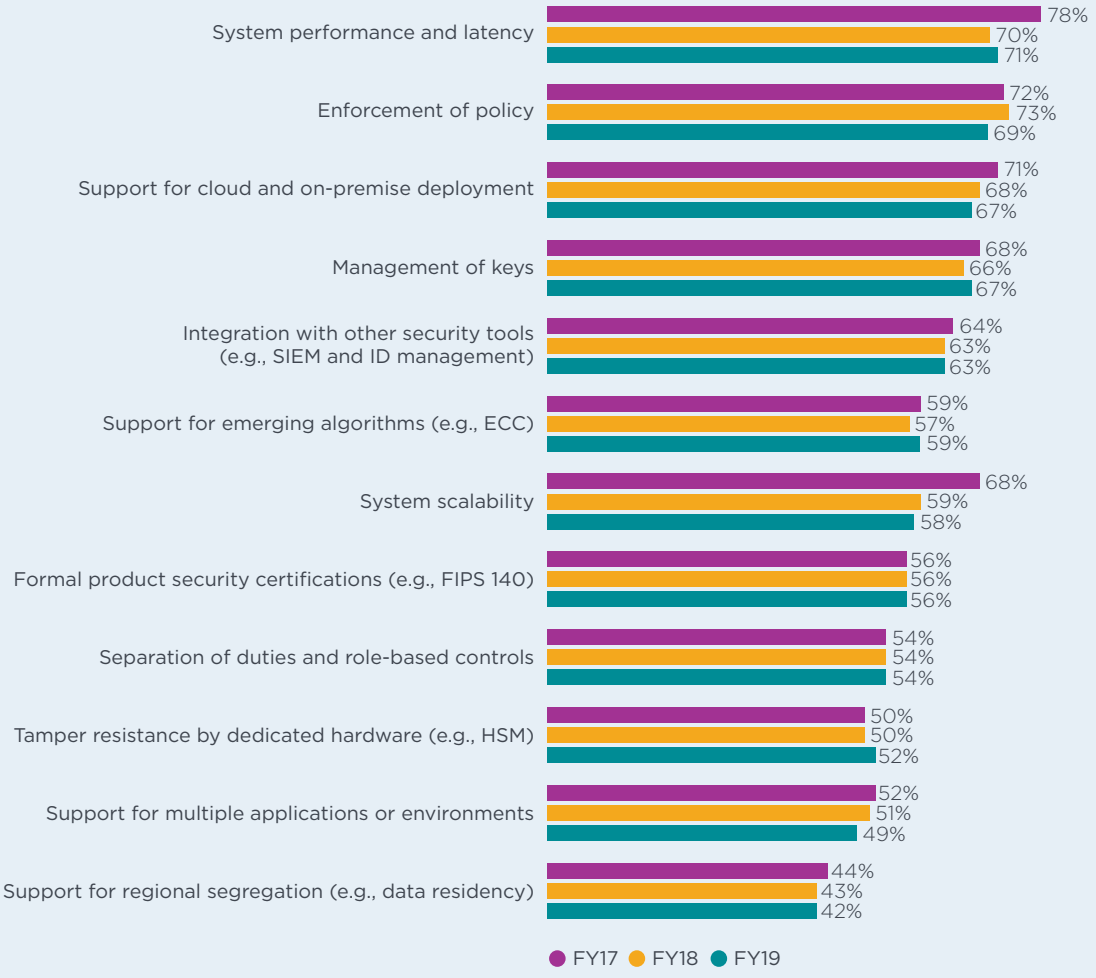


ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

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, system performance and latency, enforcement of policy 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.

Figure 10. **Most important features of encryption technology solutions**
Country samples are consolidated. Very important and Important responses combined



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 types to be encrypted are non-financial business information and health-related information, which is a surprising result given the sensitivity of health information and the recent high-profile healthcare data breaches.

Most companies plan to use blockchain. Sixty percent of respondents say their organizations will use blockchain. As shown in Figure 12, the two primary use cases are for cryptocurrency/wallets and asset transactions/management.

> "The least likely data types to be encrypted are non-financial business information and health-related information..."

Figure 11. **Data types routinely encrypted**
Country samples are consolidated. More than one choice permitted

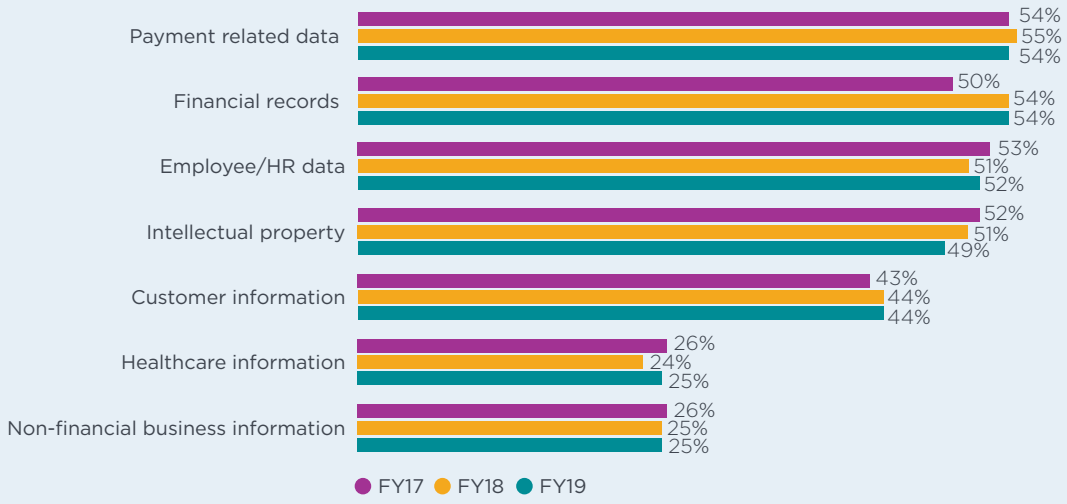
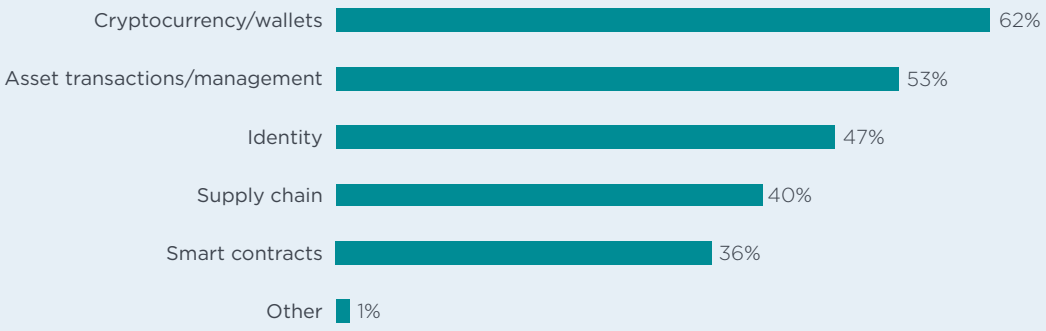


Figure 12. **What applications does your organization plan to use blockchain for?**
More than one response permitted



Respondents were asked when they think the solutions in Figure 13 will achieve mainstream enterprise adoption. The solution expected to achieve adoption the soonest is multi-party computation. Quantum algorithms will achieve adoption in eight years.

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 14 clearly shows that 60 (25+35) percent of respondents chose ratings at or above 7; thus, suggesting a fairly high pain threshold.

Figure 13. **When do you think the following solutions will achieve mainstream enterprise adoption?**
Extrapolated values in years

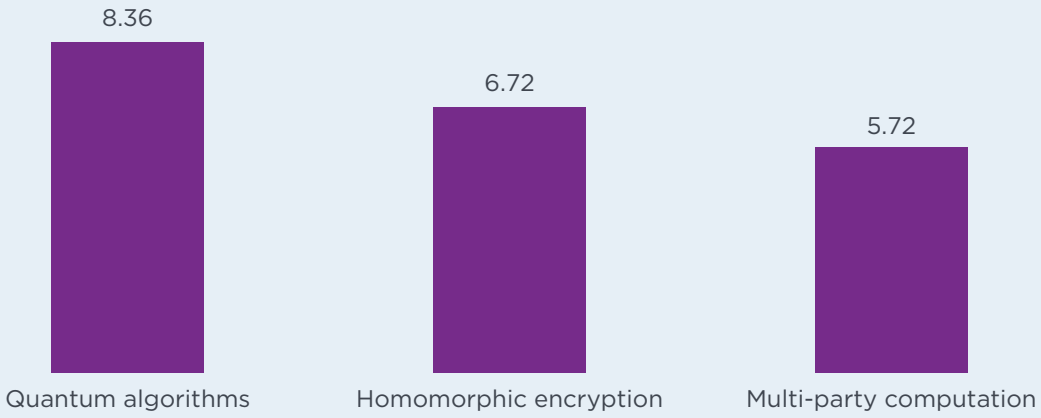


Figure 14. **Rating on the overall impact, risk and cost associated with managing keys**
Country samples are consolidated

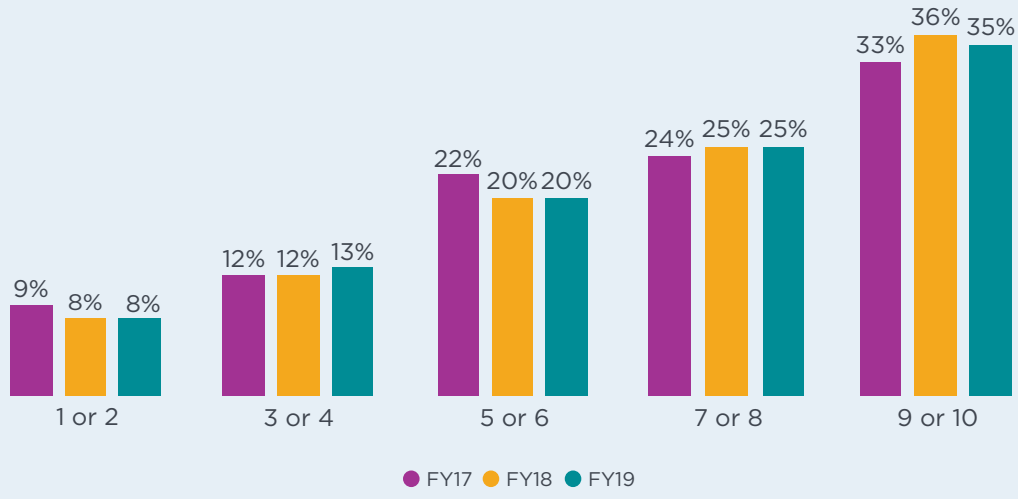


Figure 15 shows the 7+ ratings on a 10-point scale for each country. As can be seen, the average percentage in all country samples is 59 percent, which suggests respondents view managing keys as a very challenging activity. The highest percentage pain threshold of 67 percent occurs in Germany. At 38 percent, the lowest pain level occurs in France.

Why is key management painful? Figure 16 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.

Figure 15. **Percentage "pain threshold" by country**
Percentage 7 to 10 rating on a 10-point scale

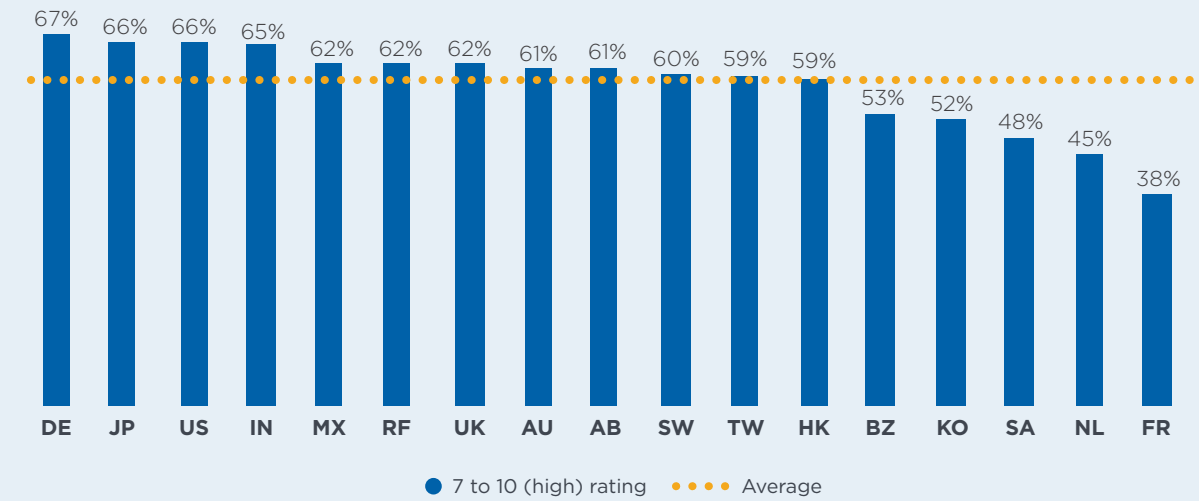
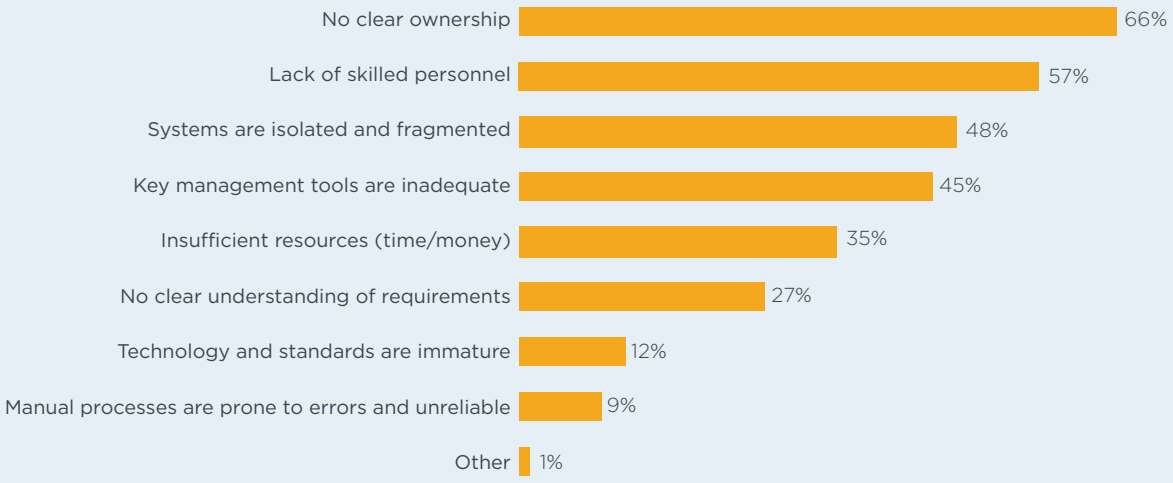


Figure 16. **What makes the management of keys so painful?**
Country samples are consolidated. Three responses permitted



Which keys are most difficult to manage? Moving into the top position on this list for the third year as the most difficult keys to manage, are keys for external cloud or hosted services. As shown in Figure 17, this is followed by SSH keys, signing keys, and end user encryption keys. 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 18, respondents' companies continue to use a variety of key management systems. The most commonly deployed systems include: (1) formal key management infrastructure (KMI), (2) formal key management policy (KMP), and (3) and manual processes.

Figure 17. **Types of keys most difficult to manage**
Country samples are consolidated. Very painful and painful responses combined

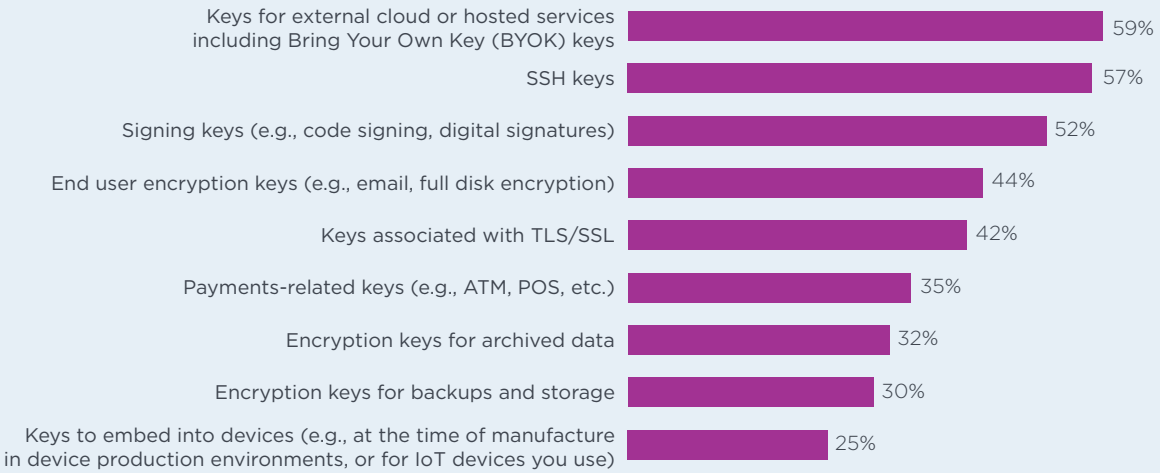
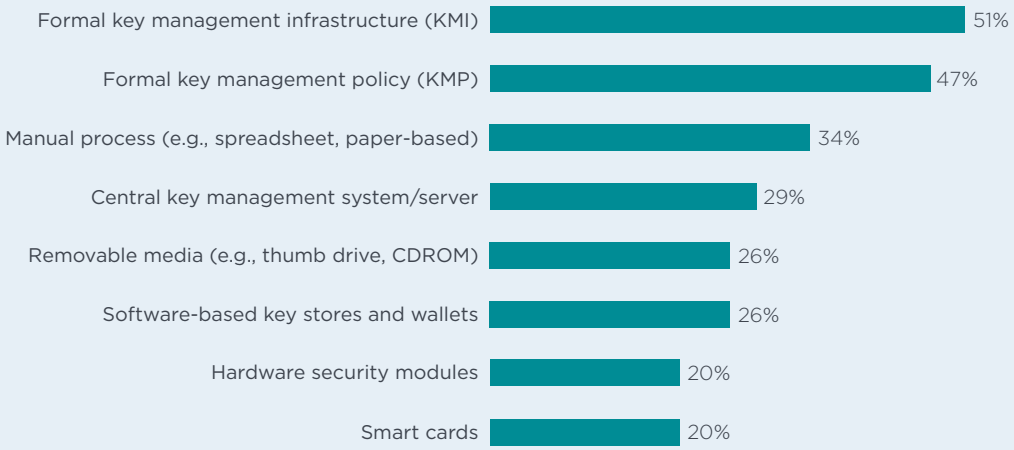


Figure 18. **What key management systems does your organization presently use?**
Country samples are consolidated. More than one choice permitted



IMPORTANCE OF HARDWARE SECURITY MODULES (HSMs)[5]

Germany, the United States and Middle East organizations are more likely to deploy HSMs. Figure 19 summarizes the percentage of respondents that deploy HSMs. Germany, the United States and the Middle East are more likely to deploy HSMs than other countries. The overall average deployment rate for HSMs is 48 percent.

Deployment of HSMs increases steadily. Figure 20 shows a eight-year trend for HSMs. As can be seen, the rate of global HSM deployment has steadily increased.

Figure 19. **Deployment of HSMs**

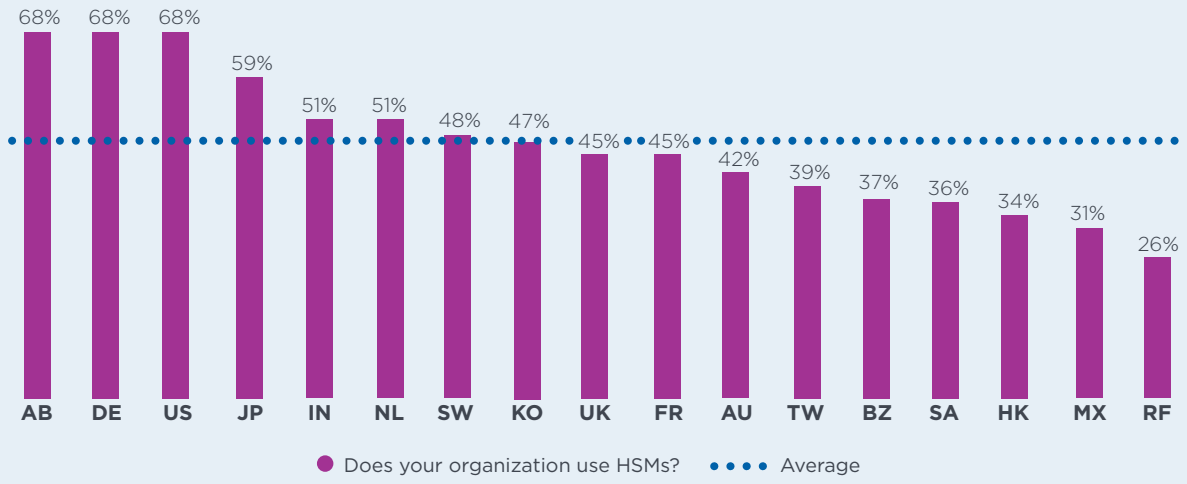
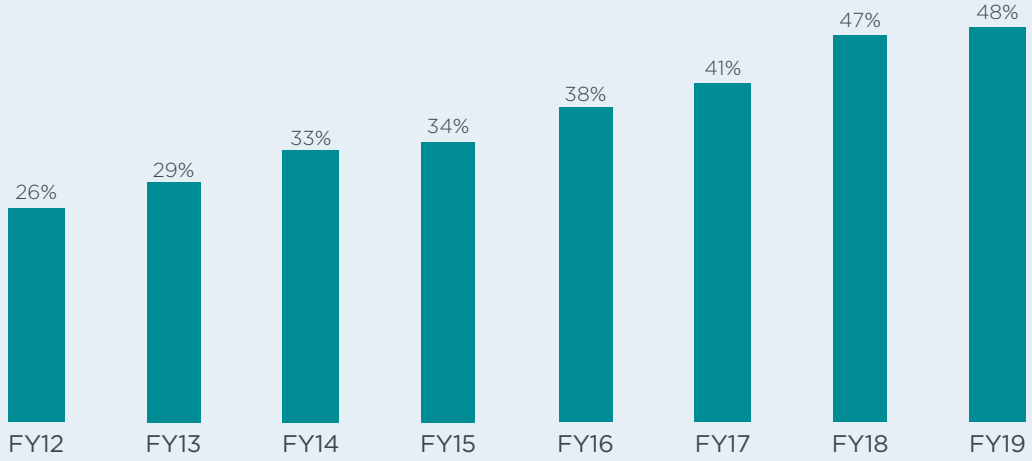


Figure 20. **HSM deployment rate over eight years**
Country samples are consolidated



[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 21, 50 percent of respondents own and operate HSMs on-premise for cloud-based applications, and 39 percent of respondents rent/use HSMs from a public cloud provider for the same purpose. In the next 12 months, respondents predict a significant increase in the ownership and operation of HSMs for the purpose of generating and managing BYOK keys to send to the cloud for use by the cloud provider, and the integration with a Cloud Access Security Broker to manage keys and cryptographic operations.

Figure 22 summarizes the percentage of respondents in 17 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 64 percent. The pattern of responses suggests Australia, Germany and the United States are most likely to assign importance to HSMs as part of their organization's encryption or key management activities.

Figure 21. **Use of HSMs in conjunction with public cloud-based applications today and in the next 12 months**
More than one choice permitted

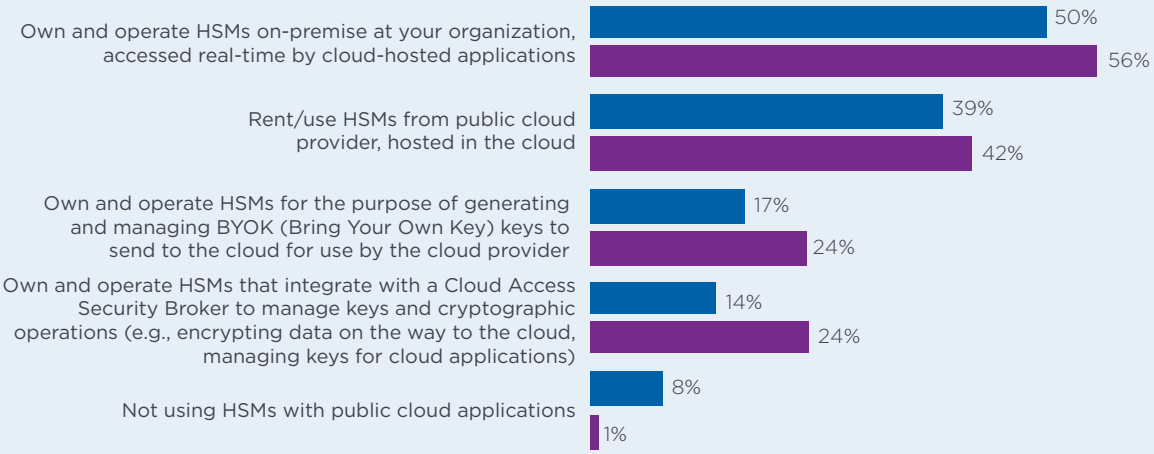


Figure 22. **Perceived importance of HSMs as part of encryption or key management**
Very important & important responses combined

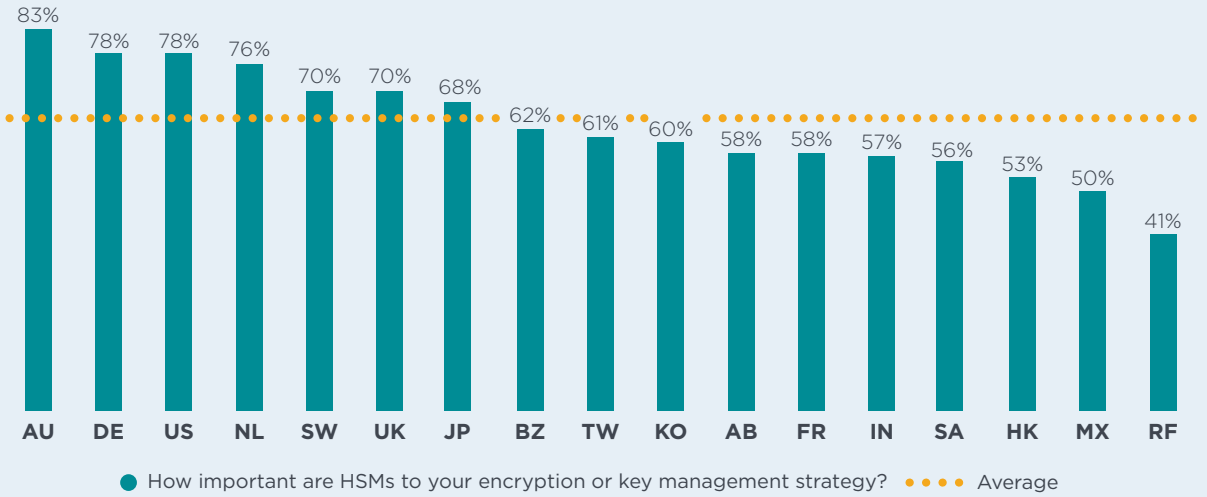


Figure 23 shows an eight-year trend in the importance of HSMs for encryption or key management, which has steadily increased over time.

What best describes an organization's use of HSMs? As shown in Figure 24, 59 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-one 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.

> The rate of global HSM deployment has steadily increased.

Figure 23. **Perceived importance of HSMs as part of encryption or key management over eight years**
Country samples are consolidated

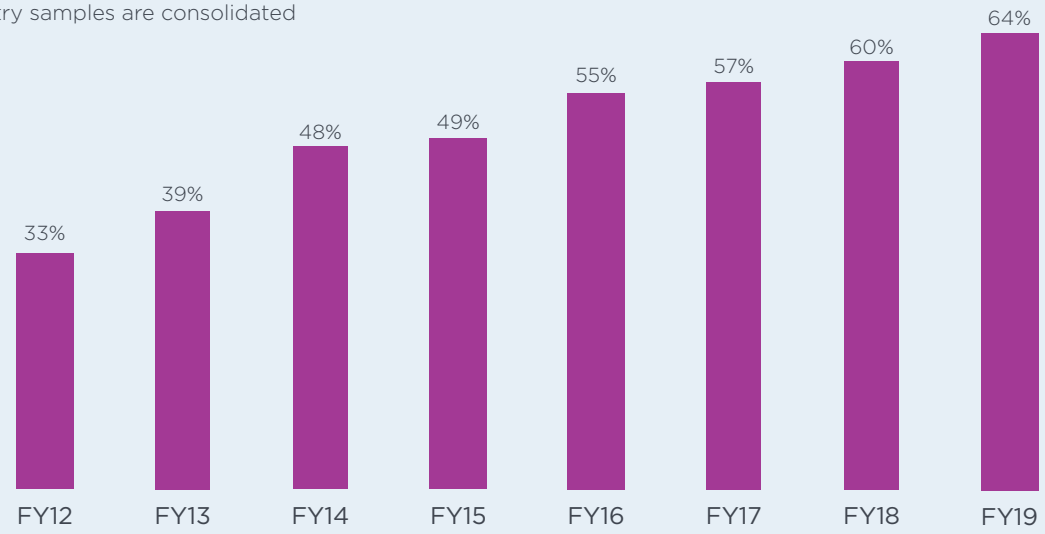
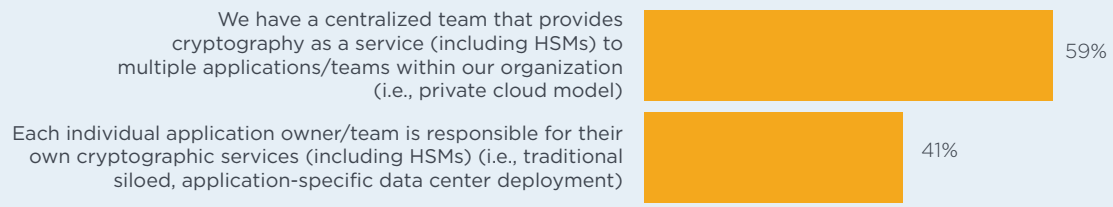


Figure 24. **Which statement best describes how your organization uses HSMs?**

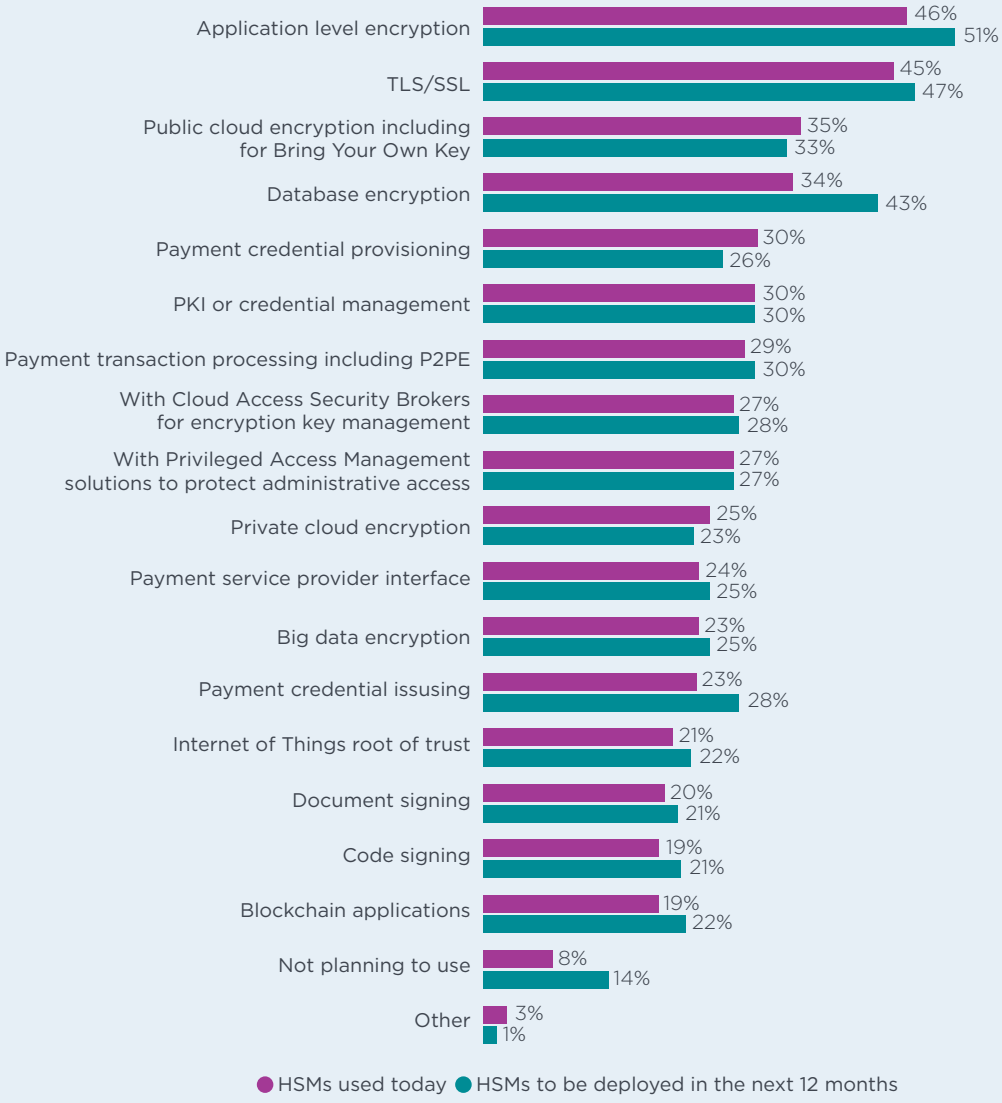


What are the primary purposes or uses for HSMs?
Figure 25 summarizes the primary purpose or use cases for deploying HSMs. As can be seen, the two top choices are application-level encryption, TLS/SSL, followed by public and cloud encryption including for BYOK and database encryption. This chart shows a significant increase in the use of database encryption 12 months from now.

It is significant to note that HSM use for application-level encryption will soon be deployed in 51 percent of the organizations represented in this study.

> **51%**
> HSM use for application-level encryption will soon be deployed in 51 percent of the organizations represented in this study.

Figure 25. **How HSMs are deployed or planned to be deployed in the next 12 months**
Country samples are consolidated. More than one choice permitted



CLOUD ENCRYPTION

According to Figure 26, 58 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 25 percent of respondents expect to do so in the next one to two years. These findings indicate that the benefits of cloud computing outweigh the risks associated with transferring sensitive or confidential data to the cloud.

According to Figure 27, with respect to the transfer of sensitive or confidential data to the cloud, the United States, Brazil, Germany, India and South Korea are more frequently transferring sensitive data to the cloud.

Figure 26. **Do you currently transfer sensitive or confidential data to the cloud?**
Country samples are consolidated

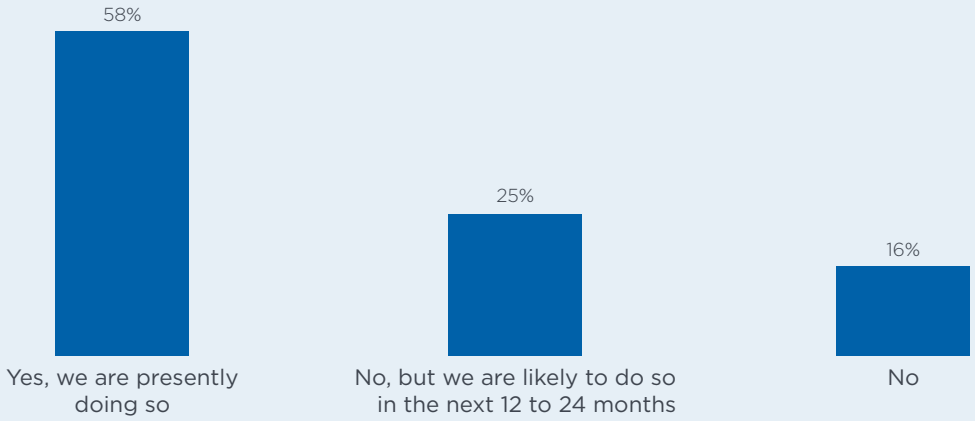
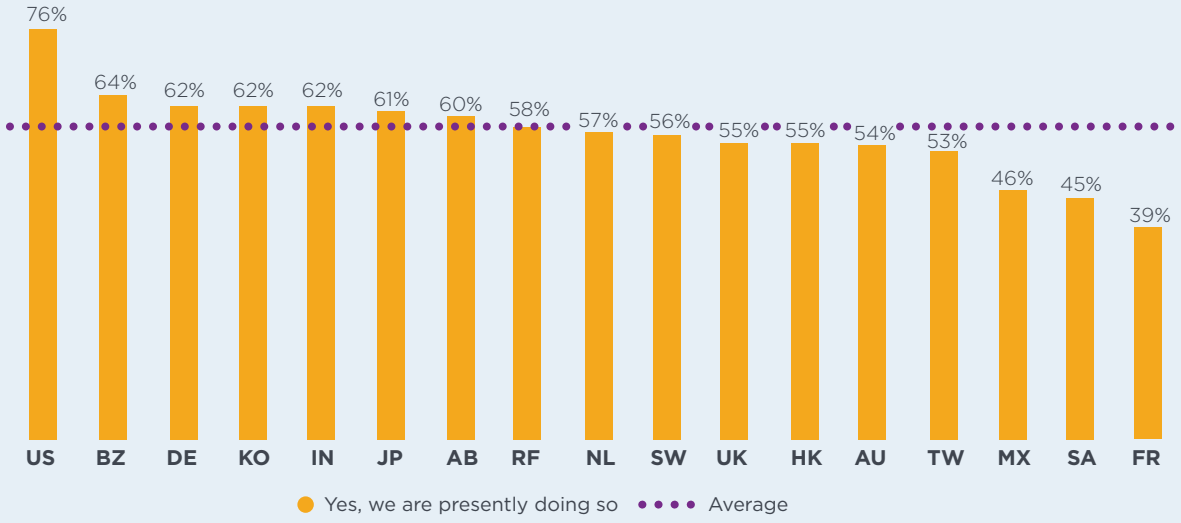


Figure 27. **Organizations that transfer sensitive or confidential data to the cloud by country**



How do organizations protect data at rest in the cloud? As shown in Figure 28, 45 percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 36 percent of respondents perform encryption in the cloud, with cloud provider generated/managed keys. Twenty percent of respondents are using some form of Bring Your Own Key (BYOK) approach.

What are the top three cloud encryption features? The top three features are support for the KMIP standard for key management (67 percent of respondents), SIEM integration, visualization and analysis of logs (62 percent of respondents) and granular access controls (60 percent of respondents), as shown in Figure 29.

Figure 28. **How does your organization protect data at rest in the cloud?**
Country samples are consolidated. More than one choice permitted

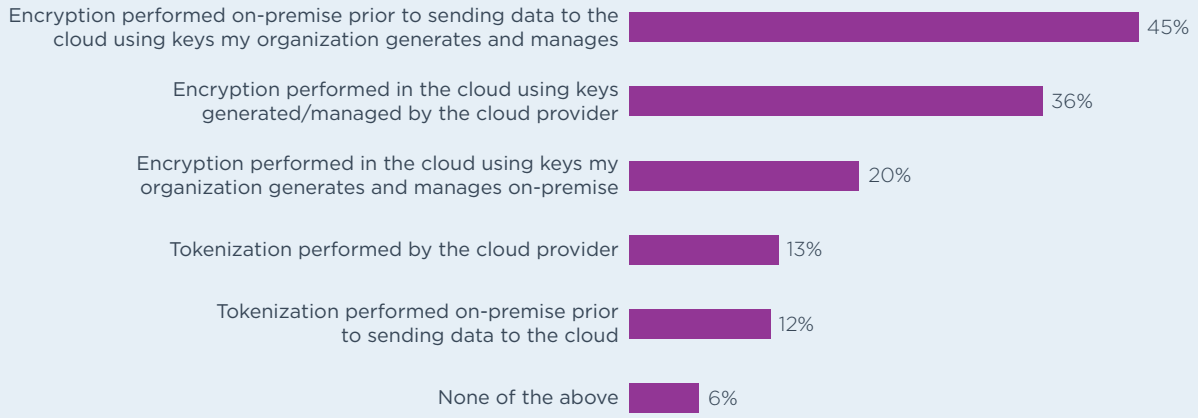
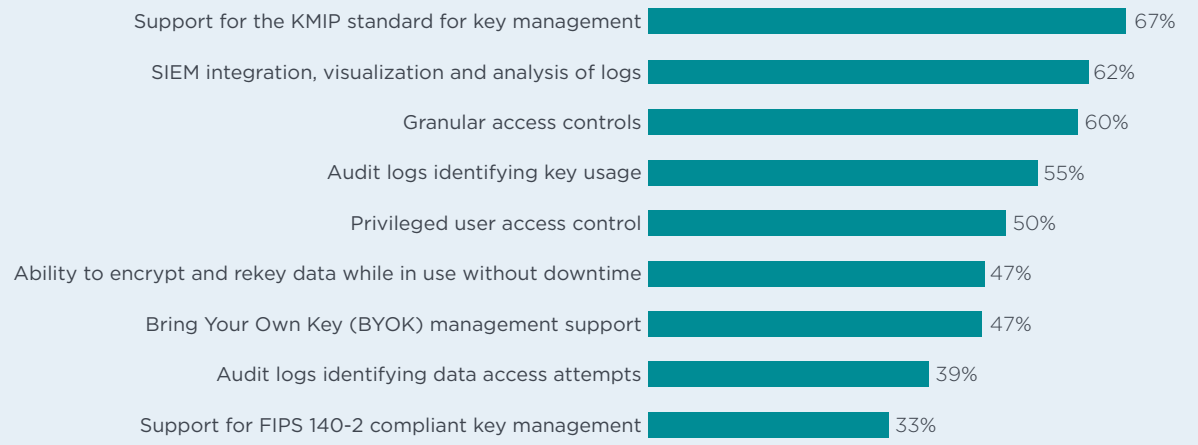


Figure 29 **How important are the following features associated with cloud encryption to your organization?**
Very important and Important responses combined



APPENDIX
METHODS & LIMITATIONS

Table 1 reports the sample response for 17 separate country samples. Data collection was started in December 2019 and completed in January 2020. Our consolidated sampling frame of practitioners in all countries consisted of 169,574 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 7,203 returns of which 746 were rejected for reliability issues. Our final consolidated 2019 sample was 6,457, thus resulting in an overall 3.8% 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 17 separate country samples. Trend analysis was performed on combined country samples. This year we added the Netherlands and Sweden.

Table 1. Survey response in 17 countries

Legend	Survey response	Sampling frame	Final sample	Response rate
AB	Middle East	9,900	342	3.5%
AU	Australia	6,993	325	4.6%
BZ	Brazil	12,686	471	3.7%
DE	Germany	11,256	473	4.2%
FR	France	11,237	354	3.2%
HK	Hong Kong	6,057	267	4.4%
IN	India	15,201	596	3.9%
JP	Japan	10,988	504	4.6%
KO	Korea	9,697	321	3.3%
MX	Mexico	10,434	353	3.4%
NL	Netherlands	8,816	302	3.4%
RF	Russian Federation	6,009	216	3.6%
SA	Southeast Asia	7,645	276	3.6%
SW	Sweden	6,988	277	4.0%
TW	Taiwan	7,161	302	4.2%
UK	United Kingdom	10,501	389	3.7%
US	United States	18,005	689	3.8%
	Consolidated	169,574	6,457	3.8%

Table 2 summarizes our survey samples for 17 countries over a 14-year period.

Figure 30 reports the respondent's organizational level within participating organizations. By design, 55 percent of respondents are at or above the supervisory levels and 44 percent of respondents reported their position as associate/staff/technician. Respondents have on average 8.5 years of security experience with approximately 5.6 years of experience in their current position.

Table 2. Sample history over 14 years

Legend	FY19	FY18	FY17	FY16	FY15	FY14	FY13	FY12	FY11	FY10	FY09	FY08	FY07	FY06
AB	342	340	308	316	368									
AU	325	327	315	331	334	359	414	938	471	477	482	405		
BZ	471	517	507	463	460	472	530	637	525					
DE	473	531	543	531	563	564	602	499	526	465	490	453	449	
FR	354	332	370	345	344	375	478	584	511	419	414			
HK	267	317												
IN	596	587	582	548	578	532	0	0	0					
JP	504	502	468	450	487	476	521	466	544					
KO	321	325	317											
MX	353	499	468	451	429	445								
NL	302													
RF	216	226	196	206	201	193	201							
SA	276	268												
SW	277													
TW	302													
UK	389	402	468	460	487	509	637	550	651	622	615	638	541	489
US	689	683	710	701	758	789	892	531	912	964	997	975	768	918
Total	6,457	5,856	5,252	4,802	5,009	4,714	4,275	4,205	4,140	2,947	2,998	2,471	1,758	1,407

Figure 30. **Distribution of respondents according to position level**
Country samples are consolidated

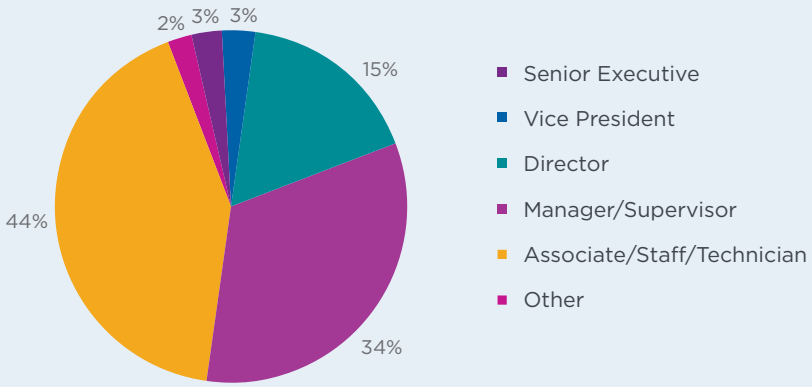


Figure 31 identifies the organizational location of respondents in our study. Over half (55 percent) of respondents are located within IT operations. This is followed by security at 20 percent of respondents and lines of business at 9 percent of respondents.

Figure 32 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. Twelve percent of respondents are located in manufacturing and industrial organizations and 10 percent of respondents are in service organizations. Another nine percent are located in the technology and software sector.

Figure 31. **Distribution of respondents according to organizational location**
Country samples are consolidated

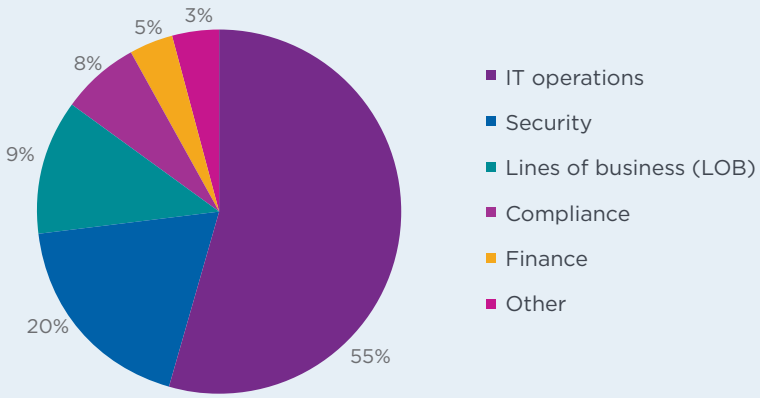
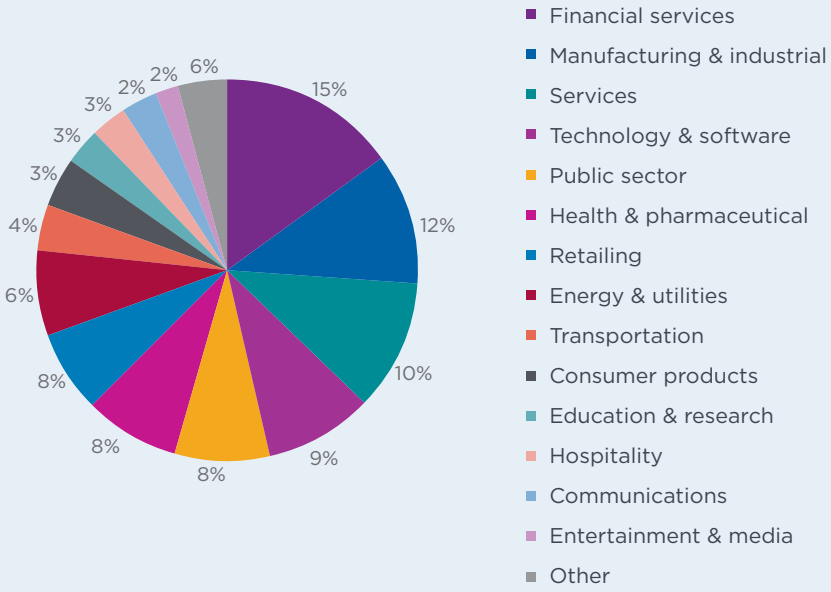


Figure 32. **Distribution of respondents according to primary industry classification**
Country samples are consolidated



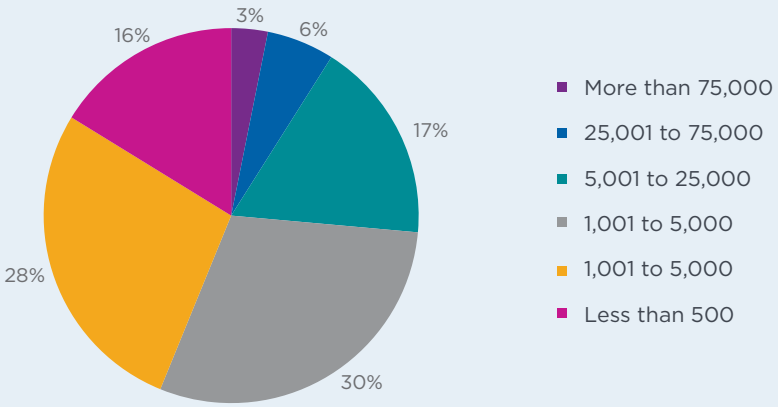
According to Figure 33 more than half (56 percent) of respondents are located in larger-sized organizations with a global headcount of more than 1,000 employees.

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 17 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 17 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 33. **Distribution of respondents according to organizational headcount**
Country samples are consolidated



View the full Global Encryption Trends Study consolidated findings at
https://bit.ly/2U6JnGp

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

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our 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, ensure the integrity of your data and put you in complete control – today, tomorrow, always. **www.ncipher.com**

ABOUT ENTRUST DATACARD

Employees, citizens and consumers increasingly expect anywhere-anytime experiences — whether they are logging on to corporate networks, crossing borders, accessing e-gov services or making purchases. They also expect the ecosystems that allow this freedom and flexibility to be entirely reliable and secure. Entrust Datacard offers the trusted identity and secure transaction technologies that make these ecosystems possible. Our 45+ years of industry-leading expertise and experience spans the globe, with more than 2,000 employees serving customers in 150 countries worldwide. For more information, visit **www.entrustdatacard.com**

> Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency — it also multiplies the security risks.

ncipher.com

entrustdatacard.com