Ponemon INSTITUTE

NCIPHER

2019 HONG KONG AND TAIWAN ENCRYPTION TRENDS STUDY

01 EXECUTIVE SUMMARY

PONEMON INSTITUTE IS PLEASED TO PRESENT THE FINDINGS OF THE *2019 HONG KONG AND TAIWAN ENCRYPTION TRENDS STUDY*, SPONSORED BY NCIPHER SECURITY.

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 the following 14 countries and regions, including Hong Kong and Taiwan. The countries and regions include: Australia, Brazil, France, Germany, India, Japan, Mexico, Middle East, the Russian Federation, South Korea (hereafter referred to as Korea), Southeast Asia, the United Kingdom and the United States.

As shown in Figure 1, organizations represented in this research recognize the importance of having an encryption strategy, either an enterprise-wide (39 percent of respondents) or a limited strategy that targets certain applications and data types (37 percent of respondents).

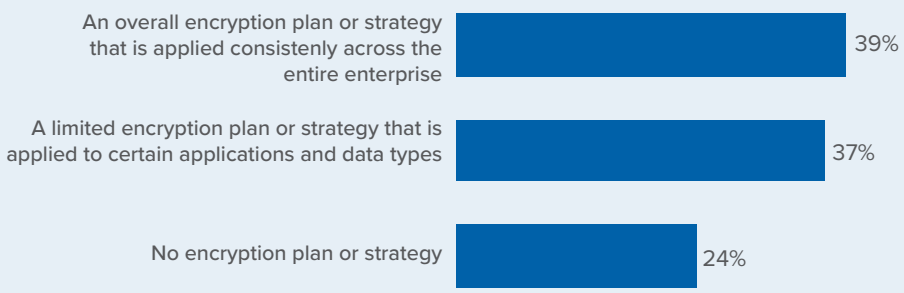
Following is a summary of our key findings. More details are provided for each key finding listed below in the next section of this report.

IT operations has the most influence in directing encryption strategies.
While responsibility for the encryption strategy is dispersed throughout the organization, IT operations (35 percent of respondents) has the most influence. Twenty-seven percent of respondents say no one single function is responsible for encryption strategy.

Which data types are most often encrypted?
Of seven data types presented in this research, organizations are mostly encrypting employee/HR data and intellectual property.

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 48 percent of respondents. Thirty-two percent of respondents say temporary or contract workers, and 31 percent of respondents say third party service providers pose the biggest threat.

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



Protection of customer's personal information is the main driver to using encryption technologies.

Protecting customer's personal information and enterprise intellectual property are the main drivers at 74 percent and 70 percent of respondents, respectively. In contrast, to reduce the scope of compliance audits (18 percent of respondents) and compliance with internal policies (17 percent of respondents) are the least influential drivers for encryption.

Discovering where sensitive data resides in the organization is the biggest challenge.

Figure 6 provides a list of six challenges to an organization's effective execution of its data encryption strategy in descending order of importance. Discovering where sensitive data resides in the organization and classifying which data to encrypt are the biggest challenges, according to 59 percent and 46 percent of respondents, respectively.

No single encryption technology dominates in organizations.

No single technology dominates because organizations have very diverse needs. Encryption of databases, Internet communications and laptop and hard drives are most likely to be extensively deployed. In contrast, encryption of Internet of Things (IoT) platforms and devices, a nascent but emerging use case, is less likely to be fully or partially deployed.

Certain encryption features are considered more critical than others.

The most important features are support for both cloud and on-premise deployment (91 percent of respondents), integration with other security tools (74 percent of respondents) and enforcement of policy (74 percent of respondents). Features that are not considered as important are system scalability and support for regional segregation (e.g. data residency) (43 percent and 33 percent of respondents, respectively).

How painful is key management?

Fifty-nine percent (20 + 39) of respondents chose ratings at 7 or above, thus suggesting a fairly high pain threshold. The top reasons are: systems are isolated and fragmented (61 percent of respondents), key management tools are inadequate (57 percent of respondents) and no clear ownership (47 percent of respondents).

Which keys are most difficult to manage?

The most difficult keys to manage are: end user encryption keys (e.g. email, full disk encryption), keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys and signing keys (e.g. code signing, digital signatures).

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. Sixty-three percent of respondents say they are important today and 70 percent of respondents say they will be important in the next 12 months. Database encryption is a growing use case for HSMs. Other top use cases for HSMs in the next 12 months are: SSL/TLS, Internet of Things root of trust, big data encryption and payment service provider interface.

How organizations are using HSM.

Sixty-two percent of respondents say they have a centralized team that provides cryptography as a service and 38 percent of respondents say each individual application owner/team is responsible for their own cryptographic services. Hong Kong and Taiwan have demonstrated the same progress at moving to a centralized model for cryptography—the global average is 61 percent of respondents.

Most organizations transfer sensitive or confidential data to the cloud.

Fifty-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 21 percent of respondents plan to in the next 12 to 24 months. Almost half (48 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 percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys the organization generates and manages and 35 percent of respondents say encryption is performed in the cloud using keys generated/managed by the cloud provider.

02 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:

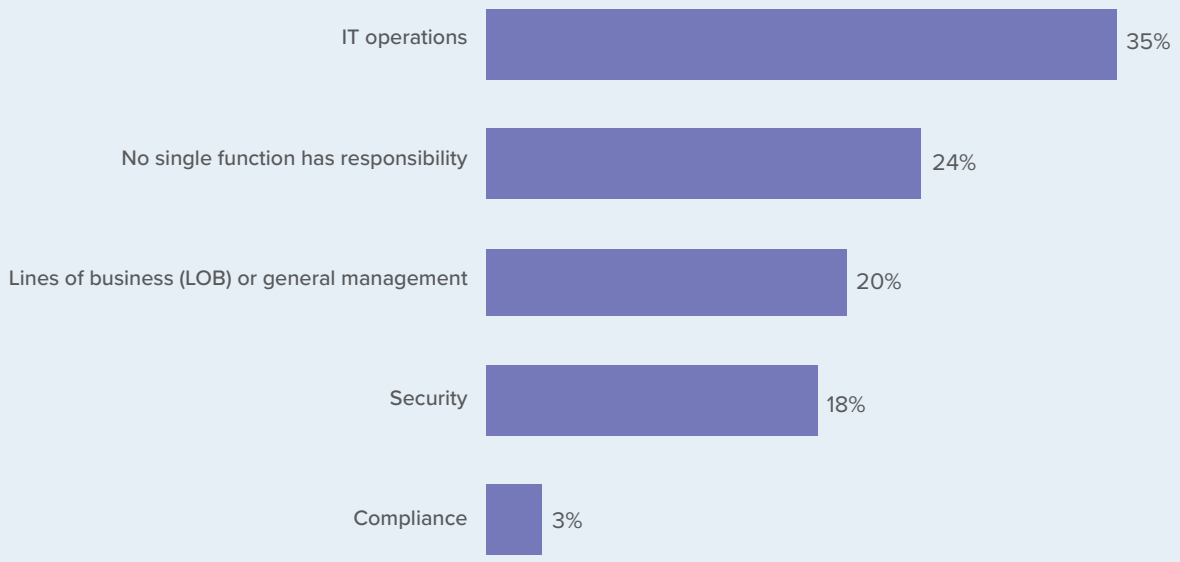
- Strategy and adoption of encryption
- Threats, main drivers and priorities
- Deployment choices
- Encryption features considered most important
- Attitudes about key management
- Importance of hardware security modules (HSMs)[1]
- Cloud encryption

STRATEGY AND ADOPTION OF ENCRYPTION

IT operations has 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 (35 percent of respondents) has the most influence. Twenty-four percent of respondents say no one single function is responsible for encryption strategy.

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

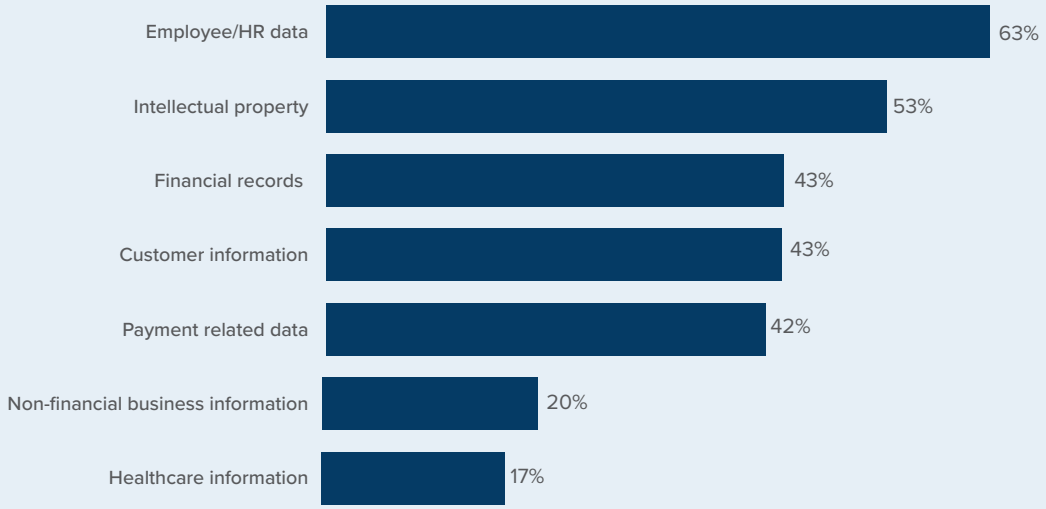


[1]HSMs are devices specifically built to create a tamper-resistant environment in which to perform cryptographic processes (e.g. encryption or digital signing) and to manage the keys associated with those processes. These devices are used to protect critical data processing activities and can be used 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, organizations are mostly encrypting employee/HR data and intellectual property.

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

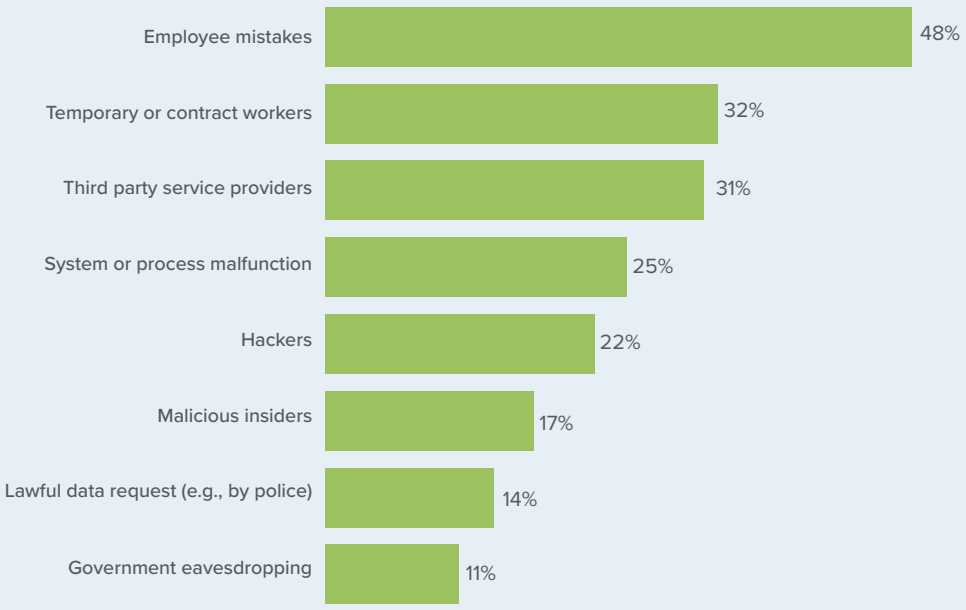


THREATS, MAIN DRIVERS AND PRIORITIES

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 48 percent of respondents. Thirty-two percent of respondents say temporary or contract workers and 31 percent of respondents say third party service providers pose the biggest threat.

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



Protection of customer's personal information is the main driver to using encryption technologies.

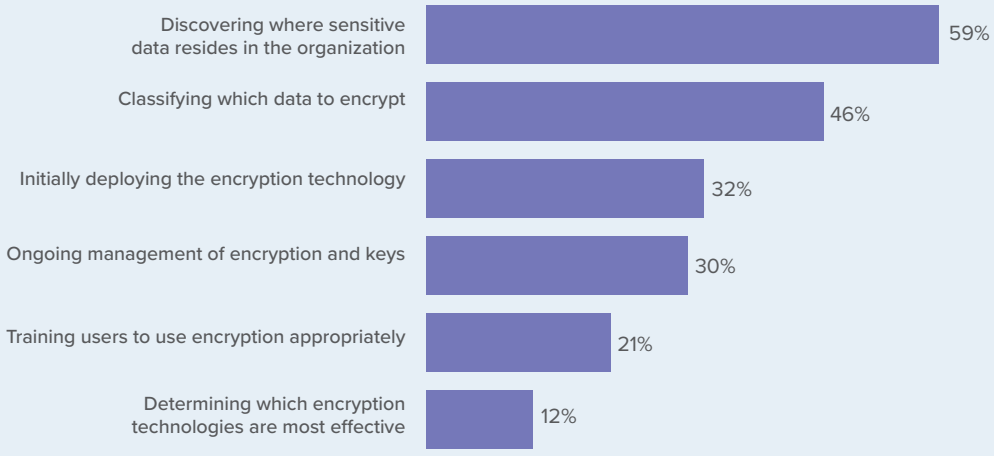
Eight drivers for deploying encryption are presented in Figure 5. The importance of protecting customer's personal information and enterprise intellectual property are the main drivers at 74 percent and 70 percent of respondents, respectively. In contrast, to reduce the scope of compliance audits (18 percent of respondents) and compliance with internal policies (17 percent of respondents) are the least influential drivers for encryption.

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

Discovering where sensitive data resides in the organization is the biggest challenge.

Figure 6 provides a list of six challenges to an organization's effective execution of its data encryption strategy in descending order of importance. Discovering where sensitive data resides in the organization and classifying which data to encrypt are the biggest challenges, according to 59 percent and 46 percent of respondents, respectively.

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



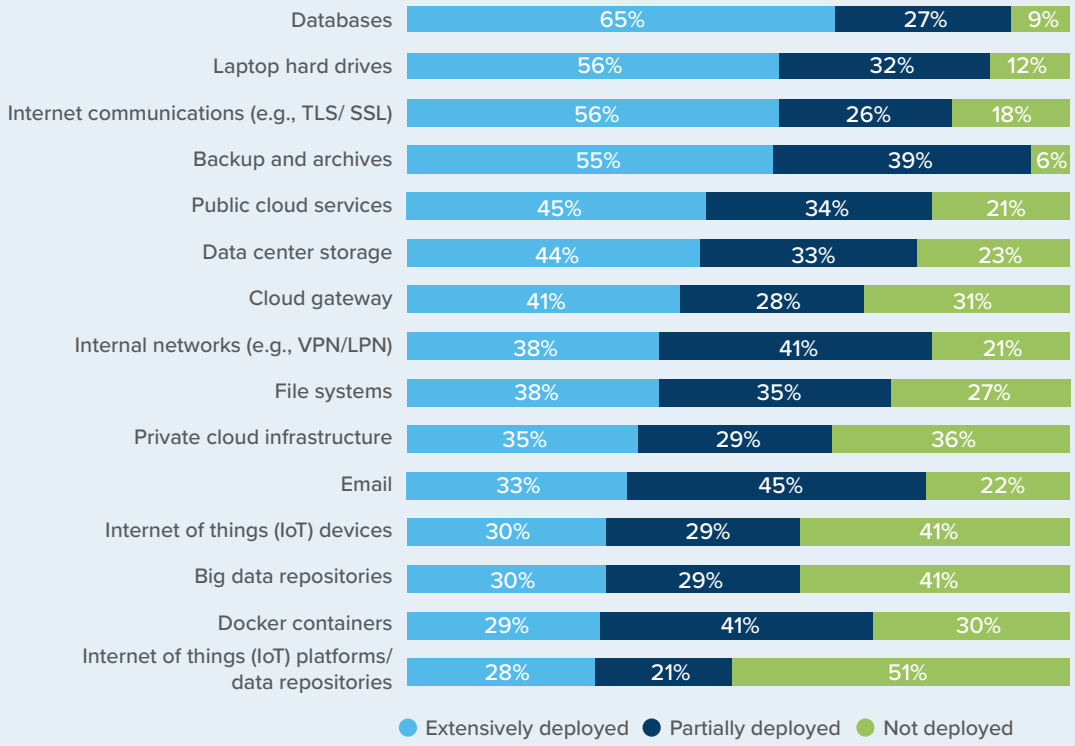
DEPLOYMENT CHOICES

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

Figure 7. **The use of encryption technologies**



No single technology dominates because organizations have very diverse needs. Encryption of databases, Internet communications and laptop and hard drives are most likely to be extensively deployed.

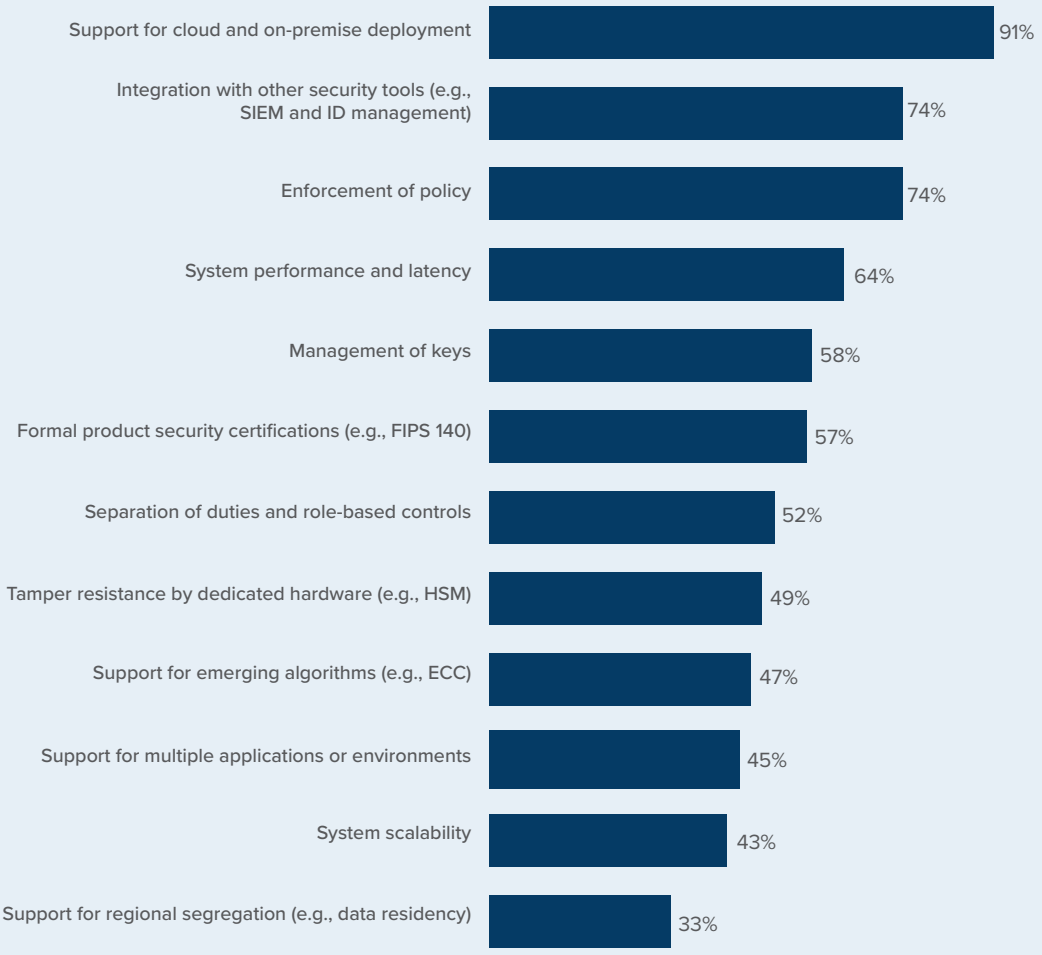
ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

Certain encryption features are considered more critical than others.

Figure 8 lists 12 encryption technology features. Each percentage defines the very important response (on a four-point scale). Respondents were asked to rate encryption technology features considered most important to their organization's security posture.

The most important features are support for both cloud and on-premise deployment (91 percent of respondents), integration with other security tools (74 percent of respondents) and enforcement of policy (74 percent of respondents). Features that are not considered as important are system scalability and support for regional segregation (e.g. data residency) (43 percent and 33 percent of respondents, respectively).

Figure 8. **Most important features of encryption technology solutions**
Very important and important responses combined

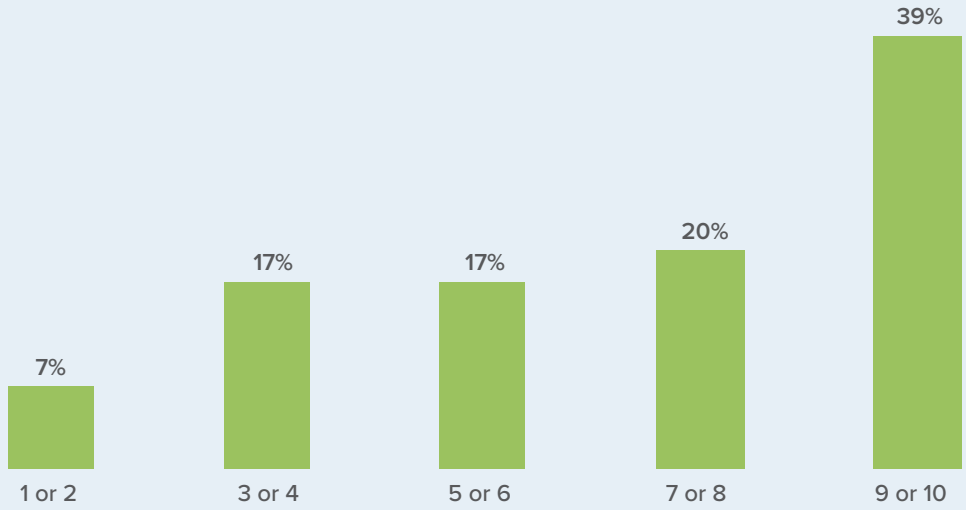


ATTITUDES ABOUT KEY MANAGEMENT

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 (20 + 39) of respondents chose ratings at 7 or above, thus suggesting a fairly high pain threshold.

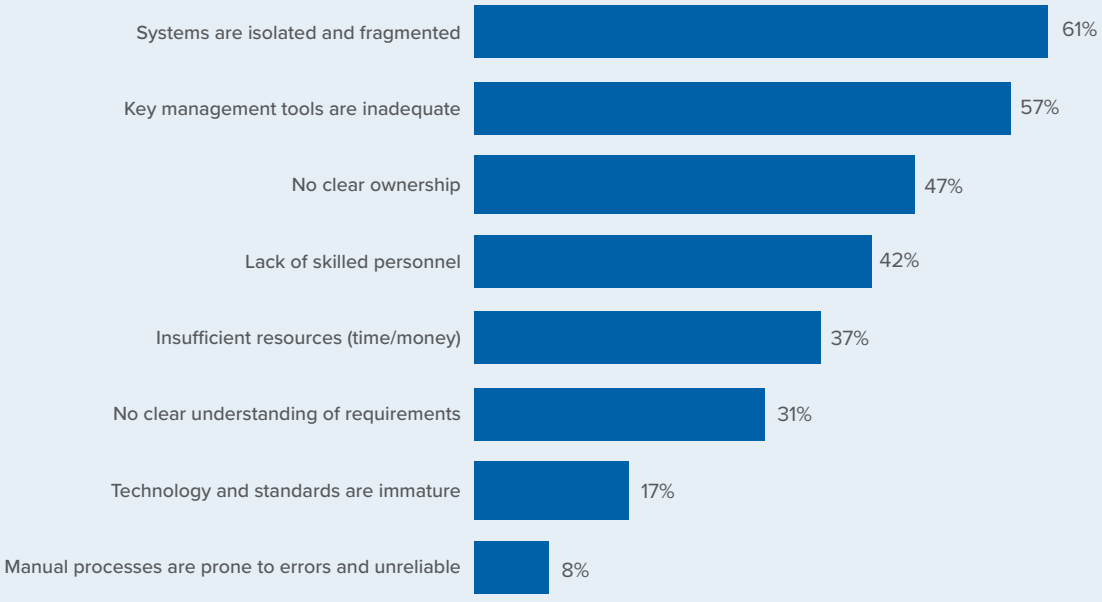
Figure 9. **How painful is key management?**
1 = minimal impact to 10 = severe impact



Why is key management painful?

Figure 10 shows the reasons why the management of keys is so difficult. The top reasons are: systems are isolated and fragmented (61 percent of respondents), key management tools are inadequate (57 percent of respondents) and no clear ownership (47 percent of respondents).

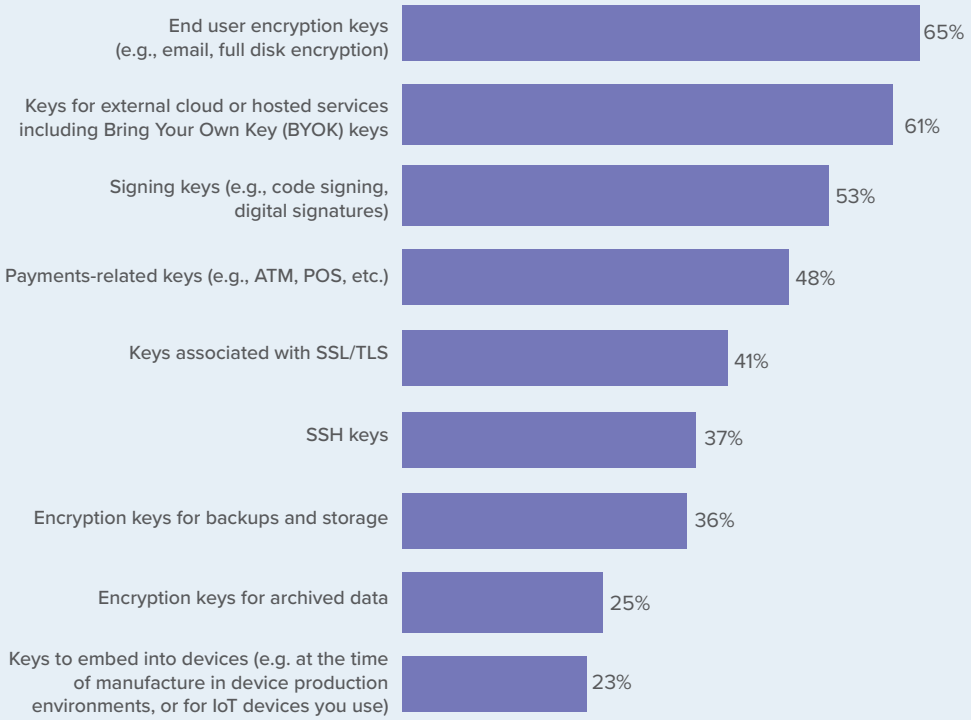
Figure 10. **What makes the management of keys so painful?**
Three responses permitted



Which keys are most difficult to manage?

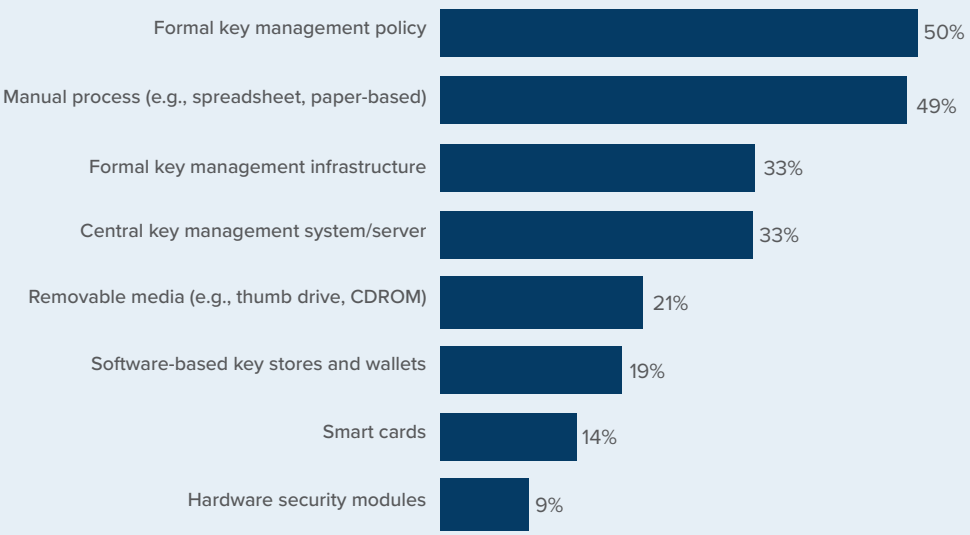
Figure 11 provides a list of keys that are most difficult to manage. These are: end user encryption keys (e.g. email, full disk encryption), keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys and signing keys (e.g. code signing, digital signatures).

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



As shown in Figure 12, respondents' companies use a variety of key management systems. The most commonly deployed systems are: formal key management policy (KMP) and manual processes (50 percent and 49 percent of respondents, respectively).

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

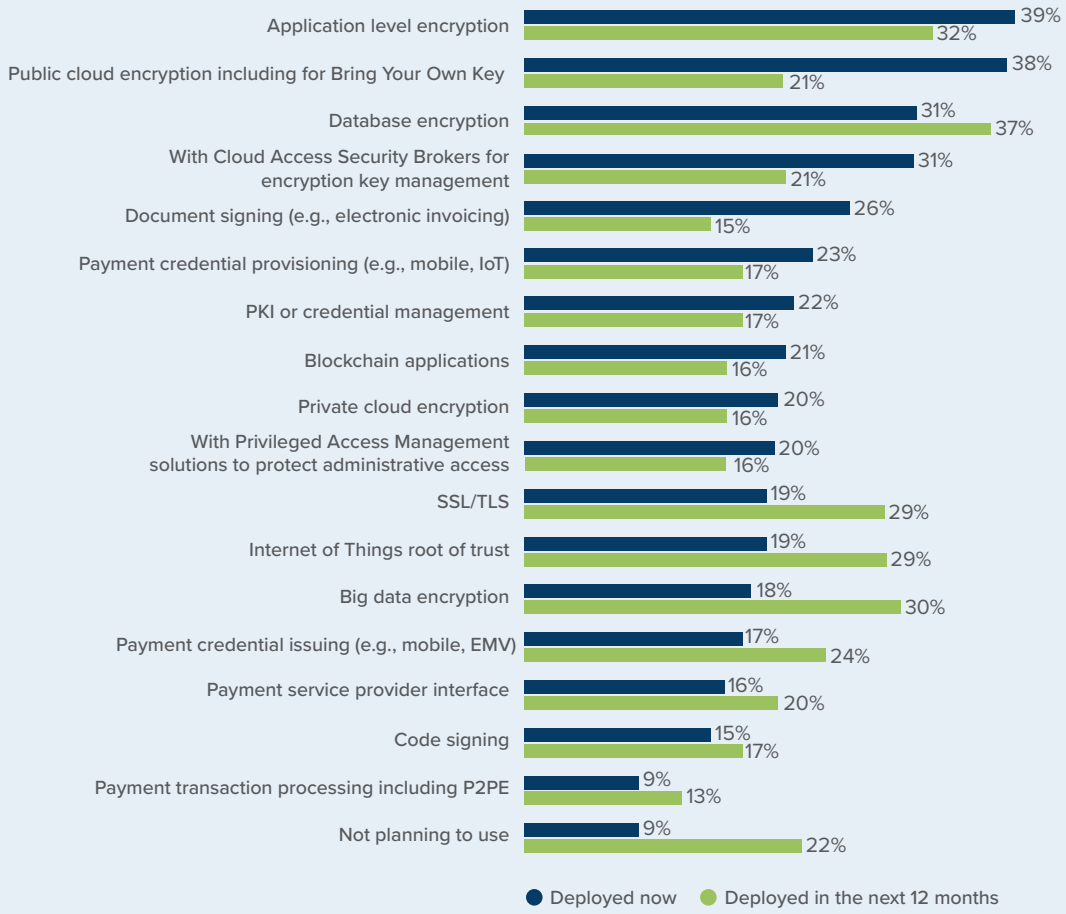


IMPORTANCE OF HARDWARE SECURITY MODULES (HSMS)

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. Sixty-three percent of respondents say they are important today and 70 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. Database encryption is a growing use case for HSMs. Other top use cases for HSMs in the next 12 months are: SSL/TLS, Internet of Things root of trust, big data encryption and payment service provider interface.

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

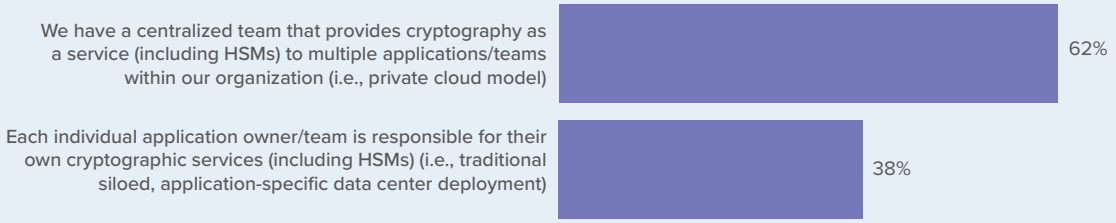


Database encryption is a growing use case for HSMs. Other top use cases for HSMs in the next 12 months are: **SSL/TLS, Internet of Things root of trust, big data encryption** and **payment service provider interface.**

How organizations are using HSMs.

According to Figure 14, 62 percent of respondents say they have a centralized team that provides cryptography as a service and 38 percent of respondents say each individual application owner/team is responsible for their own cryptographic services. Hong Kong and Taiwan have demonstrated the same progress at moving to a centralized model for cryptography—the global average is 61 percent of respondents.

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

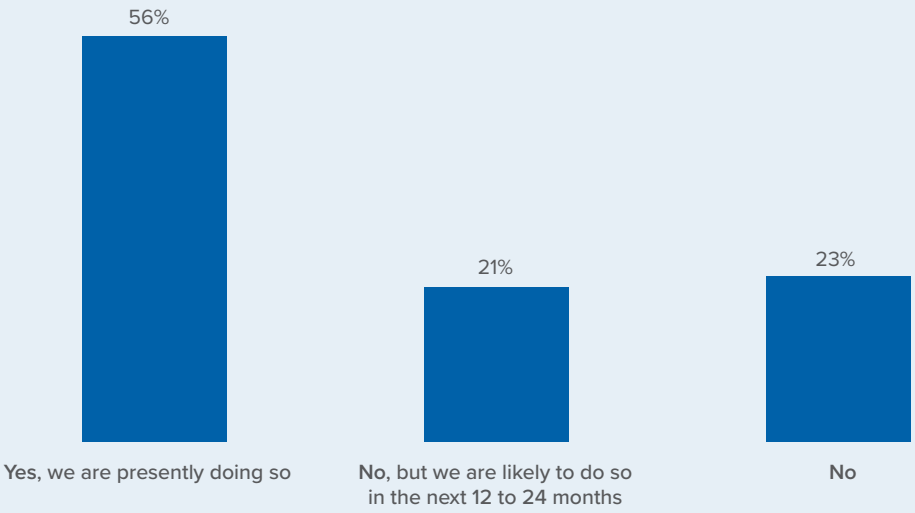


CLOUD ENCRYPTION

Most organizations transfer sensitive or confidential data to the cloud.

As shown in Figure 15, 56 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 21 percent of respondents plan to in the next 12 to 24 months. Almost half (48 percent of respondents) say it is the cloud provider who is most responsible for protecting sensitive or confidential data transferred to the cloud.

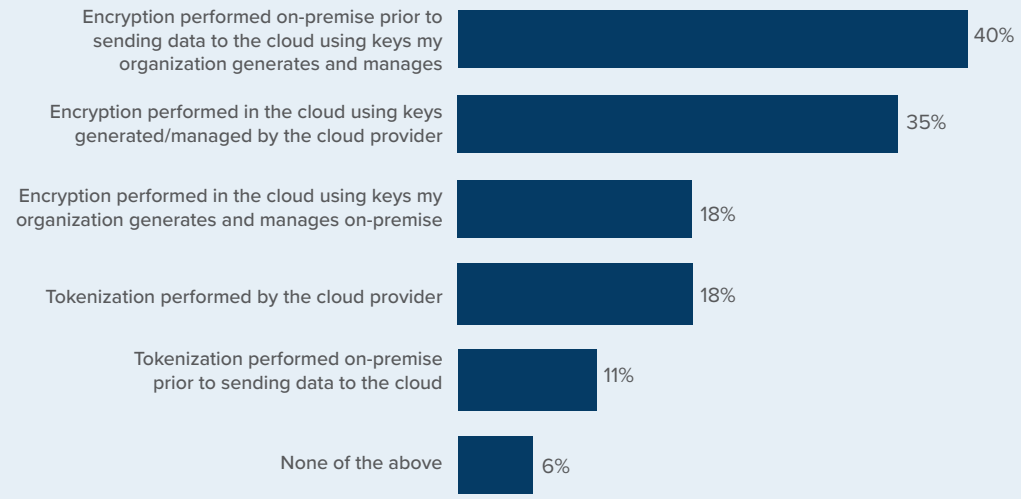
Figure 15. **Do you currently transfer sensitive or confidential data to the cloud?**



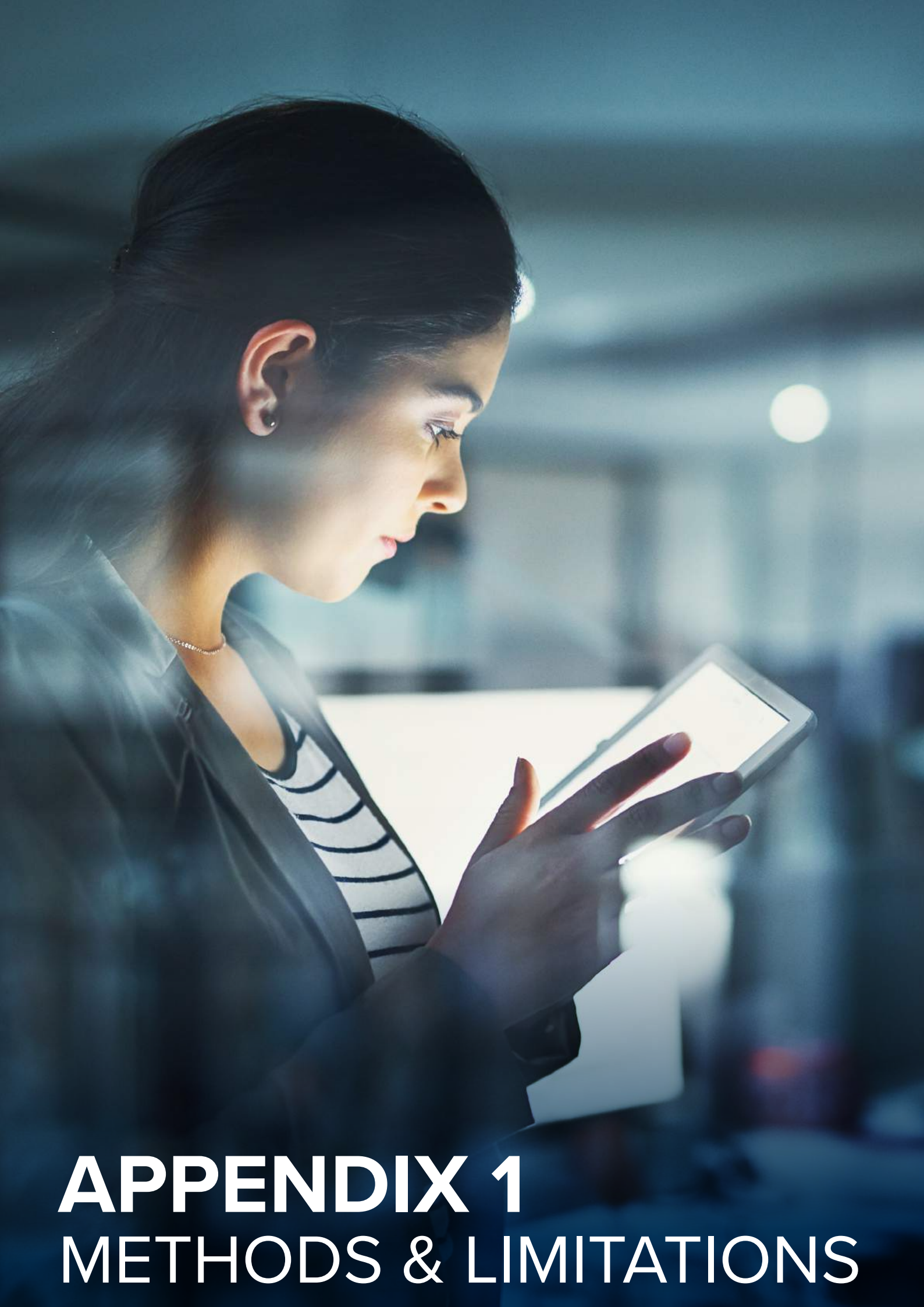
How is data at rest in the cloud protected?

As shown in Figure 16, 40 percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys the organization generates and manages and 35 percent of respondents say encryption is performed in the cloud using keys generated/managed by the cloud provider.

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



40 percent of respondents say **encryption is performed on-premise prior to sending data to the cloud using keys the organization generates and manages** and **35 percent** of respondents say **encryption is performed in the cloud using keys generated/managed by the cloud provider.**



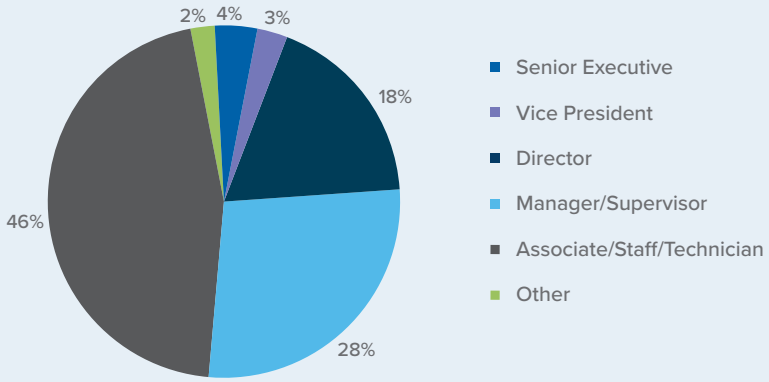
APPENDIX 1
METHODS & LIMITATIONS

Table 1 reports the sample response for Hong Kong and Taiwan. The sample response for this study was conducted in December 2018. Our sampling frame of security practitioners consisted of 8,360 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 345 returns of which 28 were rejected for reliability issues. Our final Hong Kong and Taiwan sample was 317, thus resulting in an overall 3.8% response rate.

Table 1. Sample response	Freq	Pct%
Total sampling frame	8,360	100%
Total returns	345	4.1%
Rejected or screened surveys	28	0.3%
Final sample	317	3.8%

Figure 17 summarizes the approximate position levels of respondents in our study. As can be seen, half of the respondents (52 percent) are at or above the supervisory level and 46 percent of respondents are at the associate/staff/technician level. Respondents have on average 11 years of security experience with approximately six years of experience in their current position.

Figure 17. **Distribution of respondents according to position level**



Our **sampling frame** of security practitioners consisted of **8,360 individuals** who have bona fide credentials in **IT or security fields**.

Figure 18 reports the respondents' functional area. As shown, 53 percent of respondents are located in IT operations, 15 percent are in security, 13 percent of respondents are in compliance 7 percent are in finance and another 7 percent are in lines of business.

Figure 18. **Distribution of respondents according to functional area**

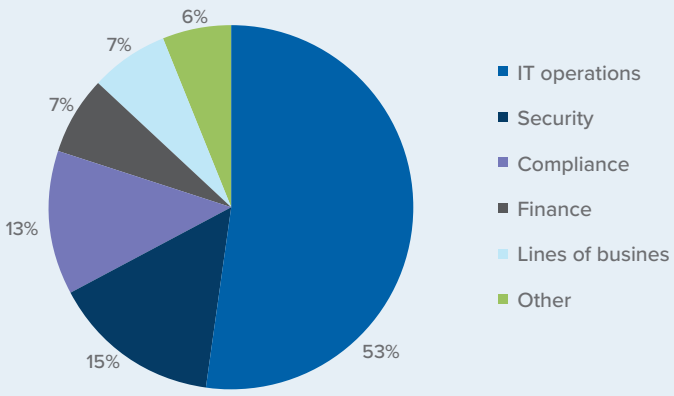
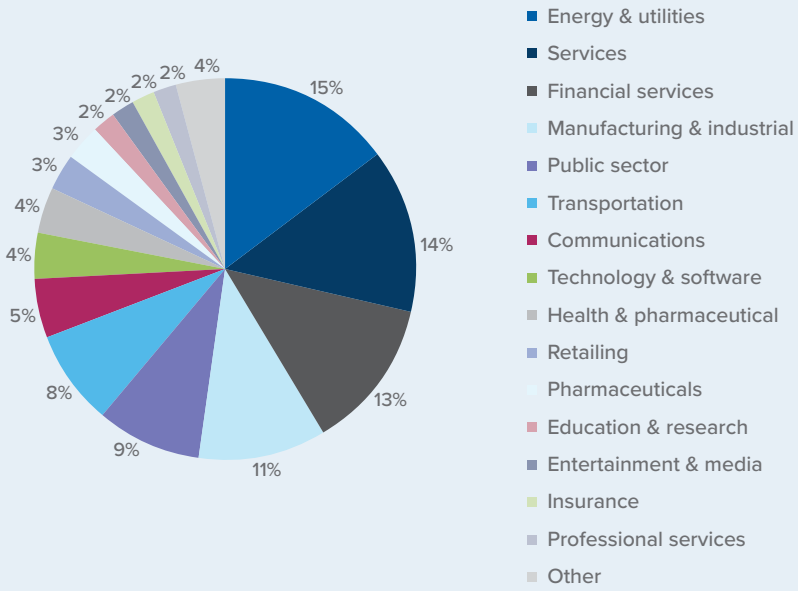


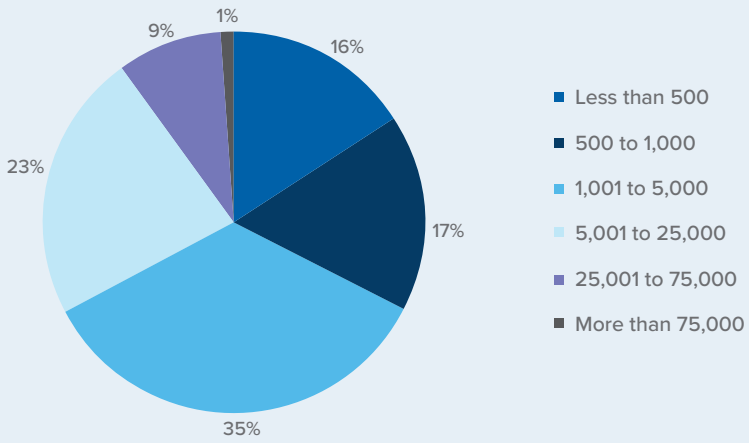
Figure 19 reports the respondents' organizations primary industry segments. As shown, 15 percent of respondents are located in the energy and utilities industry, 14 percent of respondents are in the services industry, 13 percent are located in the financial services industry, which includes banking, investment management, insurance, brokerage, payments and credit cards.

Figure 19. **Distribution of respondents according to primary industry classification**



According to Figure 20, more than half (67 percent) of respondent 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 Hong Kong and Taiwan, 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 Hong Kong and Taiwan.

■ 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
CONSOLIDATED FINDINGS

The following tables provide the results for the Hong Kong and Taiwan sample.

Survey response	HKT
Sampling frame	8360
Total returns	345
Rejected or screened surveys	28
Final sample	317
Response rate	3.8%

PART 1. ENCRYPTION POSTURE

Q1. Please select one statement that best describes your organization's approach to encryption implementation across the enterprise.	HKT
We have an overall encryption plan or strategy that is applied consistently across the entire enterprise	39%
We have a limited encryption plan or strategy that is applied to certain applications and data types	37%
We don't have an encryption plan or strategy	24%
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	HKT
Extensively deployed	55%
Partially deployed	39%
Not deployed	6%
Total	100%

Q2b-1. Big data repositories	HKT
Extensively deployed	30%
Partially deployed	29%
Not deployed	41%
Total	100%

Q2c-1 Cloud gateway	HKT
Extensively deployed	41%
Partially deployed	28%
Not deployed	31%
Total	100%

Q2d-1. Data center storage	HKT
Extensively deployed	44%
Partially deployed	33%
Not deployed	23%
Total	100%

Q2e-1. Databases	HKT
Extensively deployed	65%
Partially deployed	27%
Not deployed	9%
Total	100%

Q2f-1. Docker containers	HKT
Extensively deployed	29%
Partially deployed	41%
Not deployed	30%
Total	100%

Q2g-1. Email	HKT
Extensively deployed	33%
Partially deployed	45%
Not deployed	22%
Total	100%

Q2h-1. Public cloud services	HKT
Extensively deployed	45%
Partially deployed	34%
Not deployed	21%
Total	100%

Q2i-1. File systems	HKT
Extensively deployed	38%
Partially deployed	35%
Not deployed	27%
Total	100%

Q2j-1. Internet communications (e.g., SSL)	HKT
Extensively deployed	56%
Partially deployed	26%
Not deployed	18%
Total	100%

Q2k-1. Internal networks (e.g., VPN/LPN)	HKT
Extensively deployed	38%
Partially deployed	41%
Not deployed	21%
Total	100%

Q2l-1. Laptop hard drives	HKT
Extensively deployed	56%
Partially deployed	32%
Not deployed	12%
Total	100%

Q2m-1 Private cloud infrastructure	HKT
Extensively deployed	35%
Partially deployed	29%
Not deployed	36%
Total	100%

Q2n-1 Internet of things (IoT) devices	HKT
Extensively deployed	30%
Partially deployed	29%
Not deployed	41%
Total	100%

Q2o-1 Internet of things (IoT) platforms	HKT
Extensively deployed	28%
Partially deployed	21%
Not deployed	51%
Total	100%

Q3. How many different products does your organization use that perform encryption?	**HKT**
1 to 3	12%
4 to 6	24%
7 to 9	29%
10 to 12	27%
13 or more	8%
Total	100%

Q4. Who is most influential in directing your organization's encryption strategy? Please select one best choice.	**HKT**
IT operations	35%
Security	18%
Compliance	3%
Lines of business (LOB) or general management	20%
No single function has responsibility	24%
Total	100%

Q5. What are the reasons why your organization encrypts sensitive and confidential data? Please select the top three reasons.	**HKT**
To protect enterprise intellectual property	70%
To protect customer personal information	74%
To limit liability from breaches or inadvertent disclosure	32%
To avoid public disclosure after a data breach occurs	21%
To protect information against specific, identified threats	35%
To comply with internal policies	17%
To comply with external privacy or data security regulations and requirement	34%
To reduce the scope of compliance audits	18%
Unsure	0%
Total	300%

Q6. What are the biggest challenges in planning and executing a data encryption strategy? Please select the top two reasons.	**HKT**
Discovering where sensitive data resides in the organization	59%
Classifying which data to encrypt	46%
Determining which encryption technologies are most effective	12%
Initially deploying the encryption technology	32%
Ongoing management of encryption and keys	30%
Training users to use encryption appropriately	21%
Other	0%
Total	200%

Q7. How important are the following features associated with encryption solutions that may be used by your organization? Very important and important response combined.	**HKT**
Enforcement of policy	74%
Management of keys	58%
Support for multiple applications or environments	45%
Separation of duties and role-based controls	52%
System scalability	43%
Tamper resistance by dedicated hardware (e.g., HSM)	49%
Integration with other security tools (e.g., SIEM and ID management)	74%
Support for regional segregation (e.g., data residency)	33%
System performance and latency	64%
Support for emerging algorithms (e.g., ECC)	47%
Support for cloud and on-premise deployment	91%
Formal product security certifications (e.g., FIPS 140)	57%
Total	686%

Q8. What types of data does your organization encrypt? Please select all that apply.	**HKT**
Customer information	43%
Non-financial business information	20%
Intellectual property	53%
Financial records	43%
Employee/HR data	63%
Payment related data	42%
Healthcare information	17%

Q9. What are the main threats that might result in the exposure of sensitive or confidential data? Please select the top two choices.	**HKT**
Hackers	22%
Malicious insiders	17%
System or process malfunction	25%
Employee mistakes	48%
Temporary or contract workers	32%
Third party service providers	31%
Lawful data request (e.g., by police)	14%
Government eavesdropping	11%
Other	0%
Total	200%

PART 2. KEY MANAGEMENT

Q10. Please rate the overall "pain" associated with managing keys or certificates within your organization, where 1 = minimal impact to 10 = severe impact?	**HKT**
1 or 2	7%
3 or 4	17%
5 or 6	17%
7 or 8	20%
9 or 10	39%
Total	100%

Q11. What makes the management of keys so painful? Please select the top three reasons.	**HKT**
No clear ownership	47%
Insufficient resources (time/money)	37%
Lack of skilled personnel	42%
No clear understanding of requirements	31%
Key management tools are inadequate	57%
Systems are isolated and fragmented	61%
Technology and standards are immature	17%
Manual processes are prone to errors and unreliable	8%
Other	0%
Total	300%

Q12. Following are a wide variety of keys that may be managed by your organization. Please rate the overall "pain" associated with managing each type of key. Very painful and painful response combined.	**HKT**
Encryption keys for backups and storage	25%
Encryption keys for archived data	36%
Keys associated with SSL/TLS	41%
SSH keys	37%
End user encryption keys (e.g., email, full disk encryption)	65%
Signing keys (e.g., code signing, digital signatures)	53%
Payments-related keys (e.g., ATM, POS, etc.)	48%
Keys to embed into devices (e.g., at the time of manufacture in device production environments, or for IoT devices you use)	23%
Keys for external cloud or hosted services including Bring Your Own Key (BYOK) keys	61%

Q13a. What key management systems does your organization presently use?	HKT
Formal key management policy (KMP)	50%
Formal key management infrastructure (KMI)	33%
Manual process (e.g., spreadsheet, paper-based)	49%
Central key management system/server	33%
Hardware security modules	9%
Removable media (e.g., thumb drive, CDROM)	21%
Software-based key stores and wallets	19%
Smart cards	14%
Total	229%

Q13b. What key management systems does your organization presently not used or not aware of use?	HKT
Formal key management policy (KMP)	26%
Formal key management infrastructure (KMI)	30%
Manual process (e.g., spreadsheet, paper-based)	27%
Central key management system/server	39%
Hardware security modules	45%
Removable media (e.g., thumb drive, CDROM)	43%
Software-based key stores and wallets	39%
Smart cards	73%
Total	321%

PART 3. HARDWARE SECURITY MODULES

Q14. What best describes your level of knowledge about HSMs?	HKT
Very knowledgeable	33%
Knowledgeable	28%
Somewhat knowledgeable	23%
No knowledge (skip to Q18)	16%
Total	100%

Q15a. Does your organization use HSMs?	HKT
Yes	39%
No (skip to Q18)	61%
Total	100%

Q15. For what purpose does your organization presently deploy or plan to use HSMs? Please select all that apply.	
Q15b-1. HSMs used today	**HKT**
Application level encryption	39%
Database encryption	31%
Big data encryption	18%
Public cloud encryption including for Bring Your Own Key (BYOK)	38%
Private cloud encryption	20%
SSL/TLS	19%
PKI or credential management	22%
Internet of Things (IoT) root of trust	19%
Document signing (e.g. electronic invoicing)	26%
Code signing	15%
Payment transaction processing including P2PE	9%
Payment credential issuing (e.g., mobile, EMV)	17%
Payment credential provisioning (e.g., mobile, IoT)	23%
Payment service provider interface (e.g., TSP, real-time payments, Open API)	16%
With Cloud Access Security Brokers (CASBs) for encryption key management	31%
With Privileged Access Management (PAM) solutions to protect administrative access	20%
Blockchain applications (e.g., cryptocurrency, financial transfer)	21%
Not planning to use	9%
Other	1%
Total	394%

Q15b-2. HSMs planned to be deployed in the next 12 months	HKT
Application level encryption	32%
Database encryption	37%
Big data encryption	30%
Public cloud encryption including for Bring Your Own Key (BYOK)	21%
Private cloud encryption	16%
SSL/TLS	29%
PKI or credential management	17%
Internet of Things (IoT) root of trust	29%
Document signing (e.g. electronic invoicing)	15%
Code signing	17%
Payment transaction processing including P2PE	13%
Payment credential issuing (e.g., mobile, EMV)	24%
Payment credential provisioning (e.g., mobile, IoT)	17%
Payment service provider interface (e.g., TSP, real-time payments, Open API)	20%
With Cloud Access Security Brokers (CASBs) for encryption key management	21%
With Privileged Access Management (PAM) solutions to protect administrative access	16%
Blockchain applications (e.g., cryptocurrency, financial transfer)	16%
Not planning to use	22%
Other	1%
Total	393%

Q15c-1. If you use HSMs in conjunction with public cloud based applications, what models do you use today? Please select all that apply.	HKT
Rent/use HSMs from public cloud provider, hosted in the cloud	43%
Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications	51%
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	18%
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)	14%
Not using HSMs with public cloud applications	3%
Total	129%

Q15c-2. If you use HSMs in conjunction with public cloud based applications, what models do you plan to use in the next 12 months. Please select all that apply.	HKT
Rent/use HSMs from public cloud provider, hosted in the cloud	52%
Own and operate HSMs on-premise at your organization, accessed real-time by cloud-hosted applications	65%
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	30%
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)	23%
Not using HSMs with public cloud applications	2%
Total	173%

Q16. In your opinion, how important are HSMs to your encryption or key management strategy? Very important and important response combined	HKT
Q16a. Importance today	63%
Q16b. Importance in the next 12 months	70%

Q17. Which statement best describes how your organization uses HSMs?	HKT
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).	62%
Each individual application owner/team is responsible for their own cryptographic services (including HSMs) (i.e. traditional siloed, application-specific data center deployment).	38%
Total	100%

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

Q37. Does your organization currently use cloud computing services for any class of data or application – both sensitive and non-sensitive?	HKT
Yes, we are presently doing so	66%
No, but we are likely to do so in the next 12 to 24 months	14%
No (Go to Part 7 if you do not use cloud services for any class of data or application)	20%
Total	100%

Q38. Do you currently transfer sensitive or confidential data to the cloud (whether or not it is encrypted or made unreadable via some other mechanism)?	HKT
Yes, we are presently doing so	56%
No, but we are likely to do so in the next 12 to 24 months	21%
No (Go to Part 7 if you do not use or plan to use any cloud services for sensitive or confidential data)	23%
Total	100%

Q39. In your opinion, who is most responsible for protecting sensitive or confidential data transferred to the cloud?	HKT
The cloud provider	48%
The cloud user	22%
Shared responsibility	30%
Total	100%

Q40. How does your organization protect data at rest in the cloud?	HKT
Encryption performed in the cloud using keys generated/managed by the cloud provider	35%
Encryption performed in the cloud using keys my organization generates and manages on-premise	18%
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	18%
Tokenization performed on-premise prior to sending data to the cloud	11%
None of the above	6%
Total	128%

Q41. For encryption of data at rest in the cloud, my organization's strategy is to...	HKT
Only use keys controlled by my organization	52%
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	16%
Use a combination of keys controlled by my organization and by the cloud provider, with a preference for keys controlled by the cloud provider	20%
Total	100%

Q42. How important are the following features associated with cloud encryption to your organization? Very important and Important response provided.	HKT
Bring Your Own Key (BYOK) management support	40%
Privileged user access control	39%
Granular access controls	51%
Audit logs identifying key usage	49%
Audit logs identifying data access attempts	39%
SIEM integration, visualization and analysis of logs	64%
Support for FIPS 140-2 compliant key management	25%
Support for the KMIP standard for key management	72%
Ability to encrypt and rekey data while in use without downtime	46%
Total	455%

Q43-1. How many public cloud providers does your organization in use today?	HKT
1	37%
2	30%
3	25%
4 or more	8%
Total	100%

Q43-2. How many public cloud providers does your organization plan to use in the next 12 to 24 months?	HKT
1	25%
2	29%
3	15%
4 or more	31%
Total	100%

PART 7: ROLE AND ORGANIZATIONAL CHARACTERISTICS

D1. What organizational level best describes your current position?	HKT
Senior Executive	4%
Vice President	3%
Director	18%
Manager/Supervisor	28%
Associate/Staff/Technician	46%
Other	2%
Total	100%

D2. Select the functional area that best describes your organizational location.	HKT
IT operations	53%
Security	15%
Compliance	13%
Finance	7%
Lines of business (LOB)	7%
Other	6%
Total	100%

D3. How many years of business experience do you have?	HKT
Total years of security experience	10.9
Total years in current position	6.1

D4. What industry best describes your organization's industry focus?	HKT
Communications	5%
Education & research	2%
Energy & utilities	15%
Entertainment & media	2%
Financial services	13%
Health & pharmaceutical	4%
Manufacturing & industrial	11%
Insurance	2%
Internet & ISPs	1%
Pharmaceuticals	3%
Professional services	2%
Public sector	9%
Retailing	3%
Services	14%
Technology & software	4%
Transportation	8%

D5. What is the worldwide headcount of your organization?	HKT
Less than 500	16%
500 to 1,000	17%
1,001 to 5,000	35%
5,001 to 25,000	23%
25,001 to 75,000	9%
More than 75,000	1%
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 NCIPHER SECURITY

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

Our cryptographic solutions secure emerging technologies – cloud, IoT, blockchain, digital payments – and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times. **www.ncipher.com**

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

Search: nCipherSecurity

www.ncipher.com

nCIPHER