

2019

GLOBAL ENCRYPTION TRENDS STUDY

Executive
Summary

PONEMON INSTITUTE IS PLEASED TO PRESENT THE FINDINGS OF THE 2019 GLOBAL ENCRYPTION TRENDS STUDY¹, SPONSORED BY NCIPHER SECURITY.

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

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

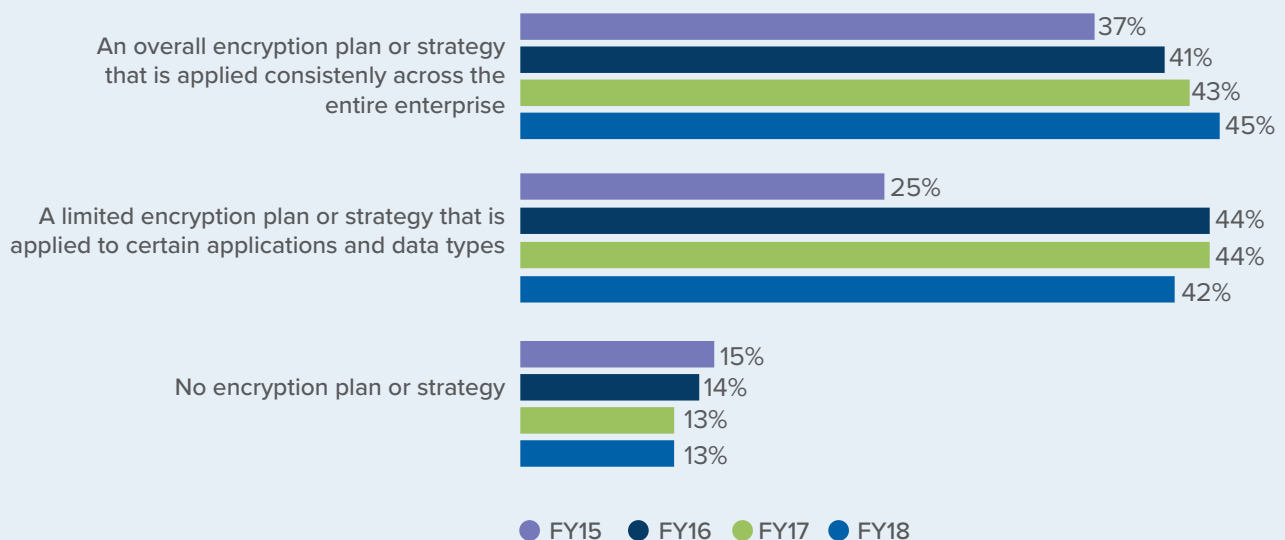
The first encryption trends study was conducted in 2005 for a US sample of respondents.³ Since then we have expanded the scope of the research to include respondents in all regions of the world.

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

The following pages contain the 2019 findings.

Figure 1. **Does your company have an encryption strategy?**

Country samples are consolidated



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

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

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

STRATEGY AND ADOPTION OF ENCRYPTION

Enterprise-wide encryption strategies increase.

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

Certain countries have more mature encryption strategies.

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

The IT operations function is the most influential in framing the organization's encryption strategy over the past 14 years.

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

TRENDS IN ADOPTION OF ENCRYPTION

The use of encryption increases in all industries. Results suggest a steady increase in all industry sectors.

The most significant increases in extensive encryption usage occur in manufacturing, hospitality and consumer products.

The extensive use of encryption technologies increases.

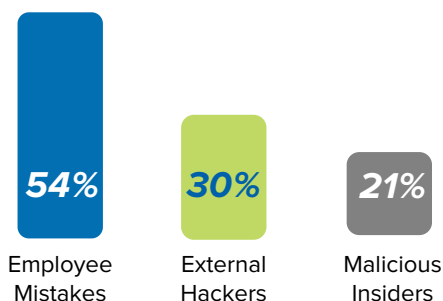
Since we began tracking the enterprise-wide use of encryption in 2005, there has been a steady increase in the encryption solutions extensively used by organizations.

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

THREATS, MAIN DRIVERS AND PRIORITIES

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

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



EMPLOYEE MISTAKES

are by far the most significant threat to sensitive data (**54%** of respondents – *more than external hackers and malicious insiders combined*).

The main driver for encryption is protection of sensitive information.

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

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

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



DATA DISCOVERY

continues to be the biggest challenge in planning and executing a data encryption strategy (**69% of respondents**).

DEPLOYMENT CHOICES

No single encryption technology dominates in organizations.

Organizations have very diverse needs. Internet communications, databases and laptop hard drives are the most likely to be encrypted and correspond to mature use cases. For the second year, the study tracked the deployment of encryption of IoT devices and platforms. As shown, 52 percent of respondents say encryption of IoT devices and 50 percent of respondents say encryption on IoT platforms have been at least partially deployed.

ENCRYPTION FEATURES CONSIDERED MOST IMPORTANT

Certain encryption features are considered more critical than others.

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

Which data types are most often encrypted?

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



POLICY ENFORCEMENT

is rated as the most important feature of encryption solutions (**73% of respondents rated higher than performance for the first time!**)



61%

of respondents rate the pain of encryption key management at **7** or higher on a **10** point scale.

1 = minimum impact, 10 = severe impact

ATTITUDES ABOUT KEY MANAGEMENT

How painful is key management?

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

Companies continue to use a variety of key management systems.

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

IMPORTANCE OF HARDWARE SECURITY MODULES (HSMS)

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

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

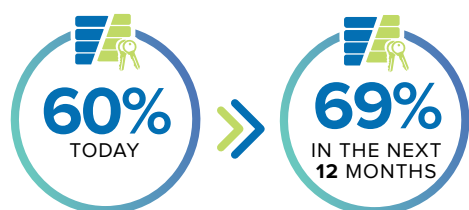
How HSMS in conjunction with public cloud-based applications are primarily deployed today and in the next 12 months.

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

COUNTRIES WITH HIGHEST HSM USAGE RATES



THE IMPORTANCE OF HSMs TO AN ENCRYPTION OR KEY MANAGEMENT STRATEGY



The overall average importance rating for HSMs, as part of an encryption and key management strategy in the current year is 60 percent.

The pattern of responses suggests Japan, Germany and Australia are most likely to assign importance to HSMs as part of their organization's encryption or key management activities.

What best describes an organization's use of HSMs?

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

What are the primary purposes or uses for HSMs?

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

CLOUD ENCRYPTION

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

60%

of organizations use HSMs to provide internal **cryptography-as-a-service**

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

How do organizations protect data at rest in the cloud?

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

What are the top three encryption features specifically for the cloud?

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

THE MOST IMPORTANT CLOUD ENCRYPTION FEATURES ARE:



73%

Support for the KMIP standard



60%

SIEM integration



58%

Granular access controls



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

[CLICK TO DOWNLOAD THE FULL REPORT](#)



Search: nCipherSecurity



www.ncipher.com

