THALES

Ponemon INSTITUTE

GLOBAL ENCRYPTION TRENDS STUDY

April 2017

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

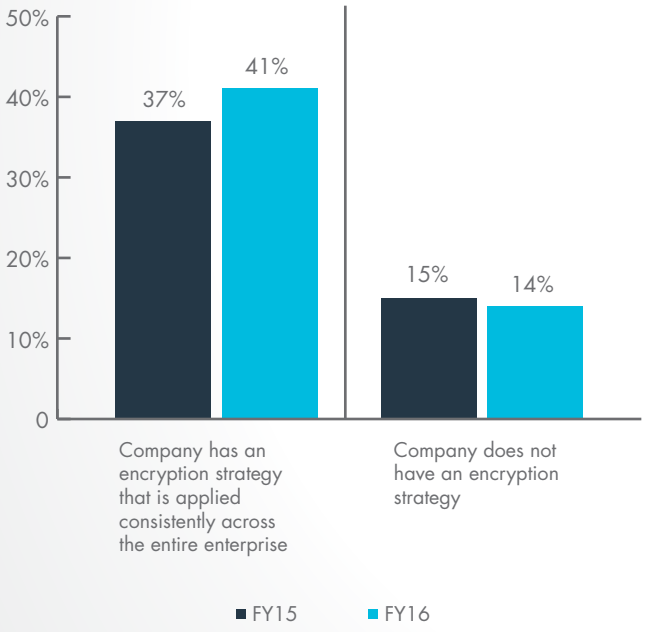
Ponemon Institute is pleased to present the findings of the 2017 Global Encryption Trends Study, sponsored by Thales e-Security. We surveyed 4,802 individuals across multiple industry sectors in 11 countries - the United States, United Kingdom, Germany, France, Australia, Japan, Brazil, the Russian Federation, Mexico, India and Arabia (which is a combination of respondents located in Saudi Arabia and the United Arab Emirates).[2]

The purpose of this research is to examine how the use of encryption has evolved over the past 12 years and the impact of this technology on the security posture of organizations. The first encryption trends study was conducted in 2005 for a U.S. sample of respondents.[3] Since then, we have expanded the scope of the research to include respondents in all regions of the world.

In our research, we consider the threats organizations face and how encryption is being used to reduce these risks. Mega breaches and cyber attacks have increased companies' urgency to improve their security posture. This is reflected in this year's findings as more companies embrace an enterprise-wide encryption strategy—which has increased from 15 percent in FY05 to 41 percent in FY16, as shown in Figure 1.

Following is a summary of our key findings, which is organized in three subsections: (1) overall findings, (2) challenges and drivers, and (3) key management. More details are provided for each key finding listed below in the next section of this report. We believe the findings demonstrate the importance of encryption and key management in achieving a strong security posture.

Figure 1. Does your company have an encryption strategy?



[1]This year's collection of data was completed in January 2017. 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 FY16. The same dating convention is used in prior years.

[2]Country-level results are abbreviated as follows: Germany (DE), Japan (JP), United States (U.S.), United Kingdom (U.K.), Australia (AU), France (FR), Brazil (BZ), Russia (RF), Mexico (MX), India (IN) and Arabian cluster (AB).

[3]The trend analysis shown in this study was performed on combined country samples spanning 12 years (since 2005).

New findings in 2017

In this year's research, we added questions about the use of Hardware Security Modules (HSMs) and public cloud services. Following are the findings.

HSM use in conjunction with cloud-based applications still favors on-premise HSM deployment. Almost half (48 percent of respondents) own and operate HSMs on-premise in support of cloud-based applications. Thirty-six percent of respondents say their organizations rent/use HSMs from a public cloud provider for their cloud applications.

Organizations will increase both on-premise and cloud HSM use in the next 12 months. Respondents say their organizations will grow their use of on-premise HSMs that are accessed real-time by cloud-hosted applications (55 percent of respondents) and will also increase their use of cloud-hosted HSMs (41 percent of respondents).

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 using a private cloud model. Forty-one percent say each individual application owner/team is responsible for their own cryptographic services (including HSMs), reflecting a more traditional siloed application-specific data center deployment.

For the first time in the history of the study, **business unit leaders** have the **highest influence over encryption strategy** (higher than IT!)

41% of **companies** now have a consistent enterprise-wide **encryption strategy**

How do organizations protect data at rest in the cloud? Forty-six percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys their organization generates and manages. However, 37 percent of respondents rely on the cloud provider to both generate/manage keys and perform encryption.

Overall findings

Enterprise-wide encryption strategies increase. As shown in Figure 1, 41 percent of respondents in this year's study say their organization has an encryption strategy applied consistently across the entire enterprise. Only 14 percent of respondents say their organization does not have an encryption strategy.

In the first year of this study (FY05), less than 15 percent of respondents said their organization had a comprehensive encryption strategy and 38 percent did not have any strategy in place.

German organizations are more likely to have a comprehensive encryption strategy. Over 65 percent of German respondents say their organization has a comprehensive encryption strategy. In contrast, only 30 percent of Arabian and 31 percent of Mexican organizations have an encryption strategy applied consistently across the entire enterprise.

Lines of business increase their influence in determining the company's encryption strategy. Thirty percent of respondents say lines of business or general management are most influential, 29 percent say IT operations, and only 16 percent of respondents say it is the security function. Only two percent of respondents chose compliance. We see four countries – namely, France, Mexico, the U.K. and U.S. – choosing their organization's lines of business management as being most influential. The remaining seven countries chose IT operations.

The extensive use of encryption technologies increases but budgets decrease. This year we examined the usage rates for 13 encryption technology categories. Our analysis shows a substantial increase in the percentage of respondents who say their organizations are extensive rather than partial users. Extensive use means the encryption technology is used consistently across the entire enterprise. Partial use means the given technology is a point solution or is narrowly deployed.

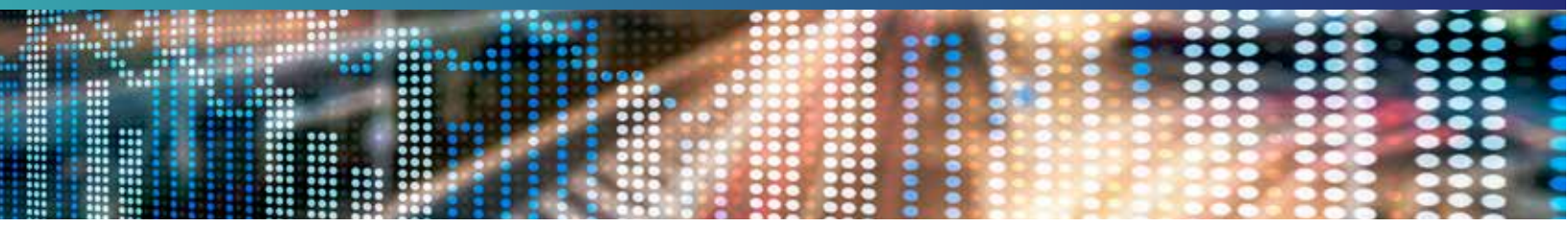
In FY05, only 16 percent of respondents were extensive users as compared to 41 percent in FY16. While the extensive use of encryption has steadily increased over 12 years, the percentage of the IT budget earmarked for encryption has actually decreased in the last three years.

The extensive use of encryption varies considerably by industry segment. Specifically, heavily regulated industries such as financial services and healthcare have the highest use rate; less regulated industries such as manufacturing and consumer products have the lowest use rate. Trends over the past four years suggest a steady increase in all industry segments. The most significant increases in extensive encryption usage occur in public sector, retail and technology and software organizations.

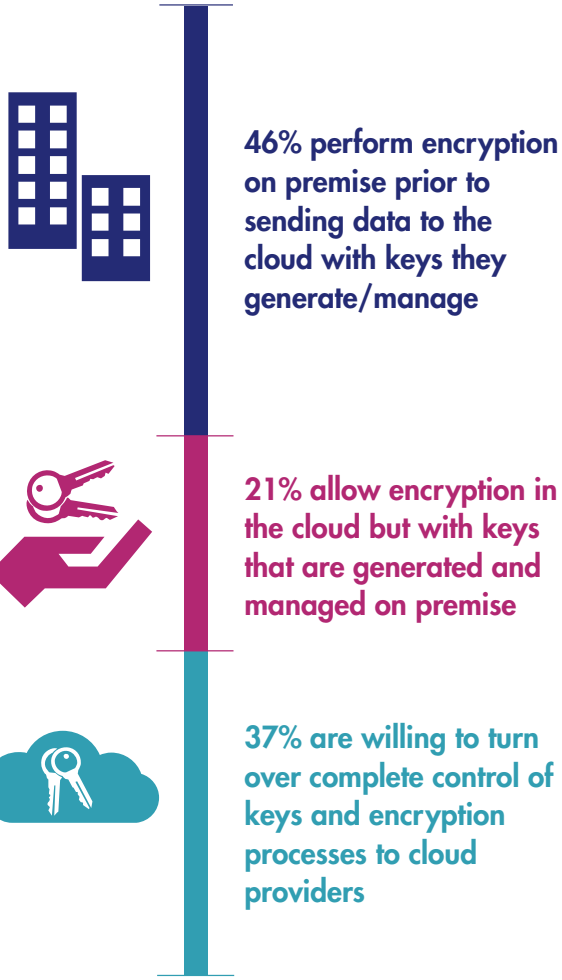
Challenges, drivers and usage

Employee mistakes are the most significant threat to sensitive data. According to 54 percent of respondents, employee error is the most significant threat to sensitive or confidential data. Thirty percent chose hackers and 29 percent chose systems or process malfunction as their most significant threat. The fact that two of the top three findings on threats relate to mistakes or errors, as opposed to targeted threats, is notable.

COMPLIANCE REMAINS THE TOP DRIVER FOR ENCRYPTION, HOWEVER IT IS FOLLOWED BY A CLOSE MARGIN BY IP PROTECTION, CUSTOMER INFORMATION PROTECTION, AND PROTECTION FROM EXTERNAL THREATS



Organizations continue to show a preference for **control over encryption** in the cloud



Compliance continues to be the main driver to invest in the extensive use of encryption. Fifty-five percent of respondents see compliance with privacy and data security requirements as the main driver to extensive encryption use within their company. Not far behind, 51 percent of respondents see protecting enterprise intellectual property as the main driver. The least significant drivers include avoiding data breach disclosures (10 percent of respondents) and compliance with internal policies (19 percent of respondents).

What is the biggest challenge to encryption deployment? Fifty-nine percent of respondents say discovering where sensitive data resides in the organization is their most difficult challenge. This is not surprising for the following reasons: the proliferation of data that is occurring with increased connectivity, larger numbers of endpoint devices and increased use of the cloud. In addition, 47 percent of all respondents cite initially deploying encryption technology as a significant challenge and 36 percent of respondents see classifying what data to encrypt as a significant challenge.

Looking across 13 encryption categories, we observe that no single technology dominates the encryption portfolio because organizations have very diverse needs. Encryption of databases, Internet communications and data center storage are the most likely to be deployed (89 percent, 85 percent and 80 percent, respectively). In contrast, encryption for big data repositories (53 percent of respondents), public cloud services (55 percent of respondents) and private cloud infrastructure (59 percent) have lower use rates but have grown from the previous year.

The use of encryption varies among countries. Respondents in Germany, U.S., Japan and U.K. have the highest deployment rates. Arabia, Mexico and Australia have the lowest deployment rates.

Certain encryption technology features are more important than others. Respondents were asked to rate encryption technology features considered most important to their organization's security posture. According to the consolidated findings, the three most important features are: (1) system performance and latency (2) enforcement of policy and (3) support for cloud and on-premise deployment. The consistent year-over-year top finding of performance and latency underscores the importance organizations place on encryption that is transparent and without negative consequences to other functions and systems.

IT security spending is increasing. The average percentage of IT security spending relative to total IT spending over 12 years has increased. The trend appears to be upward sloping, which suggests the proportion of IT spending dedicated to security activities, including encryption, is increasing over time.

Data protection spending is increasing as well. The percentage of data protection spending relative to the total IT security budget over 12 years has increased. This trend appears to be slightly upward sloping, which suggests data protection spending as a proportion of total IT security is also on the rise.

The 12-year trend in the percentage of encryption spending relative to the total IT security budget has increased from a low of 9.7 percent in FY05 to a high of 18.2 percent in FY13. We postulate three reasons for a recent decrease: (1) price pressure resulting from increased competition among vendors, (2) shifting priorities to other IT security solution areas and (3) more efficient use of presently available encryption tools.

Companies are transferring sensitive or confidential data to the cloud. Fifty-three 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. With respect to the transfer of sensitive or confidential data to the cloud, India (70 percent of respondents), Mexico (67 percent) and the U.S. (60 percent of respondents) have higher use rates than other countries. In contrast, Germany has the lowest rate.

Encryption deployment grew the most in **Big Data, Databases, and Public Cloud**

Key management and HSMs

Respondents rated the overall "pain" associated with managing keys within their organization. Fifty-nine percent of respondents rate the management of keys at a fairly high pain level. With respect to country-level results, Arabia has the highest pain level and Russia has the lowest pain level.

Why is the pain level high? The following are the top three reasons why the management of keys is so painful: (1) no clear ownership of the key management function, (2) lack of skilled personnel and (3) isolated or fragmented key management systems.

According to respondents, the types of keys that are most difficult to manage include: (1) keys for external cloud or hosted services and (2) SSH keys. The least difficult are: (1) embedded device keys, (2) encryption keys for backups and storage and (3) encryption keys for archived data.

Companies continue to use a variety of key management systems. The most commonly deployed systems include: (1) manual process (paper or spreadsheets), (2) formal key management policy and (3) central key management system/server. The fact that manual processes remain the most popular indicates reluctance to adopt tools, possibly due to lack of standardization or lack of general awareness.

Respondents in Germany, U.S. and Japan are most likely to deploy HSMs as part of their organization's key management program – an indication of their overall higher encryption and security maturity. The overall usage rate for HSMs has steadily increased over the past four years—and rose from 34 percent in FY15 to 38 percent in FY16.

The importance of HSMs to encryption and key management activities has increased. The overall average importance rating in the current year is 56 percent of respondents, which represents an increase from prior years. The pattern of responses suggests organizations in Germany, US and Japan are most likely to attribute high importance to HSMs.

What are the primary purposes for deploying HSMs? According to respondents, the two top choices are SSL/TLS and application-level encryption. Several application areas were noted as growing 4% or more over the next 12 months, including SSL/TLS, database encryption, PKI credential management, payment transaction processing, and payment credential issuing.

ABOUT PONEMON INSTITUTE

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

ABOUT THALES E-SECURITY

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

ABOUT THALES

Thales is a global technology leader for the Aerospace, Transport, Defence and Security markets. With 64,000 employees in 56 countries, Thales reported sales of €14.9 billion in 2016. With over 25,000 engineers and researchers, Thales has a unique capability to design and deploy equipment, systems and services to meet the most complex security requirements. Its exceptional international footprint allows it to work closely with its customer all over the world.

THALES

www.thalesesecurity.com