THALES

Ponemon INSTITUTE

MEXICO ENCRYPTION TRENDS STUDY

July 2018

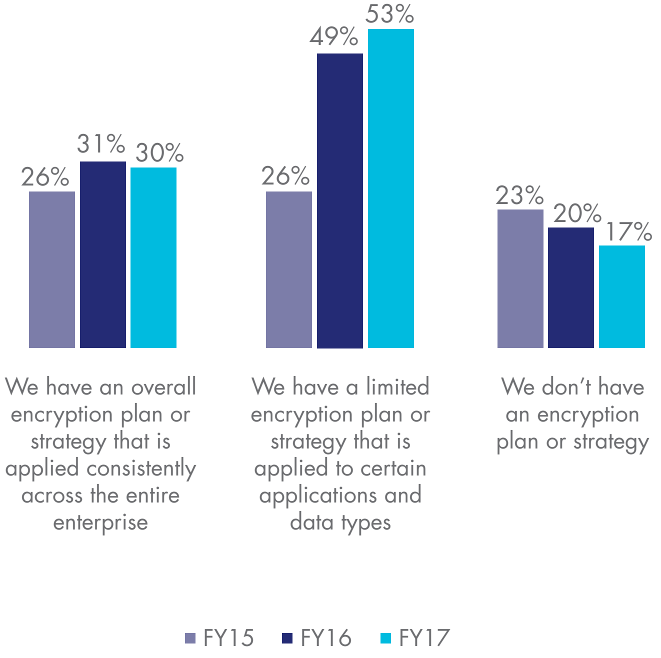
EXECUTIVE SUMMARY

Ponemon Institute is pleased to present the findings of the *2018 Mexico Encryption Trends Study,* sponsored by Thales eSecurity. We surveyed 468 individuals in Mexico to examine the use of encryption and the impact of this technology on the security posture of organizations in this region.

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

As shown in Figure 1, more organizations represented in this research continue to recognize the importance of having an encryption strategy, either an enterprise-wide (30 percent of respondents) or a limited strategy that targets certain applications and data types (53 percent of respondents).

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

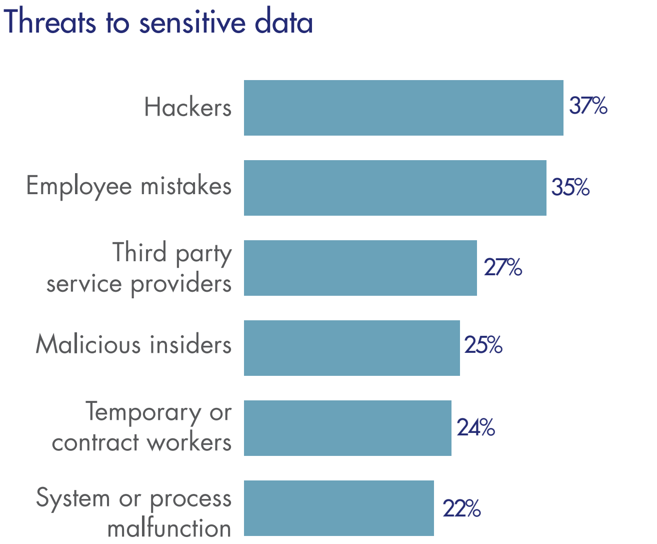


Following is a summary of our key findings. More details are provided for each key finding listed below in the next section of this report.

Influence in directing encryption strategies is dispersed throughout the organization. Twenty-seven percent of respondents say there is no single function that has responsibility for directing encryption strategies and 26 percent of respondents say lines of business are most influential. Only 23 percent of respondents say IT operations is influential.

Which data types are most often encrypted? More companies are encrypting financial records, customer information and payment-related data. Since 2015, fewer companies are encrypting employee/HR data and intellectual property.

Hackers are the most significant threat to sensitive data. The most significant threat to the exposure of sensitive or confidential data is hackers, according to 37 percent of respondents. Thirty-five percent of respondents say employee mistakes and 27 percent of respondents say third party service providers pose the biggest threat.

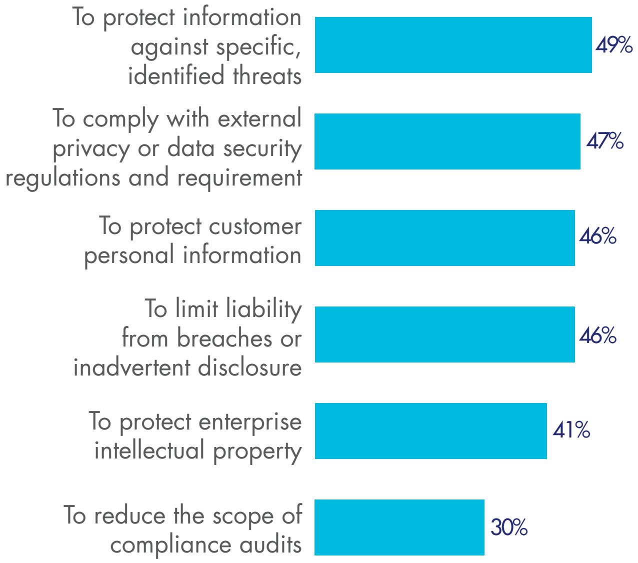


30%

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

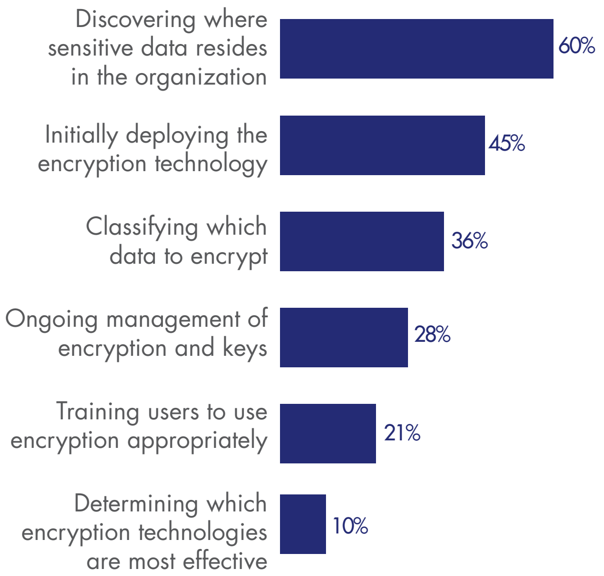
Protection against specific, identified threats is the main driver for using encryption technologies. Several of the primary drivers for using encryption have declined slightly in the past three years, while others have risen. The top four drivers are the protection of information against specific identified threats (49 percent of respondents), compliance with external privacy or data security regulations and requirements (47 percent of respondents), protection of customers' personal information (46 percent of respondents) and to limit liability from breaches or inadvertent disclosure (46 percent of respondents).

What are the drivers for encryption?



Discovering where sensitive data resides in the organization continues to be the biggest challenge. In the past three years, the biggest challenge is the ability to discover where sensitive data resides in the organization (60 percent of respondents) followed by initially deploying the encryption technology (45 percent of respondents). The challenge of training users to use encryption appropriately has declined in the past three years.

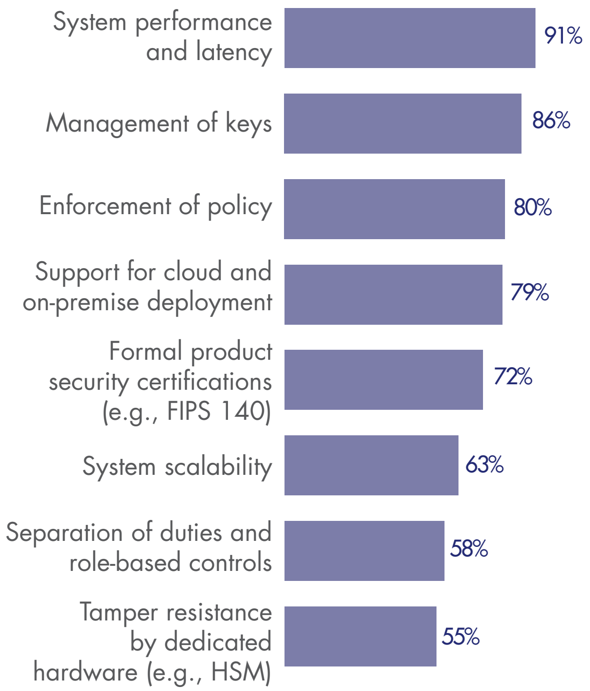
Why organizations are challenged by encryption



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

Certain encryption features are considered more critical than others. In the past three years the following features have increased the most in importance: enforcement of policy, support for cloud and on-premises deployment, separation of duties and role-based controls. System performance and latency and management of keys remain the top two features.

How important are specific features?

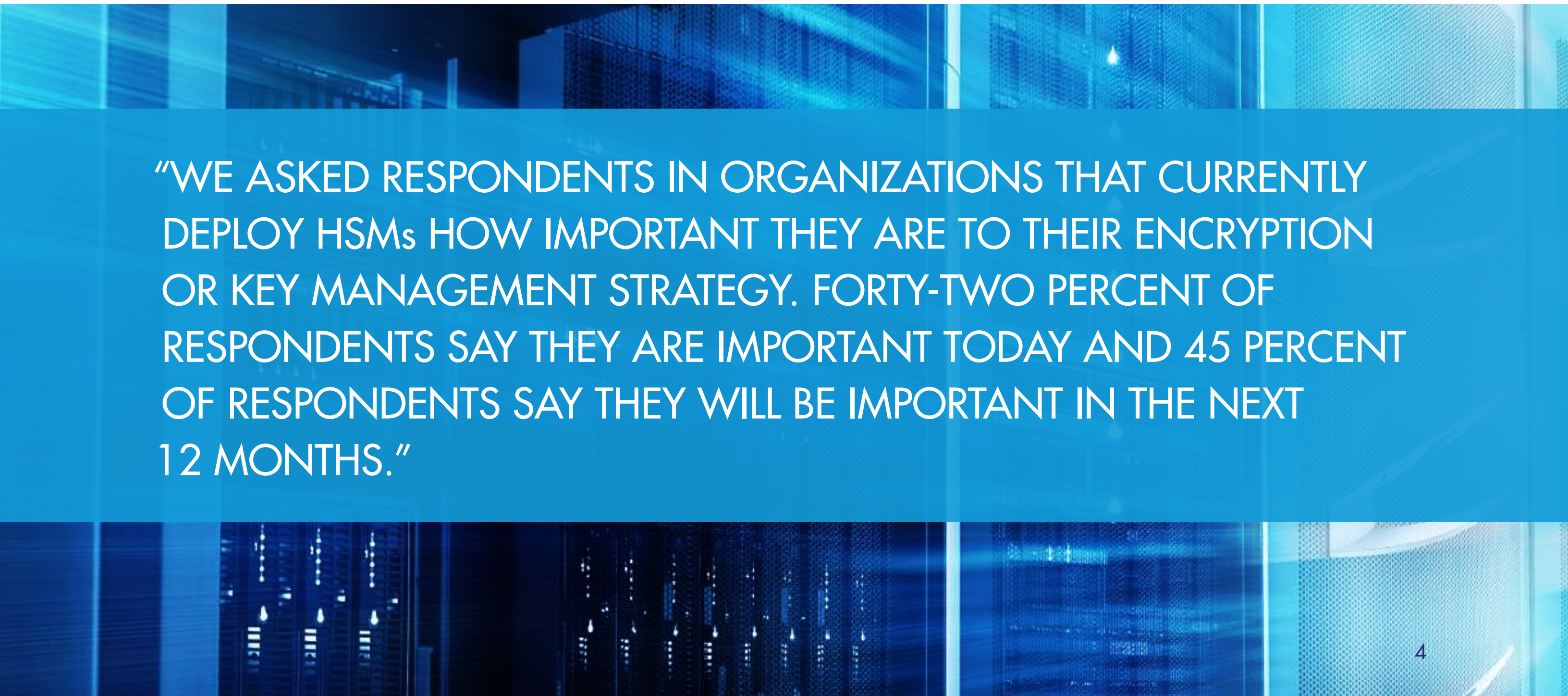


How painful is key management? Using a 10-point scale, respondents were asked to rate the overall "pain" associated with managing keys within their organization, where 1 = minimal impact to 10 = severe impact. Sixty-four percent of respondents chose ratings at 7 or above, thus suggesting a fairly high pain threshold. The reason why the management of keys is difficult is because of a lack of skilled personnel and key management tools are inadequate.

Which keys are most difficult to manage? The pain of managing certain keys has increased significantly. These are: end user encryption keys (e.g., email, full disk encryption), signing keys (e.g., code signing, digital signatures) and payments-related keys (e.g., ATM, POS, etc.). The difficulty in managing end user encryption keys has increased the most.

Key management continues to be a source of pain, with **keys for cloud services rated as most difficult to manage**

The importance of HSMs to an encryption or key management strategy will grow in the next 12 months. We asked respondents in organizations that currently deploy HSMs how important they are to their encryption or key management strategy. Forty-two percent of respondents say they are important today and 45 percent of respondents say they will be important in the next 12 months. Database encryption and public cloud encryption including for BYOK are growing use cases.



"WE ASKED RESPONDENTS IN ORGANIZATIONS THAT CURRENTLY DEPLOY HSMs HOW IMPORTANT THEY ARE TO THEIR ENCRYPTION OR KEY MANAGEMENT STRATEGY. FORTY-TWO PERCENT OF RESPONDENTS SAY THEY ARE IMPORTANT TODAY AND 45 PERCENT OF RESPONDENTS SAY THEY WILL BE IMPORTANT IN THE NEXT 12 MONTHS."

42%

HSMs were rated as either *very important or important* **today** by 42% of respondents

How organizations are using HSMs. Sixty-five percent of respondents say they have a centralized team that provides cryptography as a service and 35 percent of respondents say each individual application owner/team is responsible for their own cryptographic services.

71%

will use **multiple public cloud providers** in the next two years

Most organizations transfer sensitive or confidential data to the cloud. Fifty-two 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 24 percent of respondents plan to in the next 12 to 24 months. Thirty-six percent of respondents say it is the cloud provider who is most responsible for protecting sensitive or confidential data transferred to the cloud.

37%

Encryption in public cloud services grew **11% over last year!**

How is data at rest in the cloud protected? Thirty-seven percent of respondents say encryption is performed on-premise prior to sending data to the cloud using keys the organization generates and manages and 33 percent of respondents say encryption is performed in the cloud using keys generated/managed by the cloud provider.

"THIRTY-SEVEN PERCENT OF RESPONDENTS SAY ENCRYPTION IS PERFORMED ON-PREMISE PRIOR TO SENDING DATA TO THE CLOUD USING KEYS THE ORGANIZATION GENERATES AND MANAGES."

"FIFTY-TWO 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 24 PERCENT OF RESPONDENTS PLAN TO IN THE NEXT 12 TO 24 MONTHS."

About Ponemon Institute

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

About Thales eSecurity

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

About Thales

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

CLICK HERE TO READ THE FULL REPORT

OUR SPONSORS

VENAFI · GEOBRIDGE · CSA cloud security alliance · GuidePoint Security · CRITICALSTART · OASIS

THALES

www.thalesesecurity.com