THALES

Ponemon INSTITUTE

SOUTH KOREA ENCRYPTION TRENDS STUDY

August 2018

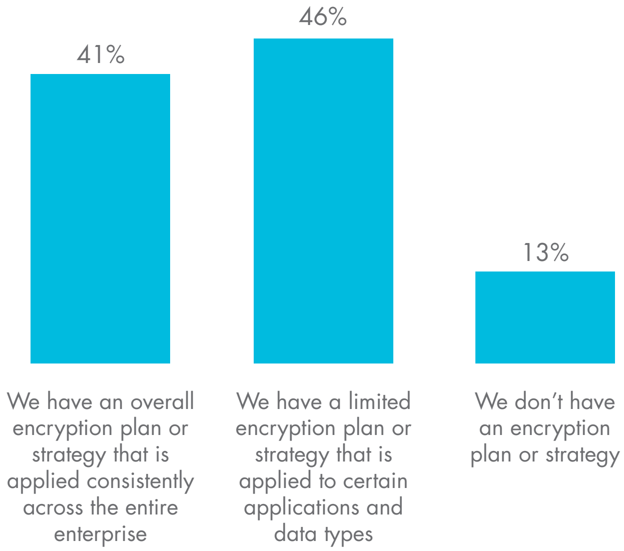
EXECUTIVE SUMMARY

Ponemon Institute is pleased to present the findings of the *2018 South Korea Encryption Trends Study*, sponsored by Thales eSecurity. For the first time, we surveyed 317 individuals in South Korea (hereafter referred to as Korea) 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 South Korea. The 11 countries include: Australia, Brazil, France, Germany, India, Japan, Mexico, the Middle East, the Russian Federation, the United Kingdom, and the United States.[1]

As shown in Figure 1, respondents represented in this research recognize the importance of having an encryption strategy, either an enterprise-wide strategy (41 percent of respondents) or a limited strategy that targets certain applications and data types (46 percent of respondents).

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



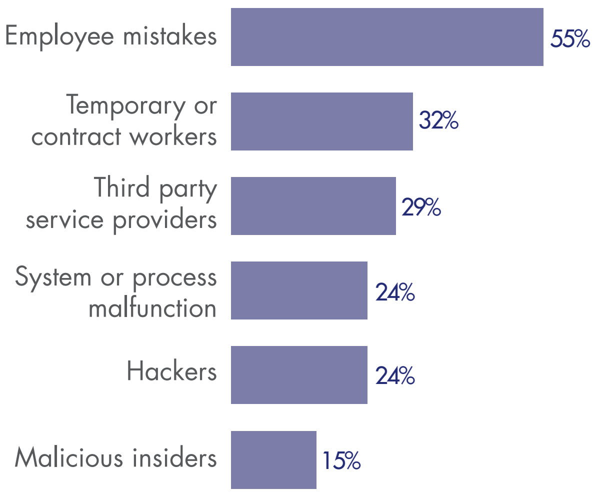
Following is a summary of our key findings. More details are provided in the next section of this report for each key finding listed below.

IT operations has the most influence in directing encryption strategies. While responsibility for the encryption strategy is dispersed throughout the organization, IT operations (43 percent of respondents) has the most influence. Twenty-two percent of respondents say no single function is responsible for encryption strategy.

Which data types are most often encrypted? Most companies are encrypting employee/HR data, followed by financial records 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 55 percent of respondents. Thirty-two percent of respondents say temporary or contract workers pose the biggest threat, and 29 percent of respondents say third party service providers pose the biggest threat.

Threats to sensitive data



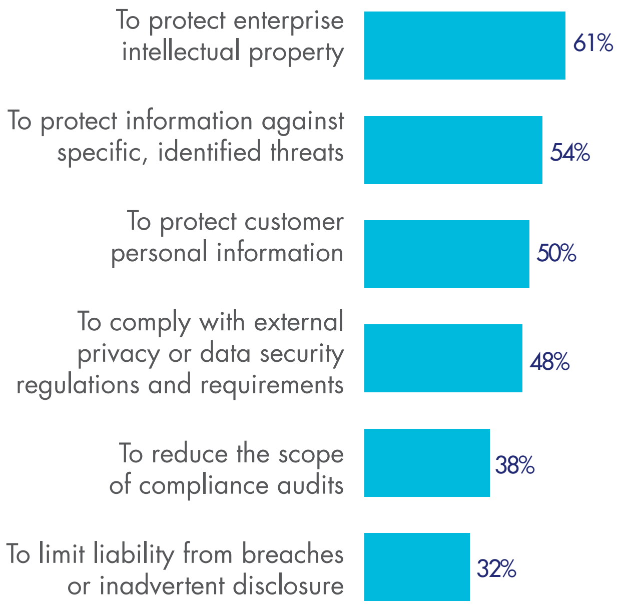
[1] The Middle East region includes the United Arab Emirates and Saudi Arabia.

41%

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

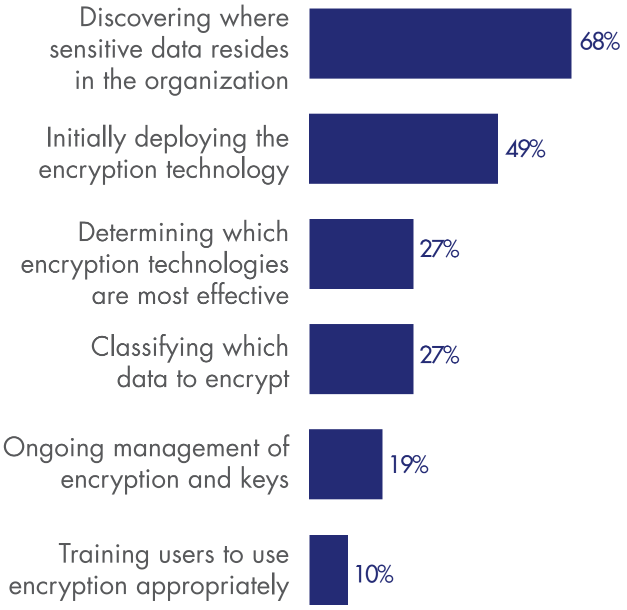
Protection of intellectual property is the main driver for using encryption technologies. Sixty-one percent of respondents say protecting enterprise intellectual property is the largest driver for using encryption technologies. This is followed by protection against specific, identified threats (54 percent of respondents).

What are the drivers for encryption?



Discovering where sensitive data resides in the organization continues to be the biggest challenge. Discovering where sensitive data resides in the organization is the biggest challenge to planning and executing a data encryption strategy, according to 68 percent of respondents. Almost half of respondents (49 percent) say the biggest challenge is initially deploying the encryption technology.

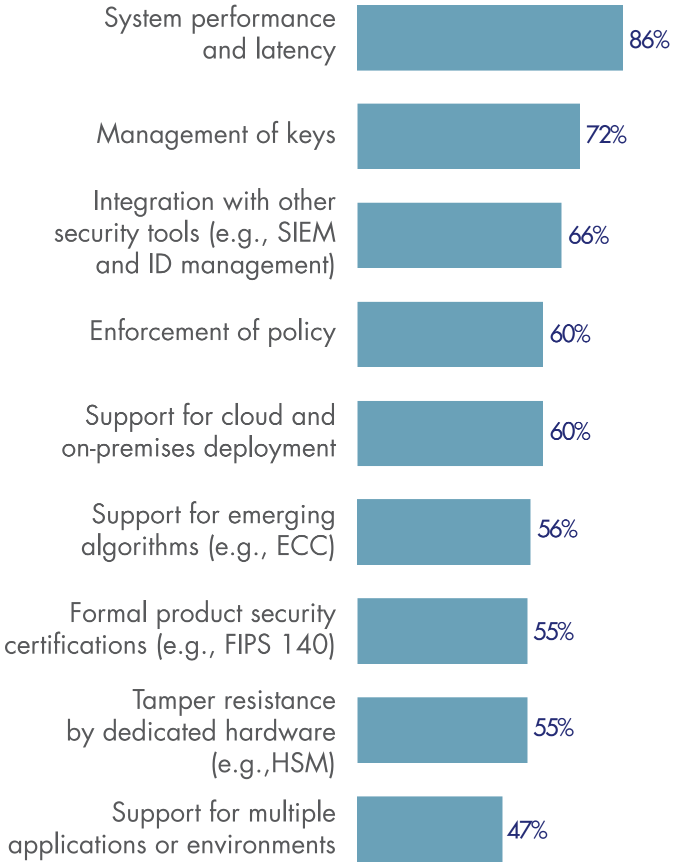
Why organizations are challenged by encryption



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

Certain encryption features are considered more critical than others. Respondents were asked to rate encryption technology features considered most important to their organization's security posture. According to the findings, the following features have the most importance: system performance and latency, management of keys and integration with other security tools (e.g., SIEM and ID management).

How important are specific features?



How painful is key management? More than half (52 percent) of respondents report the management of keys is painful. The top reasons for the pain are: systems are isolated and fragmented, no clear ownership, and lack of skilled personnel. Respondents' companies continue to use a variety of key management systems. The most commonly deployed systems are manual process (e.g., spreadsheet, paper-based) and formal key management policy (KMP).

Which keys are most difficult to manage? The most difficult keys to manage are keys for external cloud or hosted services including Bring Your Own Keys (BYOK), SSH keys and signing keys.

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

The importance of hardware security modules (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-eight percent of respondents say they are important today and 57 percent of respondents say they will be important in the next 12 months. Database encryption, SSL/TLS, blockchain applications and IoT root of trust are growing use cases for HSMs.

48%

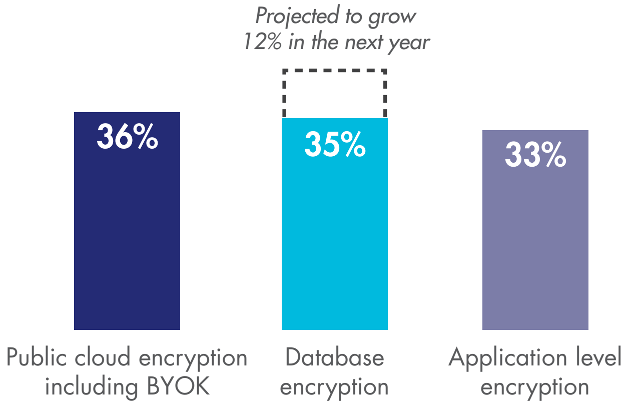
HSMs were rated as either *very important or important* **today** by 48% of respondents

75%

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

How organizations are using HSMs. Sixty-five percent of respondents say they have a centralized team that provides cryptography as a service. The global average is 61 percent. Thirty-five percent of respondents say each individual application owner/team is responsible for their own cryptographic services.

The most prevalent use cases for HSMs



Most organizations transfer sensitive or confidential data to the cloud. Sixty-five percent of respondents say their organizations currently transfer sensitive or confidential data to the cloud (regardless of whether it is encrypted or made unreadable via some other mechanism), and 20 percent of respondents plan to do so in the next 12 to 24 months. Sixty percent of respondents say the cloud provider is most responsible for protecting sensitive or confidential data that is transferred to the cloud.

72%

of respondents either extensively or partially **encrypt in public cloud services**

How is data at rest in the cloud protected? Forty-four percent of respondents say encryption is performed on-premises prior to sending data to the cloud using keys the organization generates and manages and 36 percent of respondents say encryption is performed in the cloud using keys generated/managed by the cloud provider.

"FORTY-FOUR PERCENT OF RESPONDENTS SAY ENCRYPTION IS PERFORMED ON-PREMISES PRIOR TO SENDING DATA TO THE CLOUD USING KEYS THE ORGANIZATION GENERATES AND MANAGES."

"SIXTY-FIVE PERCENT OF RESPONDENTS SAY THEIR ORGANIZATIONS CURRENTLY TRANSFER SENSITIVE OR CONFIDENTIAL DATA TO THE CLOUD (REGARDLESS OF WHETHER IT IS ENCRYPTED OR MADE UNREADABLE VIA SOME OTHER MECHANISM), AND 20 PERCENT OF RESPONDENTS PLAN TO DO SO 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