Thales: Boardrooms demanding action as data security takes centre stage

Thales reveals encryption responsibility is expanding beyond the IT department as organisations take a more nuanced approach to protecting sensitive data

SYDNEY, Australia – November 21, 2017 – High-profile data breaches and new compliance regulations are raising uncomfortable questions in Australian boardrooms, according to the 2017 Thales Encryption Trends Study.

The study, undertaken by independent research firm the Ponemon Institute and sponsored by Thales, takes a detailed look at how Australian organisations are dealing with the increasing need for encryption to protect their most sensitive data. Despite mega breaches happening around the world and here in Australia, the study reveals that local organisations are still behind global counterparts in their urgency to improve their security posture.

Organisations are however accelerating their adoption of encryption strategies, with 32 per cent of respondents saying they are applied consistently across their organisations, up from 22 per cent in 2012. More than half (55 per cent) apply a limited encryption strategy to certain applications and data types but 13 per cent have no strategy at all.

More than half (57 per cent) of respondents said payment data is the most likely to be encrypted, but this is now closely followed by employee and HR data at 55 per cent. The least likely to be encrypted is healthcare data at 23 per cent.

Line of business managers taking control

The department with most influence over encryption strategy is an important finding to emerge from the study. The influence of IT operations has halved in the past five years, from 59 per cent in 2012 to 28 per cent in 2017. On the other hand, the influence of business unit leaders increased to 27 per cent from 20 per cent in the same time period.

While this suggests a maturing of data security, Australia is behind global markets where, for the first time in the study's 12-year history, business unit leaders now had the highest influence over encryption decisions. In Australia, security departments make up 21 per cent while 24 per cent of respondents said no one single function is responsible.

Employee mistakes still the biggest threat

While mega breaches and cyber-attacks are driving executive interest in data security, 80 per cent of respondents said their own employees were the greatest threat to data security. This is a dramatic increase from 38 per cent five years ago. External hackers were named the top threat to data security for only 27 per cent of respondents.

This employee risk is compounded by the fact many organisations are still not sure where sensitive data resides in the business, with 55 per cent saying it this was the number one encryption challenge.

Compliance and the cloud

The main driver for using encryption technologies is compliance with privacy and data security requirements according to 64 per cent of respondents, compared to just 12 per cent five years ago.

With Australia's mandatory data breach notification scheme coming into effect next February, the research suggests organisations know they need to take compliance measures more seriously.

Almost half (46 per cent) of organisations currently transfer sensitive or confidential data to the cloud and a further 30 per cent plan to so within the next two years. Of these, 41 per cent said encryption is performed prior to sending data to the cloud using keys the organisation generates and manages. A further 35 per cent said the encryption is performed in the cloud using keys generated or managed by the cloud provider.

Kelly Taylor, Country Manager for Thales eSecurity Australia and New Zealand said:
"With more organisations increasing their use of cloud services, this year's Australian Encryption Trends Study demonstrates more is being done to protect data. However, it also highlights there is much more work still to do, especially ahead of tighter regulations coming in 2018.

"With more confidential and sensitive data being transferred to the cloud, encryption of that data is going to be more important than ever. But not knowing where that data resides in the organisation is still one of the biggest challenges. It also demonstrates key management tends to live in silos, and many organisations lack the skilled personnel to oversee them, which increases the chance of mistakes."

Mike Burgess, Strategic Cybersecurity Consultant, said:
"With continued reputation damaging data breaches and cyberattacks likely to continue in Australia and around the world, now is the time to act. Theft of data or disruption to data and systems should be expected. The stakes are higher than ever, with many organisations still under-prepared for data breaches. Managing this risk is a leadership issue and accountability must begin at the board level. The Thales Encryption Trends Study shows improvements, but it also illustrates there is much more to do. This means there's an opportunity for security leads to step up and make the case for cybersecurity in their organisation, and for CEO's to listen – it must be taken more seriously from top to bottom."

The Global Encryption Trends Study is now in its twelfth year. The Ponemon Institute surveyed more than 5,000 people across multiple industry sectors in the United States, United Kingdom, Germany, France, Australia, Japan, Brazil, the Russian Federation, Mexico, India, Saudi Arabia and the United Arab Emirates. Australian-specific findings are based on the surveys from 331 executives.

The 2017 Encryption Trends Study can be downloaded via: https://gets.thalesesecurity.com.au/

For industry insight and views on the data security trends check out our blog.

Follow Thales eSecurity on Twitter @Thalesesecurity, LinkedIn, Facebook and YouTube

APPENDIX: Additional Key Findings

- Half said the most common key management system is manual processes (such as spreadsheets), 36 per cent use formal key management policy, and 31 per cent use removable media such as thumb-drives and CDROMs.
- Fifty-eight per cent of respondents believe key management is very painful due to a lack of skilled personnel, isolated or fragmented systems and inadequate key management tools.
- More than half of respondents (58 per cent) use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for encryption, with 37 per cent using application level encryption, 32 per cent using payment transaction processing and 20 per cent using Hardware Security Modules.

- Bring Your Own Key (BYOK) deployments are used by 27 per cent of respondents, with 20 per cent using Cloud Access Security Brokers.
- In the next 12 months, SSL/TLS, database encryption and payment transaction processing are most likely to be deployed.

About Thales eSecurity
Thales eSecurity is the leader in advanced data security solutions and services, delivering trust wherever information is created, shared or stored. We ensure that company and government data is secure and trusted in any environment – on premises, in the cloud, in data centres and in 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 meeting the highest standards of certification for 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.
www.thalesesecurity.com

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 customers all over the world.

Positioned as a value-added systems integrator, equipment supplier and service provider, Thales is one of Europe's leading players in the security market. The Group's security teams work with government agencies, local authorities and enterprise customers to develop and deploy integrated, resilient solutions to protect citizens, sensitive data and critical infrastructure.

Thales offers world-class cryptographic capabilities and is a global leader in cybersecurity solutions for defence, government, critical infrastructure providers, telecom companies, industry and the financial services sector. With a value proposition addressing the entire data security chain, Thales offers a comprehensive range of services and solutions ranging from security consulting, data protection, digital trust management and design, development, integration, certification and security maintenance of cybersecured systems, to cyberthreat management, intrusion detection and security supervision through cybersecurity Operation Centres in France, the United Kingdom, The Netherlands and Hong Kong.

Contact:
Zahra Babuji
Howorth Communications
+61 405 231 236
zahra@howorth.com.au

Constance Arnoux
Thales Media Relations – Security
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com

Liz Harris
Thales eSecurity Media Relations
+44 (0)1223 723612
liz.harris@thales-esecurity.com