Thales, leader in information systems and communications security, announces the publication of its latest 2013 Global Encryption Trends Study. The report, based on independent research by the Ponemon Institute and sponsored by Thales, reveals that use of encryption continues to grow in response to consumer concerns, privacy compliance regulations and on-going cyber-attacks. Meanwhile, there are still major challenges in executing data encryption policy.

More than 4,800 business and IT managers were surveyed in the US, UK, Germany, France, Australia, Japan, Brazil and for the first time this year Russia, examining global encryption trends and regional differences in encryption usage. Results from the Russian survey showed adoption of encryption in the region to be very much in line with the rest of the countries surveyed. The report is now in its ninth year since its launch in 2005.

Key points:
- Steady increase in the deployment of encryption with 35% of organizations having an enterprise wide encryption strategy
- Most organizations deploy encryption to lessen the impact of data breaches
- Key management identified as a major issue by more than half of organizations

News facts:
- Steady increase in the deployment of encryption with 35% of organizations having an enterprise wide encryption strategy
- Most organizations deploy encryption to lessen the impact of data breaches
- The number one perceived threat to sensitive data is employee mistakes rather than external attack
Two biggest challenges faced by organizations executing a data encryption policy are knowing where sensitive data resides and managing the actual technology

Key management identified as a major issue by more than half of organizations

Organizations with the highest security posture are now three times more likely to have a formal encryption strategy than those with the lowest security posture

The results of the study show there has been a steady increase in the deployment of encryption solutions used by organizations over the past nine years with 35% of organizations now having an encryption strategy applied consistently across the entire enterprise compared with 29% last year. The survey also indicated that only 14% of organizations surveyed do not have any encryption strategy compared with 22% last year.

For the first time the primary driver for deploying encryption in most organizations is to lessen the impact of data breaches whereas in previous years the primary concern was protecting the organizations brand or reputation. Of those organizations that believe they have an obligation to disclose data breaches nearly half believe that encrypting their data provides a safe harbour that avoids the need to disclose that the actual breach occurred. The fastest growing reason as to why organizations are deploying encryption is to ensure they meet their commitments to their customers’ privacy with 42% of organizations focusing on their customer’s interests rather than for their own benefit which has increased by 5% compared to last year.

The number one perceived threat to the exposure of sensitive or confidential data remains employee mistakes, according to 27% of respondents. When employee mistakes are combined with accidental system or process malfunctions, concerns over inadvertent exposure outweigh concerns over actual malicious attacks by more than 2 to1. Furthermore, forced disclosures triggered by e-discovery requests now represent the second highest perceived threat to the loss of sensitive data.

When asked about where encryption is used, organizations ranked backup tapes and databases as most important followed by network encryption and laptop encryption. Cloud encryption had a relatively low ranking compared with other encryption use cases ranking outside the top 10.

The two biggest challenges facing organizations executing a data encryption policy were discovering where sensitive data actually resides, reported by 61% of respondents, and the ability to deploy encryption technology effectively, reported by 50% of respondents. Key management was identified as a major issue with more than half of organizations surveyed rating the overall challenge associated with key management as a major issue.

“Encryption usage continues to be a clear indicator of a strong security posture but there appears to be emerging evidence that concerns over key management are becoming a barrier to its more widespread adoption. For the first time in this study we drilled down into the issue of key management and found it emerging as a huge operational challenge. But questions are and should be asked about the broader topics of policy issues and choice of encryption algorithms – especially in the light of recent concerns over back doors, poorly implemented crypto systems and weak key management systems.”

Dr Larry Ponemon, chairman and founder of The Ponemon Institute
management of keys or certificates more than 7 on a scale of 1-10 (10 being highest) and 30% of organizations rated the challenge at 9 or 10. Whilst three quarters of organizations identified key management as a formal discipline within their organization, more than 70% of those organizations failed to allocate dedicated staff or tools to the task of managing keys.

The Key Management Interoperability Protocol (KMIP) standard that allows organizations to deploy centralized key management systems that span multiple use cases and equipment vendors, has already established a relatively high level of awareness among IT and IT security practitioners. KMIP is perceived to be of increasing importance and is expected to contribute to encryption and key management strategies specifically around cloud, storage and application-level encryption. More than half of those surveyed said that the KMIP standard was important in cloud encryption compared with 42% last year.

Hardware security modules (HSMs) are increasingly considered a critical component of a key management strategy. These devices are used to protect critical data processing activities and high value keys and can be used to strongly enforce security polices and access controls.

Download your copy of the new Global Encryption Trends Study
See demonstrations of Thales keyAuthority in the OASIS KMIP interoperability showcase booth #1909.
For industry insight and view on the latest key management trends check out our blog at http://www.thales-esecurity.com/blog
Follow Thales e-Security on Twitter @Thalesesecurity, LinkedIn, Facebook and YouTube

About the 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.

“Whilst key management may be emerging as a barrier to encryption deployment, it is not a new issue. The challenges associated with key management have already been addressed in heavily regulated industries such as payments processing, where best practices are well proven and could translate easily to a variety of other verticals. With more than 40 years’ experience providing key management solutions. Thales is ideally positioned to help organizations re-assess and re-evaluate their crypto security and key management infrastructure and deliver solutions that ensure their integrity and trustworthiness.”

Richard Moulds, VP strategy, Thales e-Security
About Thales e-Security

Thales e-Security is a leading global provider of data encryption and cyber security solutions to the financial services, high technology manufacturing, government and technology sectors. With a 40-year track record of protecting corporate and government information, Thales solutions are used by four of the five largest energy and aerospace companies, 22 NATO countries, and they secure more than 80 percent of worldwide payment transactions. Thales e-Security has offices in Australia, France, Hong Kong, Norway, United States and the United Kingdom.

About Thales

Thales is a global technology leader in the Aerospace, Transportation and Defence & Security markets. In 2012, the company generated revenues of €14.2 billion with 65,000 employees in 56 countries. With its 25,000 engineers and researchers, Thales has a unique capability to design, develop and deploy equipment, systems and services that meet the most complex security requirements. Thales has an exceptional international footprint, with operations around the world working with customers and local partners.

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.

Drawing on its strong cryptographic capabilities, Thales is one of the world leaders in cybersecurity products and solutions for critical state and military infrastructures, satellite networks and industrial and financial companies. With a presence throughout the entire security chain, Thales offers a comprehensive range of services and solutions ranging from security consulting, intrusion detection and architecture design to system certification, development and through-life management of products and services, and security supervision with Security Operation Centres in France and the United Kingdom.