



UK data breaches on the rise despite increase in IT security spend

New Thales research reveals that despite rise in data breaches, UK businesses still prioritise network and endpoint solutions over encryption

London, UK – 24 May 2017 - Thales, a leader in critical information systems, cybersecurity and data security, announces the number of data breaches suffered by UK organisations has increased in the past year, despite a rise in IT security spending.

The [2017 Thales Data Threat Report: European edition](#), which polled 100 IT security professionals from UK organisations, reveals that 63 percent of UK businesses increased IT security spend in 2017 – a marked jump from 2016 (54%). Yet despite this increase in IT security spend, more than two in five UK businesses (43%) were breached last year. A further 84 percent of respondents feel that their organisation is still vulnerable to data threats, with one fifth of UK organisations (20%) reporting that they feel ‘very’ or ‘extremely’ vulnerable.

New technologies, old measures

Nearly all respondents in the report (91%) said they will use sensitive data in an advanced technology environment this year, with cloud environments – SaaS (51%), IaaS (47%) and PaaS (37%) – identified as the leading environments for this usage.

As organisations deploy advanced technologies residing outside the traditional walls of the enterprise, network security solutions become increasingly redundant in stopping modern breaches. Despite this shift, UK organisations continue to invest in traditional security measures, which have worked in the past, to protect data. Nearly half of UK organisations (48%) plan to increase network IT security spending – up from 42 percent in 2016 with the majority of respondents (88%) reporting that they believe network security is ‘very’ or ‘extremely’ effective at protecting data from breaches.

Changing perceptions of encryption

The report illustrated a strong understanding of the benefits of encryption to enable digital transformation using advanced technologies. Nearly half of respondents (49%) identified data encryption and secure digital identities using encryption technologies as critical to enabling safe deployments of IoT.

Encryption was also identified as a critical security practice to meet privacy requirements – including the impending EU General Data Protection Regulation (GDPR). Designed to improve personal data protections and increase organisational accountability for data breaches, [Article 32](#) of the GDPR states that organisations must implement “appropriate, technical and organisational measures to ensure a level of security appropriate to the risk, including [...] encryption of personal data.”

With the cost of non-compliance amounting up to 4 percent of gross worldwide sales, today’s rates of data breaches could result in crippling fines for UK firms when the GDPR comes into effect in May 2018, if data protection is not properly addressed. Consequently, over half of businesses (57%) selected encryption as the top control planned to address requirements outlined in the new ruling.

With the benefits at front of mind, data at rest defences – such as encryption and access control – are planned for the second highest increase in IT security spend, with 45 percent of UK organisations increasing spending in this area (up from 34% last year).

Peter Galvin, vice president of strategy, Thales e-Security says:

“It is certainly encouraging to see that more UK businesses understand the value encryption has in protecting valuable data and enabling digital transformation. But there is still more work to be done in incentivising the remaining 55 percent of UK firms to bolster their security strategies. In today’s increasingly complex threat landscape, robust IT strategies must be in place to protect data in all its forms, wherever it is created, shared or stored.”

To help combat the rising number of data breaches, Thales has provided the following examples of best practice for organisations to adhere to:

- Leverage encryption and access controls as a primary defence for data and consider an ‘encrypt everything’ strategy
- Select data security platform offerings that address a variety of use cases and emphasize ease-of-use
- Implement security analytics and multi-factor authentication solutions to help identify threatening patterns of data use

Download your copy of the 2017 Thales Data Threat Report: European Edition [here](#).

About Thales e-Security

Thales e-Security 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 premise, in the cloud, in data centers 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 e-Security is part of Thales Group. <https://www.thalesecurity.co.uk/>

For industry insight and views on the latest key management trends check out [our blog](#). You can follow Thales e-Security on [Twitter](#), [LinkedIn](#), [Facebook](#) and [YouTube](#).

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 soon in Hong Kong.

Contact:

Dorothee Bonneil
Thales Media Relations – Security
+33 (0)1 57 77 90 89
dorothee.bonneil@thalesgroup.com

Liz Harris
Thales e-Security Media Relations
+44 (0)1223 723612
liz.harris@thales-eseurity.com