Thales: U.S. Federal Government Agencies experience more than 20% increase in data breaches

Government tackling how to best stay secure in midst of digital transformation

San Jose, CALIF. – Feb. 22, 2018 – Thales, a leader in critical information systems, cybersecurity and data security, announces the results of its 2018 Thales Data Threat Report, Federal Edition, issued in conjunction with analyst firm 451 Research. In the past year 57% of federal respondents experienced a data breach. This marks a huge jump from the 2017 report (34% of breached) and the 2016 report (18%). In contrast only 26% of non-U.S. government agencies worldwide experienced a breach this past year.

Click to Tweet: 57% of U.S. federal IT pros say breached in last 12 months, 3x higher than two years ago http://bit.ly/2vHEbt3

The new report finds that 68% of U.S. respondents believe they are 'very' or 'extremely' vulnerable to a data breach, up from 48% in the 2017 report. Among their global government counterparts, however, only 42% claim to be 'very' or 'extremely' vulnerable. While there are a number of factors to consider when addressing U.S. federal government data insecurity – such as budget restraints and issues with staffing – this year a couple stand out.

IT modernization and cloud deployments go hand-in-hand
In May 2017, the Trump administration issued Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The federal government's push for IT modernization – one that has spanned multiple administrations – is also driven in part by concerns about the cost and difficulty of defending outdated legacy systems. "The Report on Federal IT Modernization," issued by the American Technology Council in December, directs agencies to put a new focus on security at the data level, as opposed to the perimeter.

A data-centric security approach is needed largely because of the growing use of commercial cloud services. According to the 2018 report, nearly half (45%) of U.S. federal respondents used more than five Infrastructure-as-a-Service (IaaS) vendors and nearly half (48%) used more than 100 Software-as-a-Service (SaaS) applications. Over two-thirds (72%) of respondents expressed concerns about increased vulnerabilities from shared infrastructures, followed by custodianship of encryption keys (62%) and security breaches in the cloud (68%).

Garrett Bekker, Principal Analyst for Information Security at 451 Research says:
"The massive adoption of cloud computing does not correlate with implementations of data security tools suited to protect these new environments. Although 78% view data-in-motion and 77% view data-at-rest encryption as the most effective tools for protecting data, only 23% of U.S. respondents have implemented encryption in the cloud. Additionally, only 31% claimed cloud computing security was a top spending priority."

Overall security spending is up, but how effective is it?
While cloud computing security is not a top budget priority, almost all (93%) of respondents are increasing spending this year. On the surface this may appear encouraging, but a deeper dive reveals

56% still plan to spend the most on endpoint security and 48% on network security. Only 19% will spend the most on data-centric security solutions, such as encryption and tokenization.

Nick Jovanovic, Vice President of Thales eSecurity Federal, a division of TDSI, says:
"Encryption can be viewed as complex, and the management of encryption keys challenging for organizations dealing with budget and staffing limitations. But federal government agencies can start by selecting encryption and key management technologies that offer a smart, centralized approach and work across clouds, on-premises and in data centers. A good example of this is the 47% of respondents who plan to implement 'bring your own key' solutions to remotely manage their cloud deployments, which will assist them in better protecting and controlling their data."

Please download a copy of the new 2018 Thales Federal Report for more detailed security best practices.

For industry insight and views on the latest data security trends check out our blog. You can follow Thales eSecurity on Twitter, LinkedIn, Facebook and YouTube.

About Thales eSecurity
Thales eSecurity is the 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-premises, in the cloud, in data centres 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 organisation needs to protect and manage its data, identities and intellectual property, and meet regulatory compliance – through encryption, advanced key management, tokenisation, and privileged-user control and high-assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organisation's digital transformation. Thales eSecurity is part of Thales Group.

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:

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