Less than a third of global healthcare organizations remain untouched, as data breaches rise across the industry

2018 Thales Healthcare Data Threat Report reveals pressures to drive digital transformation, while maintaining the security of sensitive information

San Jose, CALIF. – Mar. 5, 2018 – Thales, a leader in critical information systems, cybersecurity and data security, today announces the results of its 2018 Thales Data Threat Report, Healthcare Edition, revealing only 30% of global healthcare organizations have remain untouched by a data breach. Worryingly 39% of these organizations have been breached in the last year alone, while the majority of respondents (70%) reported being breached in the past – a 17% increase from the 2016 report. Issued in conjunction with analyst firm 451 research, the findings also highlight the negative impact cyber criminals are having, with over half (55%) feeling 'very' or 'extremely' vulnerable to data breaches.

Click to Tweet: 70% of global #healthcare orgs report being breached in past in @thalesesecurity #2018DataThreat http://bit.ly/2FfSKwM

Digital transformation: Enabling better healthcare, but creating risks

In an effort to provide more efficient services – and with an eye towards cutting costs – the healthcare industry has more recently been turning its attention towards embracing digitally transformative technologies, including cloud, big data, Internet of Things and containers. These technologies allow organizations to better create and manage data, as well as store critical information more efficiently.

Almost all (93%) of global respondents reported using these technologies with sensitive data. With each new technology comes unique data security challenges that must be addressed, as they increase the attack surface available. Among some of the more notable findings from this year's report:

- All (100%) global respondents surveyed are leveraging cloud technologies, with 54% using three or more cloud vendors for infrastructure (IaaS) as opposed to having it onsite
- One-third (33%) of global respondents are using more than 50 cloud based software applications (SaaS); and 54% are using three or more cloud based platform (PaaS) environments
- Almost all (99%) of global respondents are using big data; 94% are working on or using mobile payments, and 94% have a blockchain project implemented or are in the process of implementing one
- 96% are leveraging IoT technologies, which may include internet-connected heart-rate monitors, implantable defibrillators and insulin pumps

Consequently, these organizations have emerged as a prime target for hackers, putting valuable medical data at risk. While a stolen credit card has a time-limited value, PHI and electronic medical records (EMR) are packed with immutable data that can, and do, fetch hundreds of dollars per stolen record on illegal online markets.

Compliance playing larger role in influencing global healthcare security attitudes

Past global healthcare reports have shown the U.S. to place more of an emphasis on compliance, compared to its global counterparts. This is primarily driven by a privately focused healthcare system, which contends with a complex web of regulations and standards. The effectiveness of a compliance-based strategy is debatable: 77% of U.S. healthcare respondents reported at least one breach at some

time in the past, making it the most breached among all U.S. verticals polled in this year's report. Despite U.S. struggles, 64% of global healthcare respondents still believe compliance requirements are 'very' or 'extremely' effective at preventing data breaches, with compliance ranking first among global healthcare respondents as a driver of security spending (51%), higher than any other sector and higher than the U.S. (44%).

Encryption viewed as critical – but does spending reflect this?
While 83% of global healthcare respondents plan to increase spending on security (a number that is above the global average), only 40% of global respondents are increasing spending for data-at-rest security tools. This stance is puzzling, when reflecting on other findings from the report. For example, the looming deadline for the General Data Protection Regulation (GDPR) means data sovereignty is top of mind for most international companies. Globally, encryption is the top choice for complying with privacy regulations (36%). Unlike their U.S. counterparts, who ranked data-at-rest defenses second-to-last in terms of effectiveness, 76% of global healthcare respondents also ranked data-at-rest defenses (such as encryption or tokenization) as the number one tool for protecting data (tied with data-in-motion defenses).

Peter Galvin, Chief Strategy Officer, Thales e-Security says:
"When it comes to data security, the global healthcare industry is increasingly under duress, which is why some of this year's findings are so counterintuitive. For example, 63% of global respondents are investing money in endpoint security, even though it offers little help in protecting data once perimeters have been breached. Data security spending needs to match healthcare's reality – which is that of an industry embracing digitally transformative technologies – in the form of investments in encryption solutions offering protection to known and unknown sensitive data that has moved beyond the traditional four walls of the healthcare environment."

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

Visit Thales at booth #8500-13, HIMSS Conference, Las Vegas, Nevada, March 5-9, 2018.

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