THALES

2018 Thales Healthcare Data Threat Report: 48% of U.S. Healthcare Organizations Breached

Percentage reporting breaches more than doubled from 2016 report

San Jose, CALIF. – Mar. 5, 2018 – Thales, a leader in critical information systems, cybersecurity and data security, announces the results of its 2018 Thales Data Threat Report, Healthcare Edition, issued in conjunction with analyst firm 451 Research. Nearly half (48%) of U.S. healthcare respondents reported getting breached in the last year alone – more than 2.5X the rate from only two years ago – and 56% report feeling either 'very' or 'extremely' vulnerable to data breaches. Further, more than three-fourths (77%) of U.S. healthcare respondents reported at least one breach at some time in the past. This is the highest percentage among all U.S. vertical industries polled in this year's report.

Click to Tweet: Only 23% of U.S. #healthcare orgs haven't been affected by a data breach, according to @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, the IoT and containers. These technologies allow organizations to better create and manage data, as well as store critical information more efficiently.

Almost all (95%) 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%) U.S. respondents surveyed are leveraging cloud technologies, with 63% using three or more cloud vendors for infrastructure (IaaS) as opposed to having it onsite
- Over half (58%) of U.S. respondents are using more than 50 cloud based software applications (SaaS); and 52% are using three or more cloud based platform (PaaS) environments
- Almost all (96%) of U.S. respondents are using big data; 90% are working on or using mobile payments, and 92% have a blockchain project implemented or are in the process of implementing one
- 92% are leveraging IoT devices, which may 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 continues to play role in influencing U.S. healthcare security attitudes

In the U.S., the Health Insurance Portability and Accountability Act (HIPAA) is the most impactful and well-known healthcare regulation. While HIPAA covers off on audit trail requirements, secure archival of protected health information (PHI), tightly controlled access to PHI, and many other regulations, it just doesn't provide organizations with detailed instructions on how to accomplish these requirements. Despite HIPAA's limitations, 70% of U.S. respondents believe compliance requirements are 'very' or 'extremely' effective at preventing data breaches. Almost half (44%) of U.S. respondents report compliance is a top spending driver. While sizable, that number has dropped considerably from last year (57%).

Encryption viewed as critical – but does spending reflect this?
In the U.S., encryption is the top choice for complying with privacy regulations (42%), followed distantly by tokenization (19%) and migrating customer data (10%). Encryption tools are also three of the top four data security tools being deployed this year, with 65% of U.S. respondents leveraging data masking; 65% identity and access management; 59% database and file encryption; and 57% encryption in the cloud.

Despite encryption's proven effectiveness at protecting large data sets, many organizations remain stubbornly focused on network and endpoint security. While the federal sector (77%), financial services (88%), and retail industries (89%) recognize encryption as the first or second most effective data security tool, 75% of U.S. healthcare respondents ranked data-at-rest defenses (such as encryption or tokenization) second to last in effectiveness. At 34%, data-at-rest defenses are still at the bottom of the spending priority list, as well.

Peter Galvin, Chief Strategy Officer, Thales e-Security says:
"When it comes to data security, the U.S. healthcare industry is increasingly under duress, which is why some of this year's findings are so counterintuitive. For example, 62% of U.S. respondents are investing money in endpoint security, even though it's rated least effective at protecting data. An alarmingly high number of U.S. respondents (39%) also report storing sensitive data in SaaS apps. Data protection strategies need to match U.S. healthcare's reality – which is that of an industry embracing digitally transformative technologies – in the form of encryption solutions offering protection to 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