Thales: Data Breaches at U.S. Financial Services Businesses on the Rise

Nearly 9 out of 10 surveyed financial IT professionals feel their business is vulnerable to data threats

SAN JOSE, Calif. – Oct. 17, 2017 –Thales, a leader in critical information systems, cybersecurity and data security, announces the results of its 2017 Data Threat Report, Financial Services Edition. Issued in conjunction with 451 Research, the report reveals 42% of U.S. financial services organizations have experienced a breach in the past. Additionally, 12% were victims of multiple data breaches.

Click to Tweet: 42% of U.S. #finserv IT pros have experienced a data breach #2017DataThreat http://bit.ly/2kBv4tm

Hackers zero in on financial businesses
As the primary repositories and channels of the world's financial data, financial services organizations are an ongoing target for cybercriminals. While these breach numbers may be unsurprising at face value, they do paint a picture of an industry contending with a more aggressive threat landscape. For example, 24% of organizations experienced a breach in the past year – a number that jumped from 19% in 2016. 86% of respondents also believe their organizations are vulnerable to data threats.

Digital transformation shaping, challenging financial data security
Many financial organizations are making the leap from legacy systems to technologies such as cloud, big data, container, and IoT solutions reflecting changing consumer preferences and marketplace pressures. While almost all (96%) respondents will use sensitive data in an advanced technology environment this year, 47% are deploying these technologies in advance of having appropriate levels of data security in place. With large volumes of data and applications moving to the cloud, 53% of respondents are most concerned about shared infrastructure vulnerabilities and lack of data-location control, with security breaches at the cloud service provider (CSP) coming in second at 52%.

Regulation top driver for encryption
In what is already a heavily regulated industry, there are now more than 100 national data privacy and sovereignty regulations. There is a strong understanding among those surveyed of how encryption can help protect critical data. Of the two-thirds of respondents affected by data privacy and sovereignty regulations and laws, 70 percent say encryption is the top control planned to address these requirements.

Garrett Bekker, principal analyst for information security at 451 Research says:
"While the financial sector has made substantial technological advances, it's still tied to security solutions that worked in the past but aren't necessarily the most effective at stopping modern attacks. There are a number of data security technologies – such as encryption and key management solutions – that could arguably do a better job of protecting data, particularly data being used in cloud, big data and IoT environments."

Peter Galvin, vice president of strategy, Thales e-Security says:
"Data breaches continue to hit the headlines and, as recently illustrated by the Equifax breach, the financial services industry is a prime target for hackers. As digitization continues to transform the industry's online infrastructures it is critical organizations implement data security solutions that follow the data – wherever it is created, shared or stored."

Other top findings from the 2017 Data Threat Report, Financial Edition:

- 78% of respondents will increase their IT security spending.
- Privileged users are the top internal data-security threat as selected by 61 percent of respondents, followed by executive staff (40 percent).
- When it comes to external threats, cyber-criminals are No. 1 (52 percent), followed by cyber-terrorists (18 percent) and nation-states (14 percent).
- A substantial majority (84 percent) of respondents reported use of IoT technologies this year.

Best practices and recommendations

Financial services organizations seeking ways to meet compliance and adopt advanced technologies—all while remaining secure—should:

- select data security platforms that address a variety of use cases, emphasize ease-of-use, and offer encryption, enterprise key management, access control and security intelligence to avoid the intricacy and high costs of implementing multiple data-security solutions;
- invest in security tools that include automation to reduce complexity; and
- implement security analytics and multi-factor authentication solutions to help identify threatening patterns of data use.

Download a copy of the 2017 Thales Data Threat Report, Financial Services Edition for more detailed security best practices.

Follow Thales e-Security on Twitter @Thalesesecurity, and on LinkedIn, Facebook and YouTube.

About Thales e-Security

Thales e-Security 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-premise, in the cloud, in data centers 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 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 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.

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 e-Security Media Relations
+44 (0)1223 723612
liz.harris@thales-esecurity.com