Thales: data breaches skyrocket with 50% of retailers experiencing a breach in the last year, up from 19% the prior year

Although 84% plan to increase IT security spending, report indicates greatest spending plans are for defenses that are ranked least effective

San Jose, CALIF. – July 18, 2018 – Thales, a leader in critical information systems, cybersecurity and data security, announces the results of its 2018 Thales Data Threat Report, Retail Edition. According to U.S. retail respondents, 75% of retailers have experienced a breach in the past compared to 52% last year, exceeding the global average. U.S retail is also more inclined to store sensitive data in the cloud as widespread digital transformation is underway, yet only 26% report implementing encryption – trailing the global average.

Click to Tweet: Three-quarters of U.S. retailers have experienced a data breach, half in the last year #2018DataThreat https://bit.ly/2u6K5G6

Year-over-year breach rate takes a turn for the worse

While last year's report showed an encouraging decrease in breaches, this year U.S. retail data breaches more than doubled from 19% in the 2017 survey to 50%. This massive increase drove U.S. retail to be the second highest vertical polled to experience a data breach in the last year, ahead of healthcare and financial services and only slightly behind the U.S. federal government.

Digital transformation brings increased risks to data

According to the report, 95% of U.S. retail organizations will use sensitive data in an advanced technology environment (such as cloud, big data, IoT and containers) this year. More than half believe that sensitive data use is happening now in these environments without proper security in place. Each of these technology environments comes with unique security challenges. As the attack surface increases, unique data security challenges need to be addressed.

Garrett Bekker, principal analyst for information security at 451 Research says:

"These increases come as no surprise to retailers. While nearly 95% of retailers acknowledge vulnerability to data breaches, now almost half recognize they are extremely vulnerable. This is an increase of 30% from the previous year. While this trend can be partially attributed to U.S. retailers aggressively pursuing a multi-cloud strategy, these organizations continue, year after year, to spend on the same security solutions that worked for them previously. With increasingly porous networks and expanding use of external resources (SaaS, PaaS and IaaS most especially), traditional endpoint and network security are no longer sufficient to protect sensitive data."

The increase in attacks against the retail sector calls into question why spending on data security isn't more significant. Ironically, in the U.S., the traditional concerns about data security related to perceived

complexity and business performance impact are now outpaced by a perceived lack of need, which was cited by 52% of respondents. Although not exactly the same globally, a lack of organizational buy-in was tied to 41% not perceiving a need for data security. The message here is that management needs a sense of urgency, and security professionals must do a better job of selling the importance of data security.

Security spending is up but not aligning with risk

The good news is that U.S. retail organizations are responding to the ever-increasing threat with 84% citing plans to increase IT security spending and 28% noting the increase would be significant. The bad news is that spending is not going to what respondents believe are the most effective defenses.

The retail sector recognizes the need for encryption to protect sensitive data. Forty-nine percent require encryption to increase cloud usage and 44% need system level encryption and access controls to expand the use of big data. More than half (52%) believe encryption (along with anti-malware tools) is needed to drive IoT adoption. This is in addition to encryption being the number one choice to satisfy compliance and data security laws such as GDPR, Korea's PIPA and APPI in Japan.

Seemingly contradicting themselves, both U.S. and global retail ranked endpoint and mobile defenses as those that will get the largest spending increase (72% U.S.; 52% global)) even though they rank them the least effective. A bright spot is that more organizations are recognizing the threat to cloud data and with that 49% of respondents have ranked cloud at the top of their IT security spending priorities.

Peter Galvin, chief strategy officer, Thales eSecurity says:

"This year's significant increase in data breach rates should be a wakeup call for all retail organizations. Digital transformation is well underway and the business benefits of the cloud, big data, IoT and mobile payment technologies are compelling and fueling widespread adoption. However, with the flow of sensitive data through all of these disparate platforms and technologies, the attack surface increases exponentially and with it the risk of a data breach."

Other key findings:

- 67% of U.S. retailers are planning to implement database and file encryption this year
- 2 of the top 3 tools needed for additional cloud use are encryption with enterprise key control or cloud provider key management
- For the first time, compliance is not identified as one of the top 5 security spending drivers

Please download a copy of the new 2018 Thales Data Threat Report, Retail Edition for more detailed security best practices at https://bit.ly/2u6K5G6

Industry insight and views on the latest data security trends can be found on the Thales eSecurity blog at blog.thalesesecurity.com.

Follow Thales eSecurity on Twitter @Thalesesecurity, and on LinkedIn, Facebook and YouTube.

About Thales eSecurity

Thales eSecurity is a 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

The people we all rely on to make the world go round – they rely on Thales. Our customers come to us with big ambitions: to make life better, to keep us safer. Combining a unique diversity of expertise, talents and cultures, our architects design and deliver extraordinary high technology solutions. Solutions that make tomorrow possible, today. From the bottom of the oceans to the depth of space and cyberspace, we help our customers think smarter and act faster - mastering ever greater complexity and every decisive moment along the way. With 65,000 employees in 56 countries, Thales reported sales of €15.8 billion in 2017.

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