THALES

451 Research

2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

RETAIL EDITION

RESEARCH BRIEF

#2017DataThreat

TABLE OF CONTENTS

OUR SPONSORS

INTRODUCTION

The unbroken string of high profile data breaches serves as stark proof that data on any system can be attacked and compromised. With each new computing paradigm shift – cloud, Big Data, IoT, and so on – come new security vulnerabilities to be exploited. It's no surprise that the security industry overall now tallies in excess of 1,500 vendors by 451 Research's count, with as many as nine new startups per month and roughly 10 new security categories created each year.

Thus, it is troubling that both attitudes as well as security strategies may not be keeping up with many emerging threats. In the Global Edition of the *Thales 2017 Data Threat Report*, nearly two thirds (63%) of respondents indicated that their organizations deploy new technologies such as cloud, big data, IoT and containers in advance of having the security in place to protect them. With retail, that figure is even more sobering, soaring to 80% in global retail organizations (specifically located outside the U.S.) – though it is much lower (55%) in U.S. retail. This may be due in part to heavy speed-to-market initiatives in the hotly contested retail space.

The retail sector faces unique challenges, certainly in the U.S., as brick and mortar sales drop quicker than expected and more and more sales move online, where data has greater exposure. This occurs at a time when, across virtually all vertical sectors, more and more enterprise data is being created, transported, processed and stored outside the corporate network boundaries. Retail in particular is often characterized by a massive vendor matrix to support highly complex global supply chains.

In this vertical market version of the *Thales Data Threat Report*, we'll focus directly on the retail market and its unique characteristics which, for the first time, features a breakout between U.S. retail and global retail respondents. As will be seen, the report reflects often significant differences between these two sets of respondents. This report also reflects specific concerns security professionals have regarding the effectiveness of security tools and compliance mandates, as well as the security implications associated with new technology environments such as cloud, Big Data, IoT and, this year, containers.

The *2017 Thales Data Threat Report* is based on a survey conducted by 451 Research during October and November of 2016. We surveyed 1100 + senior security executives from across the globe, including more than 100 respondents in key regional markets in the U.S., U.K. Germany, Japan, Australia, Brazil and Mexico, and in key segments such as Federal Government, Retail, Finance and Healthcare.

"NEARLY TWO THIRDS (63%) OF RESPONDENTS INDICATED THAT THEIR ORGANIZATIONS DEPLOY NEW TECHNOLOGIES SUCH AS CLOUD, BIG DATA, IOT AND CONTAINERS IN ADVANCE OF HAVING THE SECURITY IN PLACE TO PROTECT THEM."

KEY FINDINGS:

- Results from IT security professionals at U.S. retailers reflect a mix of good news, but some bad news as well. As for good news, only 19% of U.S. retail respondents reported being breached in the last year, an improvement from the 22% rate reported in last year's report, and significantly less than the global average (26%). Retail was the only U.S. vertical measured that improved their year over year breach rate.

- More good news: Only 19% of U.S. retail respondents report feeling 'very' or 'extremely' vulnerable to security threats – the lowest of any respondent category and down from 39% in last year's report, compared with 39% of global retail and 30% of all global respondents.

- On the not-so-good news side, 43% of global retail (excluding U.S. respondents) reported that their organization encountered a data breach in the last year, which was the highest reported breach rate of any vertical or geographic category surveyed other than Australia (44%).

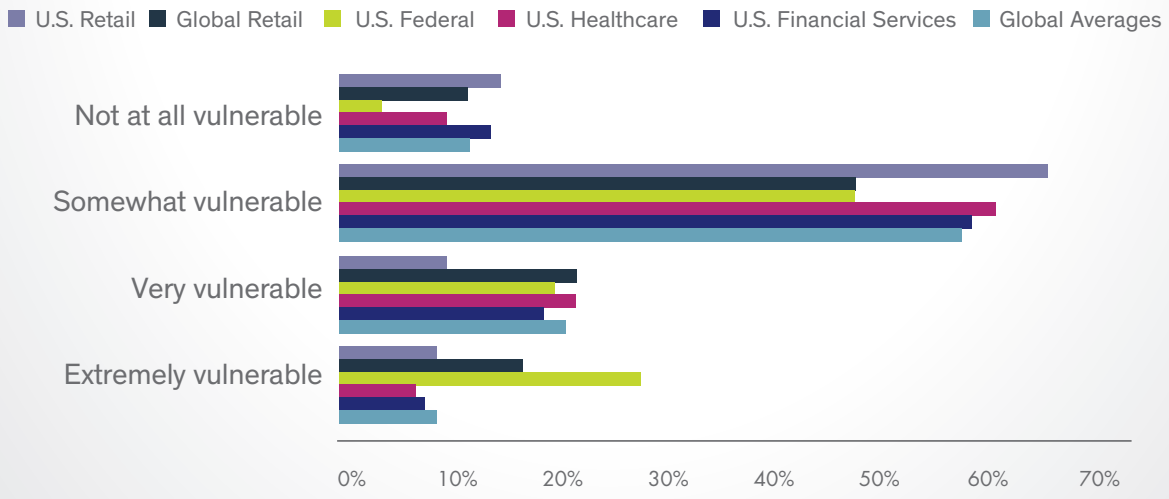
- Complexity (44%) emerged as U.S. retail's main barrier to securing sensitive data, which is also the top barrier cited by all global respondents (50%). For global retail, budget constraints top the list of barriers at 53%.

- Some 53% of U.S. retail say their organizations are deploying advanced technologies ahead of having adequate security in place, compared with 63% of all global respondents and a much higher 80% in global retail.

- U.S. retail is also less likely to store sensitive data in advanced technologies than are respondents in all other global and vertical markets. To secure these nascent advanced environments, U.S. Retail favors protecting sensitive data within these environments with encryption. For example, encryption was selected as the most desired security control to expand their organization's use of IoT platforms (64%) and Containers (56%).

Feelings of Vulnerability

Only 19% of U.S. retail organizations feel very or extremely vulnerable whereas 39% of retail organizations globally feel the same



"ONLY 19% OF U.S. RETAIL RESPONDENTS REPORTED BEING BREACHED LAST YEAR, AN IMPROVEMENT FROM LAST YEAR'S 22% RATE, AND SIGNIFICANTLY LESS THAN THE GLOBAL AVERAGE (26%)."

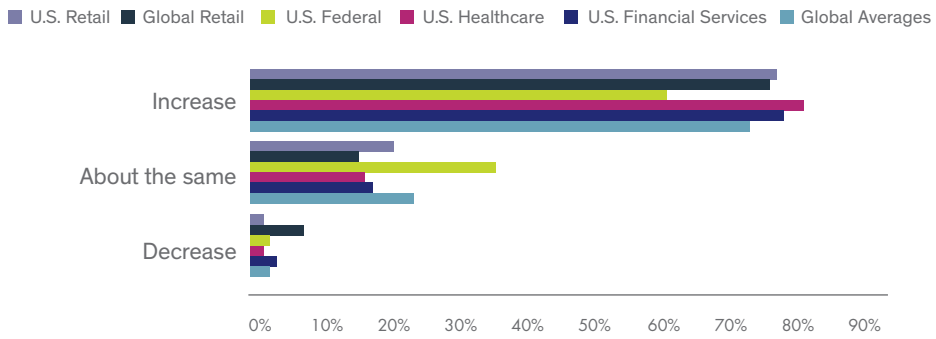
THE GOOD NEWS

On the positive side, U.S. retail is upping security spending this year, with 77% of respondents indicating planned increases, a marked increase from 61% a year ago. It is largely in line with global retail (76%) and all global respondents (73%). Additional good news is that only 19% of U.S. retail reported being breached last year, well below the overall global average of 26% and an improvement from a 22% rate in last year's report.

"A staggering 43% of global retail respondents reported a breach in the past year alone, approaching twice the global average of 26%."

Security Spending in Next Twelve Months

Most retail organizations plan to increase their security spending over the next 12 months



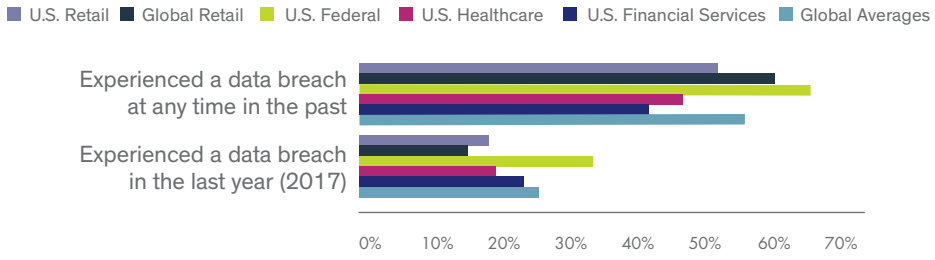
THE NOT-SO-GOOD NEWS

Breach results were not so rosy for global retail, however – a staggering 43% of global retail respondents reported a breach in the past year alone, approaching twice the global average. To provide some perspective, the next-highest breach response was U.S. federal, a full 11 points lower at 34%. Overall, 52% of U.S. retail have been breached at some point, below both the global average (56%) and the global retail figure (60%).

"Only 19% of U.S. retail feel 'very' or 'extremely' vulnerable to security threats, far less than the overall global average of 30% and the much higher global retail (39%)."

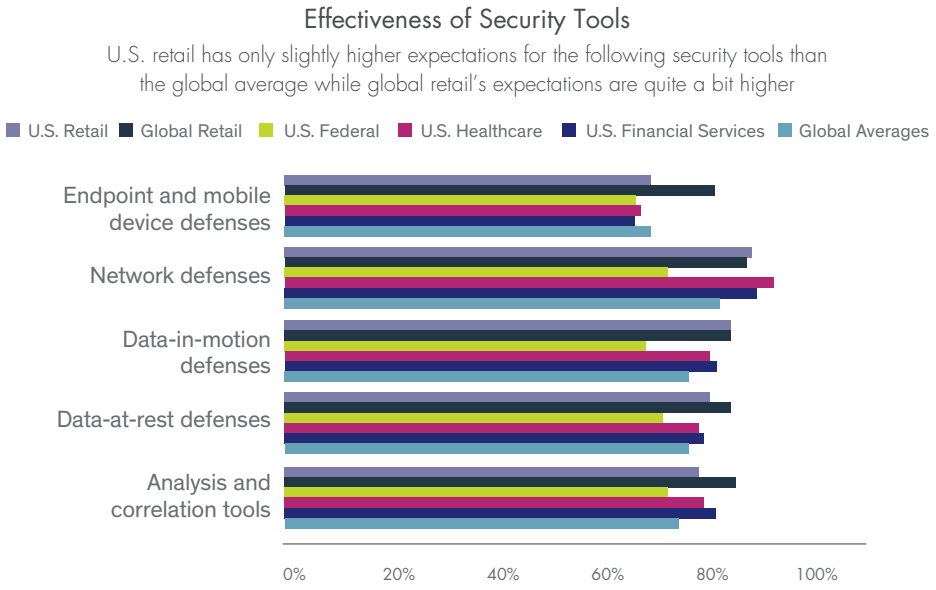
Data Breaches Experienced

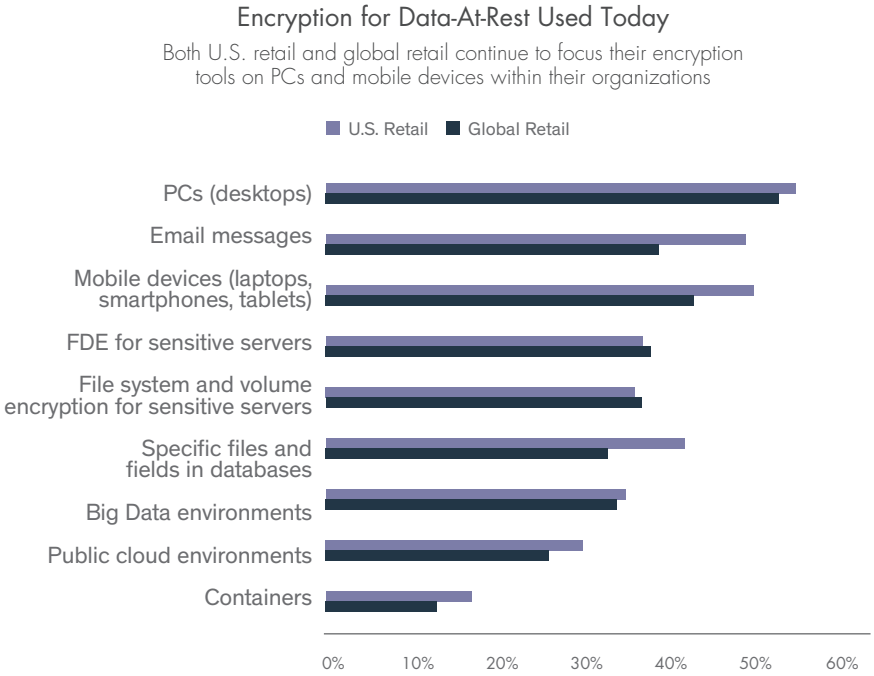
Where U.S. retail saw fewer data breaches than the global average last year, global retail saw almost twice as many



Given the low incidence of breaches, it is not surprising that only 19% of U.S. retail feel 'very' or 'extremely' vulnerable to security threats, far less than the overall global average of 30% and the much higher global retail (39%). Some 88% of U.S. retail report feeling some vulnerability, mirroring the overall global average.

As we discussed at length in our global report, the growth of new technologies like cloud, IoT, containers and big data have arguably rendered traditional security defenses like network and endpoint security less effective. Yet old habits die hard in security, and like other verticals and regions, both U.S. and global retail rank network security as the most effective at preventing data breaches (88% U.S. retail, 87% global retail), and also plan on spending the most on network security (67% each), ahead of the global average of 62%. In contrast, both U.S. and global retail rank data-at-rest security near the bottom in terms of effectiveness (80% and 84%), and also spending plans (49% and 44%, respectively).



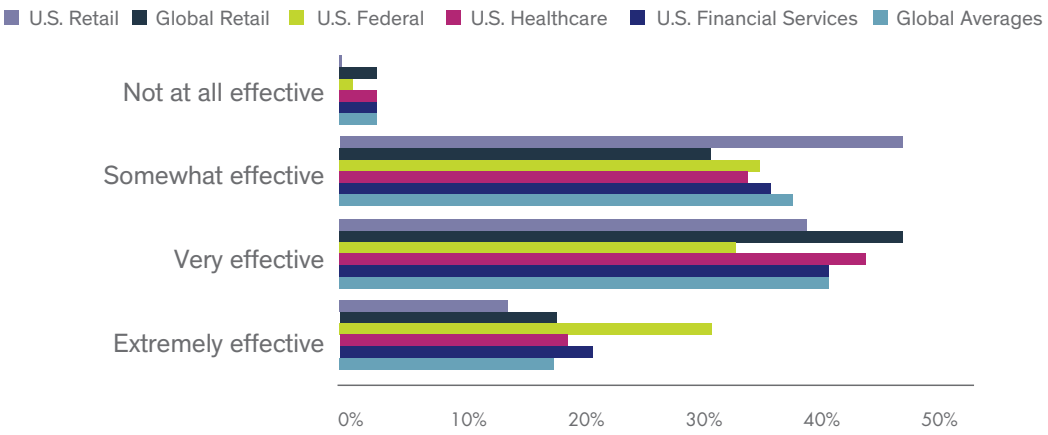


In line with our global results, it is not surprising that complexity, or at least the perception of being complex, is the top barrier to adopting data security for both U.S. retail (44%) and by overall global respondents (50%). But for global retail, lack of budget hampers data security efforts the most, cited by 53% as the top barrier, edging out complexity (49%).

Compliance remains the number one reason for spending on security globally (44%), by a comfortable margin over implementing security best practices (38%). Though compliance remains a top spending driver for both U.S. retail (41%) and global retail (44%), best practices rises to the top for U.S. retail (47% from 40% in 2016), and increased use of cloud resources (46%) – a new response for this year's survey – gained the top slot for global retail. Given the widespread impact of the PCI Data Security Standard (PCI DSS) in retail, we are somewhat encouraged to see other motivations for spending gaining ground. It's also worth noting that U.S. retail had the lowest ratings (53%) for compliance being 'very' or 'extremely' effective at securing data, a large drop from 65% a year ago and below the 59% global average; global retail, however, still maintains a sanguine outlook on compliance (65%), revealing yet another area of significant divergence between U.S. and global retail. Compliance does not necessarily equate to security. Compliance and regulatory edicts often fall behind the contemporary threat environment, which is highly dynamic. This is as true in retail as it is in some of the more highly regulated vertical markets, such as financial services and healthcare.

Compliance Requirement Effectiveness at Preventing Data Breaches

Global retail has much higher expectations for compliance requirement effectiveness than U.S. retail or the global average

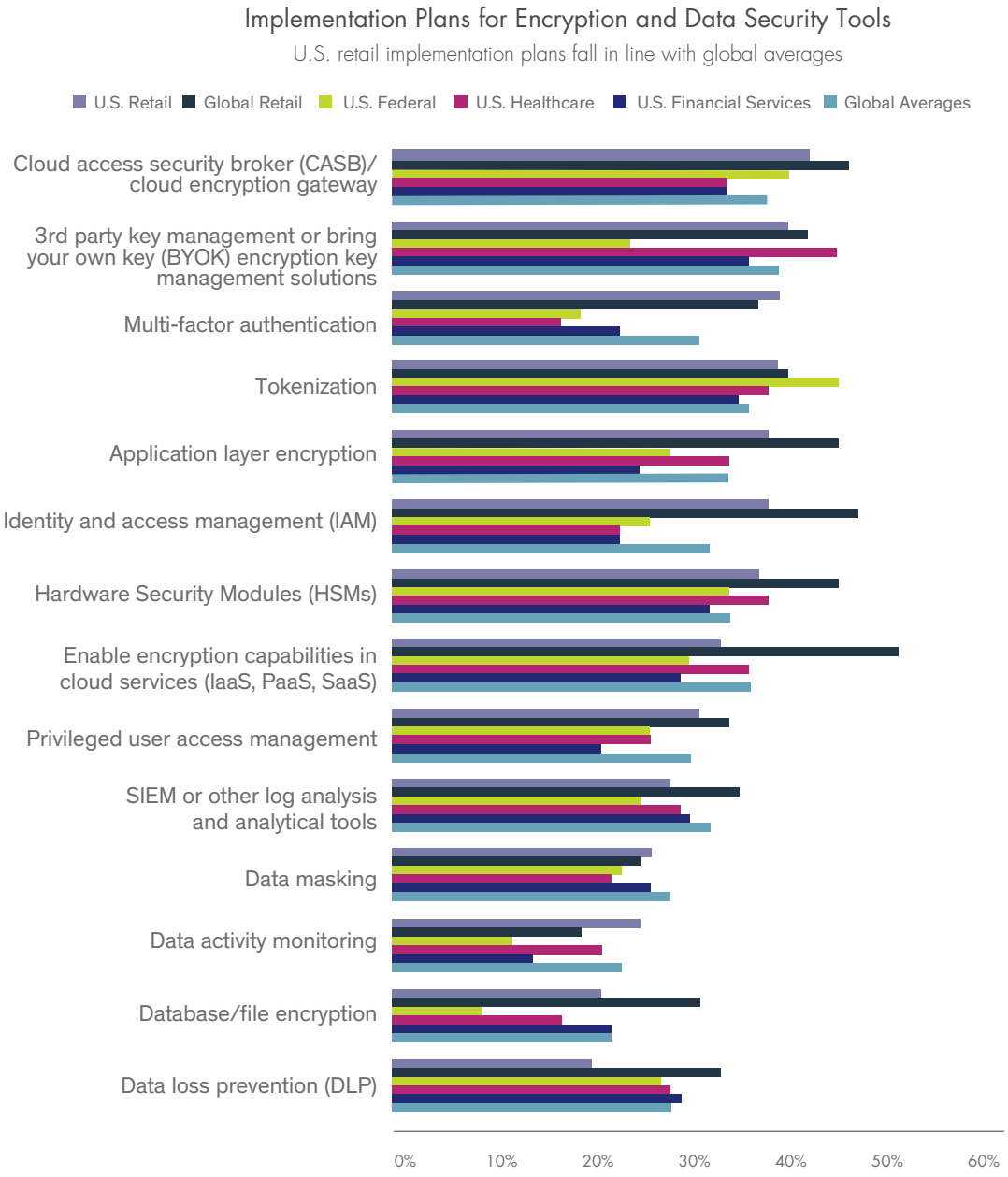


"THOUGH COMPLIANCE REMAINS A TOP SPENDING DRIVER FOR BOTH U.S. RETAIL (41%) AND GLOBAL RETAIL (44%), BEST PRACTICES RISES TO THE TOP FOR U.S. RETAIL (47% FROM 40% IN 2016), AND INCREASED USE OF CLOUD RESOURCES (46%) – A NEW RESPONSE FOR THIS YEAR'S SURVEY – GAINED THE TOP SLOT FOR GLOBAL RETAIL."

TOPICAL AREAS

New security implementations

In terms of data security tools U.S. retail plans to implement this year, cloud access security broker (CASB) tops the list at 42%, compared to the global average of 38%, with global retail slightly higher at 46%. CASB edged out encryption with Bring-Your-Own-Key (BYOK), the top global choice (39%), at 40% for U.S. retails, and global retail at 42%. The third choice both for U.S. retail and globally is multifactor authorization at 39% (37% global retail). The top data security tool chosen by global retail (51%) is enabling encryption in the cloud, once again revealing a sharp divergence from U.S. retail where the figure is only 33%.



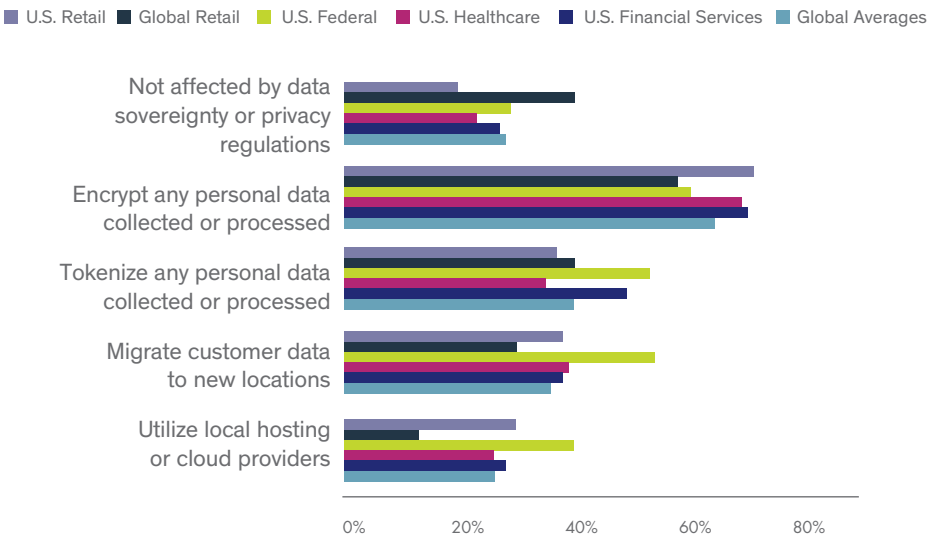
Data sovereignty & privacy regulations

Given widely-publicized concerns over federal government surveillance and the emergence globally of sweeping data privacy laws such as the EU's GDPR, data sovereignty is a highly topical issue in security circles. And similar to overall global responses, the top choice for satisfying local data privacy regulations for U.S. retail is encryption (71%), ahead of the global average of 64%; global retail again diverges at 58%. Similar to the global results, tokenization is third in U.S. retail at 37% but second in global retail at 40%. That being said, both encryption and tokenization are strong tools to protect one's organization and customers from the threat of a data breach. Where cardholder data (CHD) must be stored or transferred, encryption acts as a barrier to access across open and public networks. In cases in which it is unnecessary to hold onto CHD, tokens may be used instead to remove the need for such personal information to cross these networks, protecting both the customer's data and the organization's liability.

"In sum, U.S. retail is generally far more cautious then global retail in deploying new technologies without adequate security, and somewhat more in line with overall global respondents."

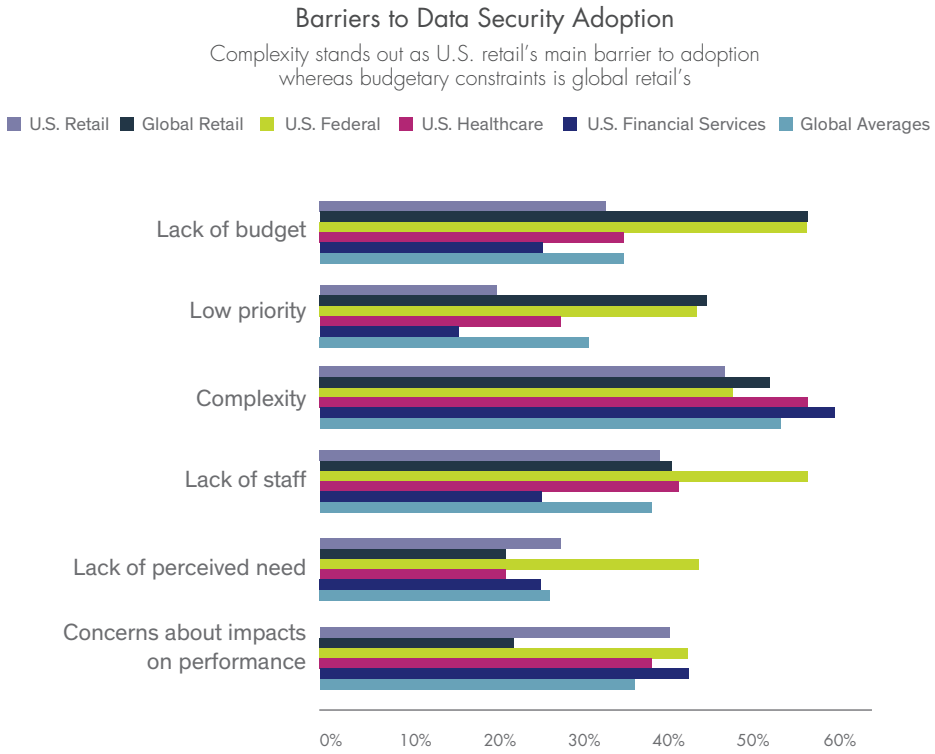
Plans for Data Sovereignty Regulations

Significantly more U.S. retail organizations plan to encrypt personal data to remain compliant with data sovereignty and data privacy regulations than global retail organizations



Security as an 'afterthought'

On a disheartening note, nearly two-thirds of organizations globally (63%) continue to deploy advanced technologies ahead of having adequate security for them. To its credit, U.S. retail does so less aggressively (53%) but this practice is common in a full 80% of global retail – a huge disparity from the U.S. figure. Not surprisingly, U.S. retail is also less likely to store sensitive data in various new tech platforms such as SaaS (56% U.S. vs. 70% global retail); IaaS (38% U.S. retail vs. 57% global retail); Big Data (39% U.S. retail vs. 52% global retail); and PaaS (44% U.S. retail vs. 52% global retail). The corresponding global averages are 57% SaaS; 44% PaaS; 47% Big Data; and 49% IaaS. In sum, U.S. retail is generally far more cautious then global retail in deploying new technologies without adequate security, and somewhat more in line with overall global respondents.



CLOUD, BIG DATA, IOT

Whether for securing data in the cloud, IoT or containers or for assurance with GDPR and PCI DSS, encryption and tokenization remain top choices. Specifically for U.S. retail organizations, compliance with the PCI DSS standard which controls the technical and operational requirements for companies that accept or process card payment transactions, is extremely important. PCI DSS documentation states that tools such as encryption or tokenization may help reduce risk or help meet PCI DSS requirements more easily.

Cloud

With respect to specific cloud security concerns, for U.S. retail the top cloud security concern is security breaches/attacks at the service provider (57%), which also ranked number one globally at 59%. Custodianship of encryption keys was second (54%) and vulnerabilities from shared infrastructure third at 53%. For cloud security controls, both U.S. retail (65%) and global retail (63%) prefer encryption with local key storage by a wide margin over other options and ahead of the overall global average of 61%. The adoption level of BYOK parallels the adoption levels of cloud overall, and thus, we expect interest in BYOK encryption to increase as data increasingly migrates to the cloud.

To be sure, protecting data in public cloud environments has unique challenges for enterprises, primarily dealing with an off-premises, shared environment where they no longer maintain 100% control.

Big Data

From a security perspective, the 'three Vs' of big data – volume, velocity and variety – present several new challenges when it comes to protecting sensitive data. For starters, the velocity of big data requires tools that can operate at line speed and don't introduce latency. Furthermore, given the sheer volume of data created, customers may often be completely unaware of potentially sensitive personally identifiable information (PII) residing within a Hadoop cluster, and as data migrates to wherever it is required for analysis within the cluster, may be located anywhere within the environment.

Heading the list of Big Data security concerns for U.S. retail is the security of reports that include sensitive data as well as foreign privacy regulations (both 43%). A close second (42%) was the concern that sensitive data may reside anywhere in the Big Data environment; this was the top concern (49%) for global retail.

IoT

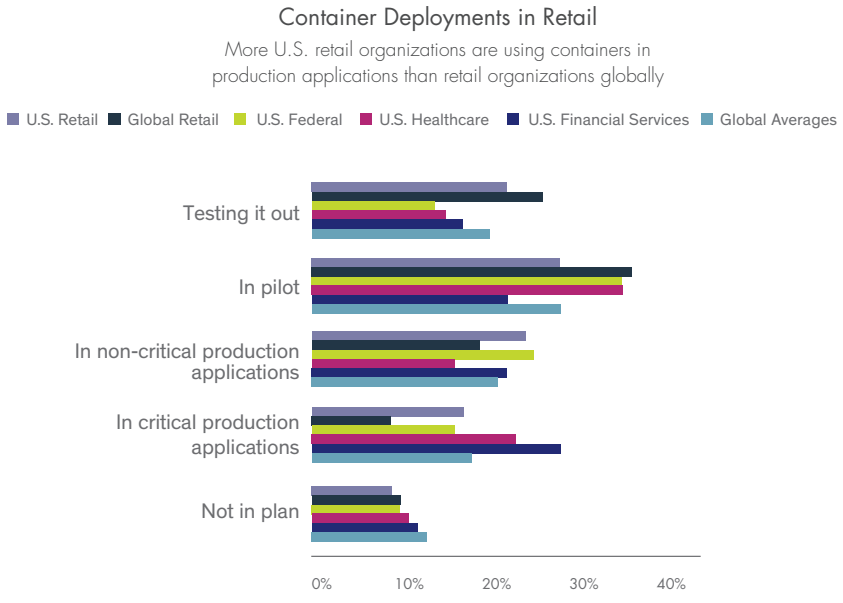
Overall, as with last year's study, the perception of IoT risk remains low, at least relative to other emerging technologies. As we noted previously, the sheer magnitude of IoT promises to be unprecedented, with conservative estimates suggesting over 20 billion IoT devices could be deployed within three years. And similar to other new technologies like cloud and Big Data, security is the number one barrier to broader adoption of IoT.

Though U.S. retail showed conservative adoption rates for cloud, containers and Big Data, when it comes to storing sensitive data on IoT devices, U.S. retail is much more likely to do so (41%) than the global average (31%) or global retail (28%). Not surprisingly, protecting sensitive data stored on those IoT devices is the top concern in U.S. retail (40%) and global retail (44%), as well as the global average (36%).

The use of encryption/tokenization would encourage more U.S. retail users to implement IoT (65%), again diverging broadly from global retail (48%) and to a lesser extent from the global average (56%). Some 58% of U.S. retail would be encouraged by anti-malware protection in IoT; and 54% by authentication/secure digital identification, which mirrors the global retail figure.

Containers

Containers reflect another area of sharp divergence between U.S. and global retail. While 41% of U.S. retail is already using containers for production applications, versus the overall global figure of 39%, just 28% are doing so for global retail.



Security concerns, the top barrier in most vertical and geographic segments, is a distant second (40%) in U.S. retail and in global retail (42%). Budget constraints stands as the top barrier in U.S. retail to container adoption (56%) and in global retail (52%) vs. just 40% globally.

Some of the unique challenges and requirements of securing containers include providing visibility into container access patterns, policies that will persist and travel with containers as they are copied or moved, and the ability to isolate data between containers and provide granular access controls using a default-deny framework. The top container security concern in U.S. retail is unauthorized access (45%) vs. 44% for global retail, where the top concern overall is the spread of malware between containers (45%). Finally, better encryption/data security would make U.S. retail more willing to use containers (56%) vs. 42% in global retail – another point of divergence. Global retail ranked anti-malware at the top choice (52%) vs. 46% in U.S. retail and 45% globally.

RECOMMENDATIONS

RE-PRIORITIZE YOUR IT SECURITY TOOL SET	With increasingly porous networks, and expanding use of external resources (SaaS, PaaS and IaaS most especially) traditional end-point and network security are no longer sufficient. When implemented as a part of the initial development (for ease of implementation versus retrofitting at a later date), data security offers increased protection to known and unknown sensitive data found within advanced technology environments. Look for data security tool sets that offer services-based deployments, platforms and automation that reduce usage and deployment complexity for an additional layer of protection for data.
DISCOVER AND CLASSIFY	Get a better handle on the location of sensitive data, particularly to deal with Big Data, IoT and data sovereignty mandates
DON'T JUST CHECK OFF THE COMPLIANCE BOX	Compared to other verticals, U.S. Retail respondents have the least faith in compliance mandates – and Global Retail the highest. Either way, retail organizations should consider moving beyond compliance and adopting security tools such as encryption or tokenization that may be more appropriate as new technologies like cloud IoT and containers are increasingly adopted.
ENCRYPTION AND ACCESS CONTROL	Encryption needs to move beyond laptops and desktops. **Cloud:** Encrypt and manage keys locally, BYOK is an enabler for enterprise SaaS, PaaS and IaaS use **Big Data:** Employ discovery as a complement to encryption and access control within the environment **Containers:** Encrypt and control access to data both within containers and underlying data storage locations **IoT:** Use secure device ID and authentication, as well as encryption of data at rest on devices, back end systems and in transit to limit data threats **Data Sovereignty:** Consider both encryption and tokenization as a way to avoid hefty fines from violating nascent privacy laws such as GDPR

ANALYST PROFILE

Garrett Bekker
Principal Analyst
451 Research

Garrett Bekker is a Principal Analyst in the Information Security Practice at 451 Research. He brings a unique and diverse background, having viewed enterprise security from a variety of perspectives over the past 15 years. Garrett spent more than 10 years as an equity research analyst at several investment banking firms, including Merrill Lynch, where he was the lead enterprise security analyst, as an investment banker, and also in sales and marketing roles with early-stage enterprise security vendors. Throughout his career, Garrett has focused on a wide variety of subsectors within enterprise security and is now focusing primarily on identity and access management (IAM) and data security, with a special interest in applying the former to cloud-based resources.

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

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.

Please visit **www.thalesesecurity.com** and find us on Twitter **@thalesesecurity**.

THALES

www.thalesesecurity.com

©2017 Thales