THALES

451 Research

2017 THALES DATA THREAT REPORT

Trends in Encryption and Data Security

FINANCIAL SERVICES EDITION

RESEARCH BRIEF

#2017DataThreat

TABLE OF CONTENTS

OUR SPONSORS

INTRODUCTION

Given the continuum of high profile data breaches that seems to be in the news every day, it should be painfully apparent to even casual observers that any system at any organization can be attacked and compromised, at any time. As we have seen throughout the brief history of the internet, each new computing paradigm shift – whether client-server computing and Web applications, Service-Oriented Architecture, or more recently cloud, Big Data and IoT, and so on – ushers in new security vulnerabilities to be exploited.

It's no surprise then 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.

From that perspective, it is troubling that both attitudes and security strategies may not be keeping up with the pace of technological change, as well as the rate at which new threats and attack methods are devised. To illustrate, the Global Edition of the *Thales 2017 Data Threat Report* showed that nearly two thirds (63%) of global 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. In other words, deploy first, secure later is the common modus operandi.

In financial services specifically, that figure soars to a full 73% of global respondents, or nearly three-fourths – though within U.S. financial services it plummets to 47%. This wide discrepancy likely reflects traditionally higher regulatory compliance burdens among U.S. financial firms, and potentially increased conservatism and new regulations the U.S. financial sector has faced following the 2009 financial meltdown, most notably from the Dodd-Frank Act. Indeed, there are other discrepancies between the U.S. and global financial sectors that may be explained, at least in part, by the differing regulatory environments each group faces.

Thus, in this vertical market version of the *Thales Data Threat Report*, we'll focus directly on the financial services market and its unique characteristics, and for the first time we will highlight differences between respondents from the U.S. and global financial services sectors. The 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 1,100 + 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.

"THE GLOBAL EDITION OF THE *THALES 2017 DATA THREAT REPORT* SHOWED THAT NEARLY TWO THIRDS (63%) OF GLOBAL 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. IN FINANCIAL SERVICES SPECIFICALLY, THAT FIGURE SOARS TO A FULL 73%, OR NEARLY THREE-FOURTHS OF GLOBAL RESPONDENTS."

KEY FINDINGS:

Overall, the report showcases a mix of good and bad news for the financial services sector. On the plus side, for both the U.S. and global financial sectors security spending continues to trend upwards. In U.S. financial, 78% of respondents reported security spending will be 'much higher' or 'somewhat higher' than in the previous year, the highest of any vertical other than U.S. Healthcare (81%) and ahead of the overall global average of 73%.

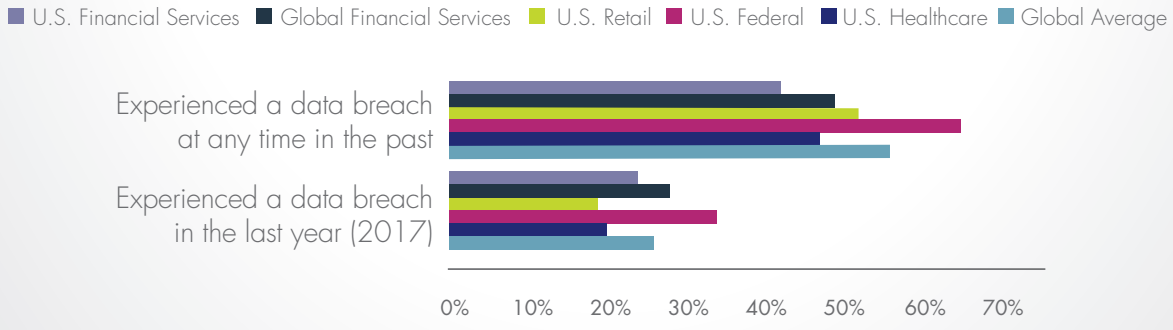
- The not-so-great news is that 24% of U.S. financial firms reported a breach last year, slightly lower than the overall global average of 26%, but higher than most other U.S. verticals and also up markedly from 19% the previous year. Further, just 42% of U.S. financials reported being breached at any time in the past, below the overall global average of 56% – the implication is that U.S. financials are becoming more of a target.

- More good news – only 47% of U.S. financial respondents indicated their organizations are deploying advanced technologies ahead of having adequate security in place, comfortably below the overall global average of 63%; however, that number leaps to 73% among global financial respondents. And for securing these nascent environments (cloud, IoT, containers), encryption and tokenization are the top choices for both segments, and also for meeting local data privacy and sovereignty laws.

- While these are encouraging signs, the U.S. financial services sector chose network security as the top security segment on which spending will increase, which at 73% is well ahead of the global average of 62% and also ahead of any other sector or vertical. In contrast, in both the U.S. and global financial services sectors, data security ranks at the bottom in terms of spending plans. In addition to institutional inertia, the most likely explanation for data security's low ranking is complexity, or at least the perception of complexity of data security. 56% of U.S. financial respondents and 61% of global financial respondents, respectively, cited complexity as the top obstacle to implementing data security.

Data Breach Rates

U.S. financial services saw fewer data breaches than the global average both in the last year and at any other point in the past



"IN THE U.S. FINANCIALS, 78% OF RESPONDENTS REPORTING SECURITY SPENDING WILL BE 'MUCH HIGHER' OR 'SOMEWHAT HIGHER' THAN LAST YEAR, THE HIGHEST OF ANY VERTICAL OTHER THAN U.S. HEALTHCARE (81%) AND AHEAD OF THE OVERALL GLOBAL AVERAGE OF 73%."

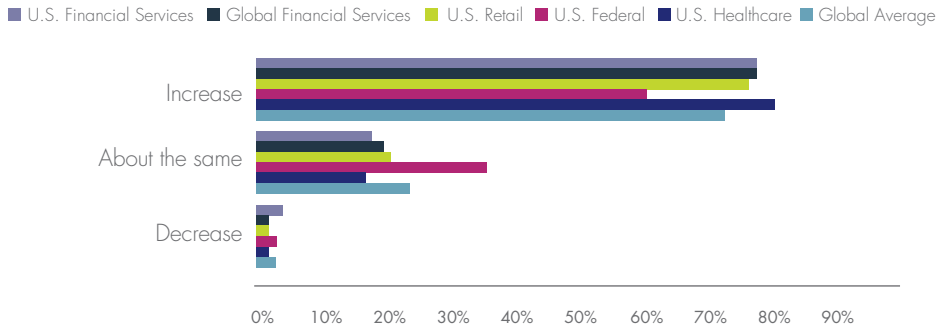
MAIN REPORT

Overall the report reflects fairly good news for the financial services sector compared to other sectors. In both the U.S. and global financial sectors, security spending continues to trend upwards, with 78% of respondents reporting security spending will be 'much higher' or 'somewhat higher' than last year, the highest of any vertical other than U.S. Healthcare (81%) and ahead of the overall global average of 73%, and also ahead of 70% among U.S. financial respondents in the 2016 survey. Clearly financial services firms enjoy fewer budget restraints on security spending than do other verticals sampled.

"In both the U.S. and global financial sectors, security spending continues to trend upwards, with 78% of respondents reporting security spending will be 'much higher' or 'somewhat higher' than last year."

Security Spending in Next Twelve Months

Most financial services organizations plan to increase security spending over the next 12 months

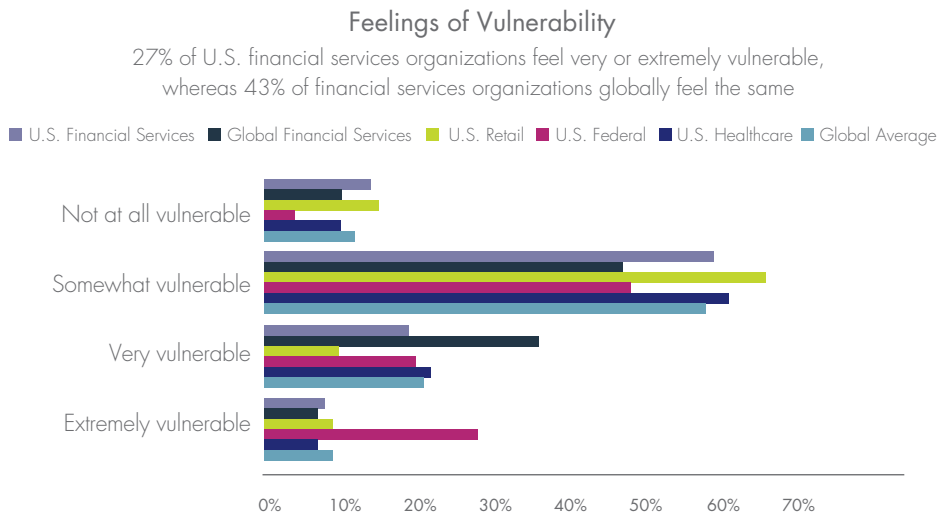


The not-so-great news is that 24% of U.S. financial firms reported a breach last year, slightly lower than the overall global average of 26%, but higher than all other U.S. verticals with the exception of U.S. federal at 34%, and also up markedly from 19% the previous year. This perhaps shouldn't be a big surprise since U.S. financial firms are a prime target of attackers, because, in the infamous words of Willie Sutton 'that's where the money is'. A slightly higher percentage (28%) of global financial institutions also reported being breached in the past year.

"27% of U.S. respondents said they feel 'very' or 'extremely' vulnerable to data threats, slightly below the global average of 30%. "

If we extend our time horizon, however, just 42% of U.S. financials report being breached at any time in the past, below the overall global average of 56% and the lowest of all U.S. verticals; just 49% of global financials likewise reported being breached at some point in the past. While this may appear encouraging on the surface, the disturbing implication is that financial firms are being increasingly targeted than they were previously.

Somewhat paradoxically, just 27% of U.S. respondents said they feel 'very' or 'extremely' vulnerable to data threats, slightly below the global average of 30%. Global financial respondents, however, show a much greater degree of concern, with a full 43% indicating 'very' or 'extremely' vulnerable compared to the global average, and ahead of all other global verticals other than global healthcare (47%).

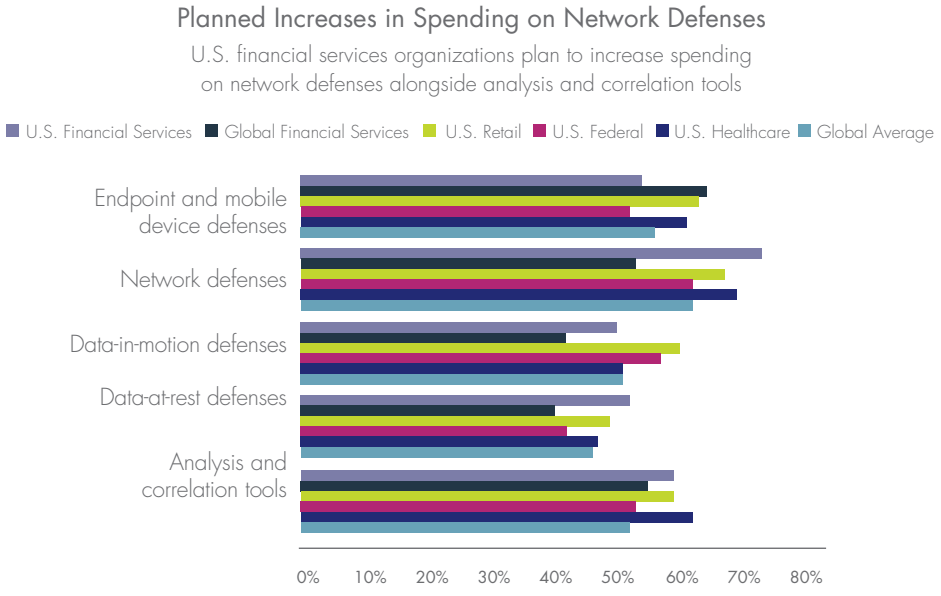


"Old habits die hard – in terms of spending plans, the U.S. financial services sector has the most favorable view of network security among all sectors."

Old habits die hard

As we have seen with most other verticals and geographic regions, more respondents in the U.S. financial services sector plan to increase spending on network security than any other security segment, and at 73% is well ahead of the global average of 62% and any other sector or vertical. The second-ranked option was 'analysis and correlation tools' at 59%, followed by endpoint security (54%).

By sharp contrast, global financial institutions rank endpoint security at the top of the spending list at 64%, followed by analysis and correlation tools (55%), with network security falling into third place (53%) and data-at-rest defenses at 52%.



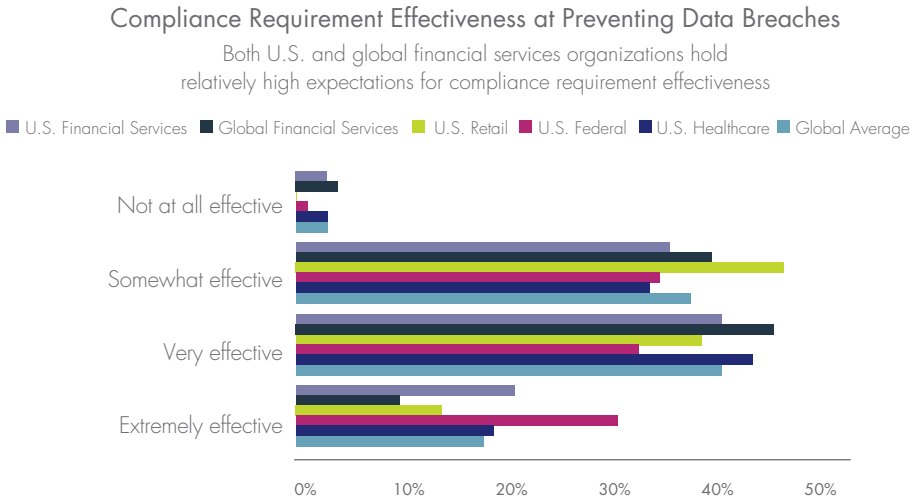
"What is perhaps more disturbing is that in both the U.S. and global financial services sectors, data security ranks at the bottom in terms of spending plans."

What is perhaps more disturbing is that in both the U.S. and global financial services sectors, data security ranks at the bottom in terms of spending plans. For example, in U.S. financial services, data-at-rest security was selected by 52%, and data-in-motion defenses by 50%, dead last among all choices. Similarly for global financial services, 42% selected data-in-motion and just 40% chose data-at-rest defenses, again dead last among all options. Somewhat troubling is that spending in the U.S. on data-in-motion defenses is dead last at just 50%.

The sad truth is that as the data breaches continue to pile up, we continue to spend the bulk of our resources on the same old solutions, while approaches like data security that could arguably do a better job of protecting data, particularly among new technologies like cloud, Big Data and IoT, continue to lag.

The sheer enormity and dynamic nature of the threat environment today makes data security a similarly enormous task, and thus it is not surprising that complexity is cited as the top barrier among global respondents and in most verticals. The same holds true among both U.S. and global financial respondents by a very wide margin (56% of U.S. financial respondents and 61% of global financial respondents, respectively, cited complexity as the top obstacle). The second biggest hurdle in the U.S. financial sector was the potential impact on business performance (40%), and for global respondents the 'lack of perceived need' was the number two choice at 30%. Notably, lack of staff to manage data security, the number two barrier globally (36%), was less of a concern for both segments (24% U.S. financial, 28% global financial).

Once again owing to heavy regulations, compliance requirements are the top reason for security spending at 49% for U.S. financial respondents, with reputation and brand second at 45%, followed by penalty avoidance – which is clearly related to compliance – at 41%. Notably, nearly two-thirds (62%) of U.S. financial respondents believe that compliance spending is 'very' or 'extremely' effective for securing data, compared to the global average of 59% and global financial services at 56%.



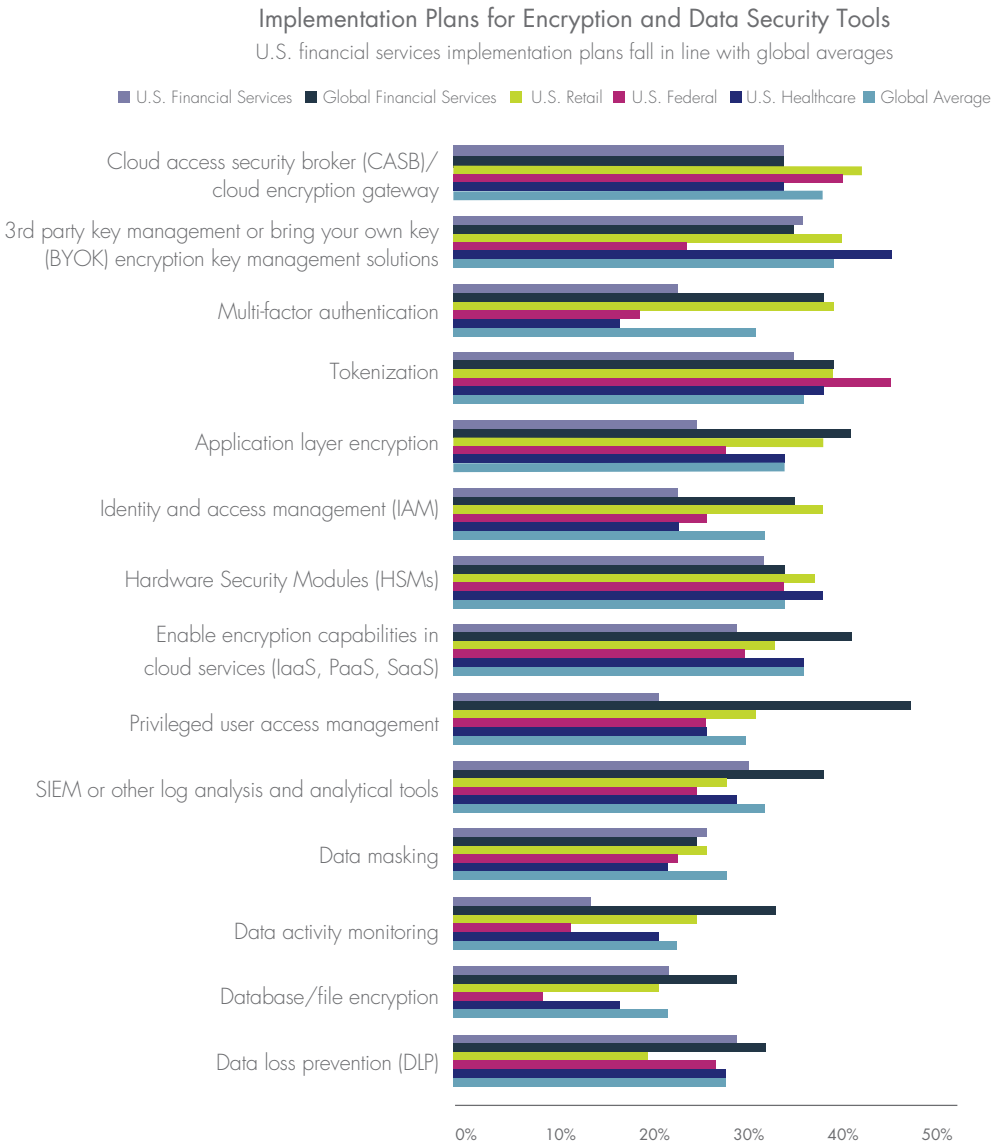
It's not surprising then that U.S. financial respondents also cited compliance as the main reason for spending on security (49%), followed closely by reputation and brand protection (45%). For global financial firms, reputation and best practices (38%) edged out compliance (37%) for the top spot.

"IT'S NOT SURPRISING THEN THAT U.S. FINANCIAL RESPONDENTS ALSO CITED COMPLIANCE AS THE MAIN REASON FOR SPENDING ON SECURITY (49%), FOLLOWED CLOSELY BY REPUTATION AND BRAND PROTECTION (45%). FOR GLOBAL FINANCIAL FIRMS, REPUTATION AND BEST PRACTICES (38%) EDGED OUT COMPLIANCE (37%) FOR THE TOP SPOT."

TOPICAL AREAS

With respect to planned data security implementations, we noticed a strong disparity between the two segments. Among U.S. financial respondents, for example, 36% say they plan to implement encryption with bring-your-own-key (BYOK) capabilities this year, compared with 39% globally; 35% will deploy tokenization (vs. 36% globally); and 34% will deploy cloud access security broker (CASB) vs. 38% globally.

For global financial respondents, however, 47% will implement privileged user access management (vs. only 30% globally); 41% will go with application layer encryption; and 39% with tokenization.



Data Sovereignty

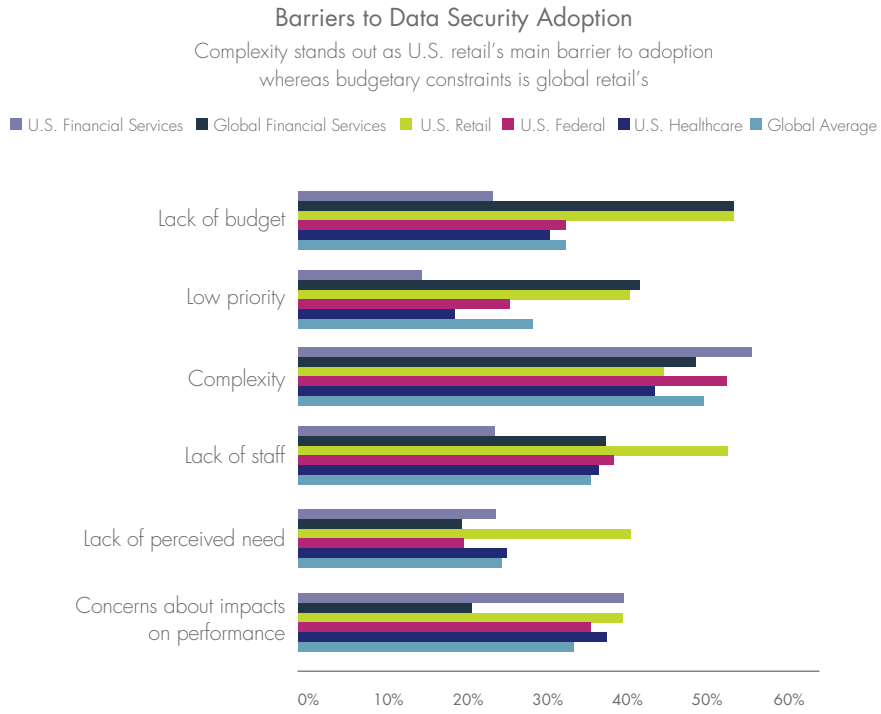
Given the rise in governmental concerns about surveillance as well as the imminent arrival of GDPR in the EU next year and APPI already in effect in Japan, interest is swirling about data sovereignty. For U.S. financial respondents, encryption clearly leads the pack of choices at 70% for satisfying local sovereignty rules, compared with a global average of 64% and 66% for global financial. A distant second in the U.S. is tokenization (49%) as well as with global financial (54%).

What was somewhat surprising was that plans to migrate customer data to remain compliant with data sovereignty laws and choosing local service providers were at the bottom of the list globally (36% and 26% respectively, and also for the financial sector (38% and 28% for U.S. financial). Notably, global financial institutions were less likely to do so (33% and 21%, respectively) despite substantial anecdotal evidence over the past several years that non-U.S. firms would like to migrate data back home and use local providers.

Security as an afterthought

As noted earlier, a troubling finding in the global report was the tendency to deploy advanced technologies ahead of putting the proper security measures in place. While nearly two-thirds (63%) of global respondents admitted to such pressures, the U.S. financial sector does markedly better in this regard (47%). Global financial services, by contrast, does markedly worse (73%). Indeed, U.S. financial is the only sector in which more than half of respondents do not deploy advanced technologies ahead of having security to protect them.

Yet both sectors are placing sensitive data in these new technologies, putting that data at risk for compromise in the process. In the U.S. financial sector, for example, SaaS was the number one advanced technology where sensitive data is stored (61% vs. 57% globally); Big Data was second at 58% (vs. 47% globally); and IaaS third at 45% (vs. 49% globally). The implication is that while users everywhere are moving sensitive data to new environments, U.S. financial appears to be doing a better job of prioritizing the security of that data, while global financial respondents have a lot of work to do and are at substantial risk of serious compromise.



"Given the rise in governmental concerns about surveillance as well as the imminent arrival of GDPR in the EU next year and APPI already in effect in Japan, interest is swirling about data sovereignty."

CLOUD, BIG DATA, IOT AND CONTAINERS

So to the extent that security measures are taken, what are the top choices? In general, encryption and tokenization are top technologies for securing data in new environments such as cloud, IoT and containers. To illustrate, for U.S. financial, 60% favor encryption with locally stored keys as the technology that would most increase willingness to use public cloud, while 51% would opt for encryption with keys stored and managed by the cloud service provider.

Similarly, for IoT, 49% of U.S. financial chose encryption/tokenization and 59% of global financial did likewise, though it's worth noting that U.S. financial was the only sector that selected anti-malware as the top IoT security control (54%). For containers (54% U.S., 53% global financial services), and data sovereignty (70% U.S. financial, 66% global), encryption and tokenization were the top choices.

Cloud

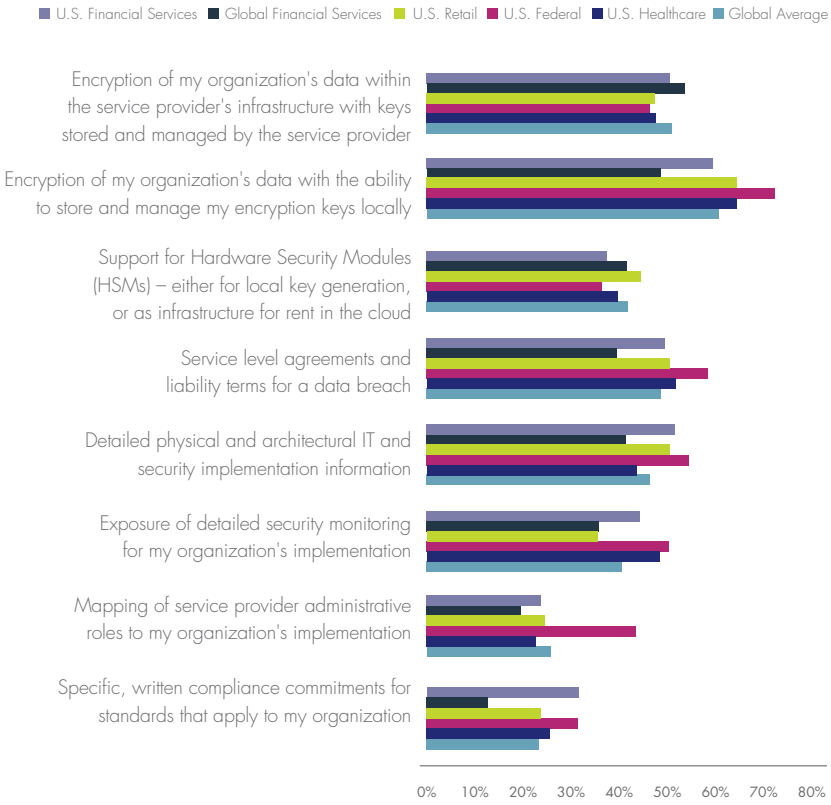
With tidal volumes of data and applications moving to the cloud, global respondents are most concerned about attacks on the cloud service provider (59%). However, for U.S. financial respondents, 53% are most concerned with security vulnerabilities from shared infrastructure, while slightly less (52%) are concerned with security breaches and attacks at the cloud service provider level.

For global financial, the top concern is privileged user abuse (58%), much higher as compared with U.S. financial (49%) and the global average (53%). There is further divergence between U.S. and global financial when it comes to encryption with keys managed by the CSP and managed locally, with U.S. 60% of respondents opting for local storage vs. 51% with CSP management compared with global financial (49% local vs. 54% service provider.)

It's worth noting that global financial firms demonstrated a preference for encryption with keys managed by the cloud service provider (54% versus 51% for U.S. financial), with just 49% opting for encryption with customer-managed keys versus 60% among U.S. financial firms. The disparity is noteworthy, particularly in light of the concerns from non-U.S. firms regarding potential surveillance by U.S. government agencies.

Items to Increase Willingness to Use Public Cloud Services

U.S. financial services organizations that would choose encryption of their data in public cloud services also have a preference towards the storage of encryption keys locally



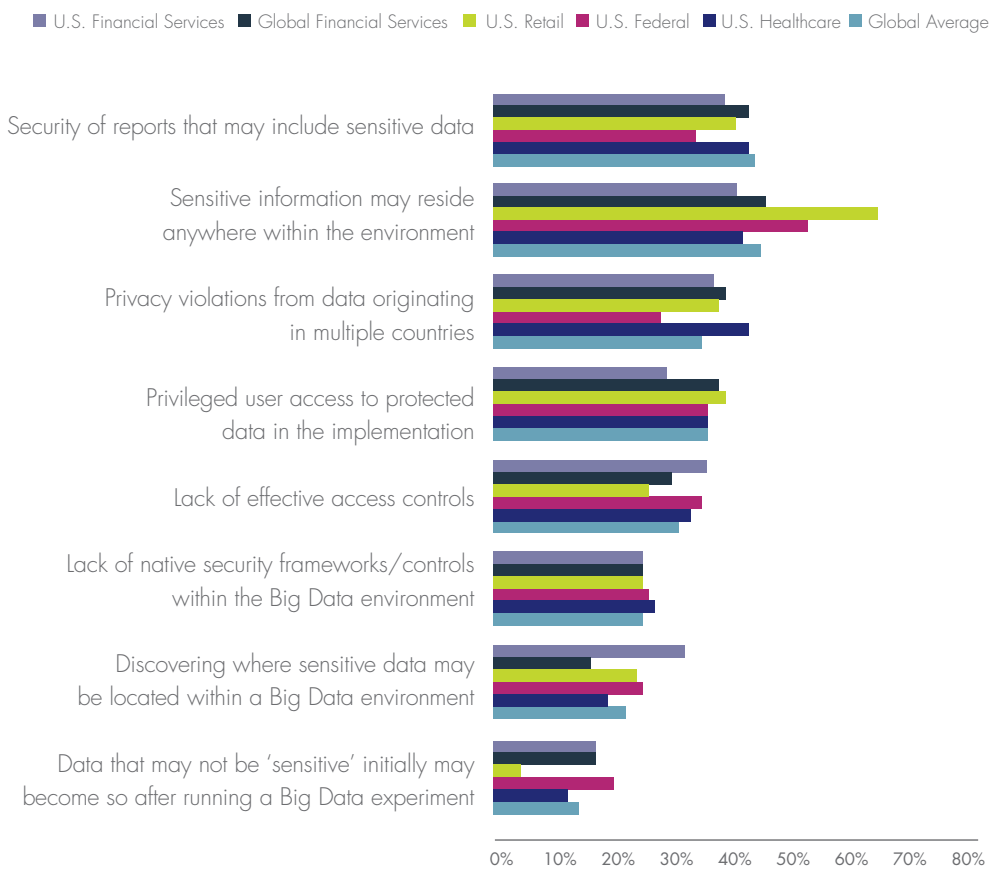
"U.S. financial is the only sector in which more than half of respondents do not deploy advanced technologies ahead of having security to protect them."

Big Data

More U.S. financial respondents (58%) say their firms store sensitive data on Big Data platforms than global respondents (47%) and also far more than global financial respondents (39%). The top two Big Data security concerns for both U.S. (41%) and global (46%) financials are that sensitive data can be stored anywhere in a Big Data environment, followed by concern over the security of Big Data reports (39% U.S. financial, vs. 43% of global financial).

Biggest Concerns Regarding Big Data Security

The top concern for both U.S. and Global Financial Services is that sensitive information may reside anywhere within the environment



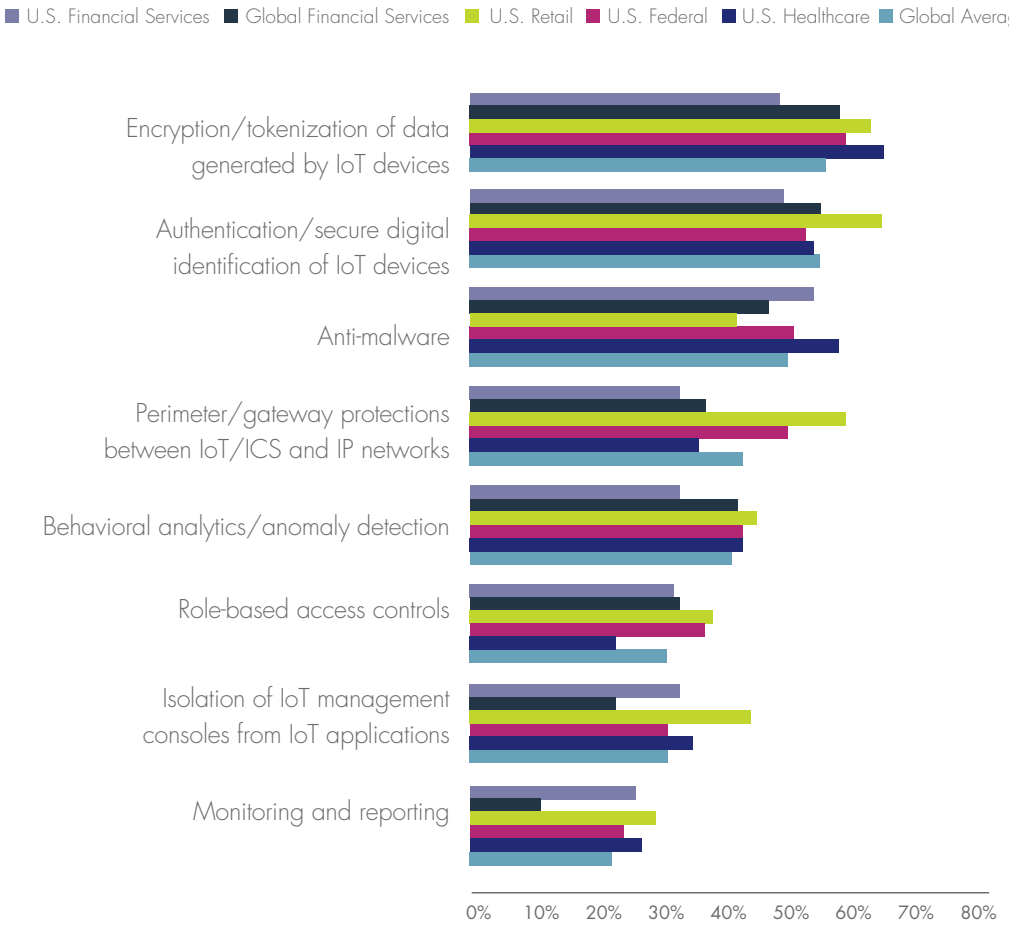
"IT'S WORTH NOTING THAT GLOBAL FINANCIAL FIRMS DEMONSTRATED A PREFERENCE FOR ENCRYPTION WITH KEYS MANAGED BY THE CLOUD SERVICE PROVIDER (54% VERSUS 51% FOR U.S. FINANCIAL), WITH JUST 49% OPTING FOR ENCRYPTION WITH CUSTOMER-MANAGED KEYS VERSUS 60% AMONG U.S. FINANCIAL FIRMS."

IoT

Both U.S. financial (35%) and global financial (34%) store sensitive data in IoT environments, slightly ahead of the global average of 31%. The top IoT security concerns are discovering and identifying sensitive data generated by an IoT device (37% for U.S. financial), and protecting any sensitive data generated by an IoT device (40% global financial, 35% U.S. financial). Meanwhile 54% of U.S. financials would be more willing to use IoT environments if better anti-malware were available (vs 47% of global financial and 50% global average), while 49% of U.S. financial would be more willing to deploy to IoT with encryption/tokenization and authentication of IoT devices.

Items to Increase Willingness to Implement IoT Platforms

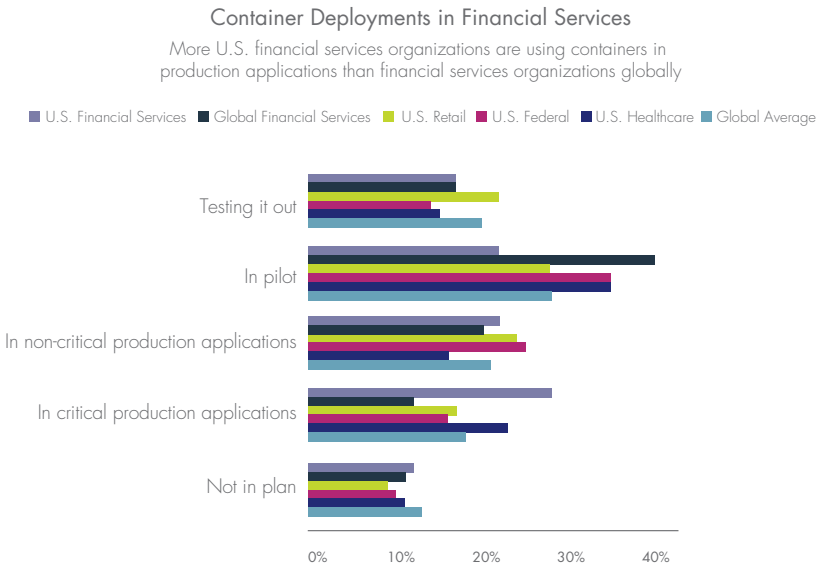
As opposed to global financial services who place encryption/tokenization as the top security incentive to implement IoT platforms in their own environments, U.S. financial services would prefer more effective anti-malware to be in place



Containers

Once again U.S. financial leads the pack when it comes to advanced technology, with 50% using containers for actual production environments vs. the 39% global average, and notably, just 32% for global financial. In general U.S. financial has deployed containers much more rapidly and earlier in their development than they deployed Big Data, dev/ops or IoT.

The leading barrier to greater container deployment in U.S. financial is security (45%) followed by budget (37%); the latter is the leading barrier cited by global financial (45%). Some of the specific security concerns voiced by U.S. financials was the security of container images (45%, versus 33% global financial and the overall global average of 35%. Once again, 54% of U.S. financial respondents say that encryption/data security would make them more willing to use containers, similar to both the global average and global financial (53%). Finally 44% of U.S. financial respondents would be more willing to use containers with anti-malware vs. 45% globally and 51% for global financial.



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	Financial services 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 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.

Garrett Bekker
Principal Analyst
451 Research

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 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-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 eSecurity is part of Thales Group.

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

THALES

www.thalesesecurity.com