Trends in
SaaS DATA PROTECTION

Across the U.S. and U.K.

SPANNING
by EMC

Executive Summary

While SaaS applications bring tremendous benefits to organizations, including increased agility, accessibility, collaboration, and innovation, there are also a few challenges and misconceptions about the cloud that companies relying on this technology must overcome.

As SaaS is still a rapidly evolving field, it's easy for organizations working in the cloud to have these concerns:

▶ What, if anything, is being done to ensure my data isn't accidentally or maliciously deleted?

▶ Can I rely on software providers to host our data and ensure its protection?

▶ Where is our company's data stored?

▶ In an increasingly global economy, can I be certain my data will comply with local and regional privacy laws?

While concerns about data protection and accessibility are understandable, it's important to emphasize that through implementation of a few key best practices and keeping up with compliance standards, SaaS adoption can be a safe, smooth experience that allows your organization to operate more effectively than ever before.

To get a look at the SaaS landscape across the globe – the use, perceptions, regulations, and impact of the cloud – Spanning by EMC commissioned a survey of 1,037 IT decision makers who have involvement in SaaS applications for their organization.

SPANNING
by EMC

This extensive survey of IT professionals in the U.S. and U.K. helps us:

▶ Better understand trends and perceptions in SaaS adoption, utilization and data protection;

▶ Determine if there are significant differences between IT professionals in the U.S. and the United Kingdom;

▶ Gauge the impact of changing European Union data privacy rules and regulations; and,

▶ Shed light on perceptions about who is responsible for SaaS data protection, organizational confidence in SaaS data protection, and the top concerns about moving data to the cloud.

The survey identified four key findings:

1: Similar SaaS adoption trends in U.S. and U.K.
In both the U.S. and U.K., companies are moving to the cloud by deploying the same types of SaaS applications, and largely, the same type of data, in the public cloud.

2: Different perceptions on SaaS data protection but same need exists
On both sides, approximately 80 percent of respondents have suffered some type of SaaS data loss and have similar fears related to future cloud data security. However, respondents from the States are much more confident in their SaaS app providers' ability to restore their data in the event of a loss.

3: Similar states of awareness and usage of SaaS backup
Respondents were most likely to expect their SaaS application providers to ensure data protection. While the majority knew of standalone SaaS application data backup and recovery solutions, only 37 percent of respondents in the U.S. and 31 percent in the U.K. actually utilize the third-party backup solutions.

4: Data sovereignty concerns remain for both sides
On both sides of the Atlantic, there is concern about the effect of new E.U. data privacy requirements. Even with the new regulations, nearly 70 percent of U.K. respondents disagree or feel neutral about the statement, "The existence of E.U. regional data centers will resolve the issue of data being accessed by agencies like the NSA or [Government Communication Headquarters] GCHQ."

SPANNING
by EMC

SaaS Adoption Trends

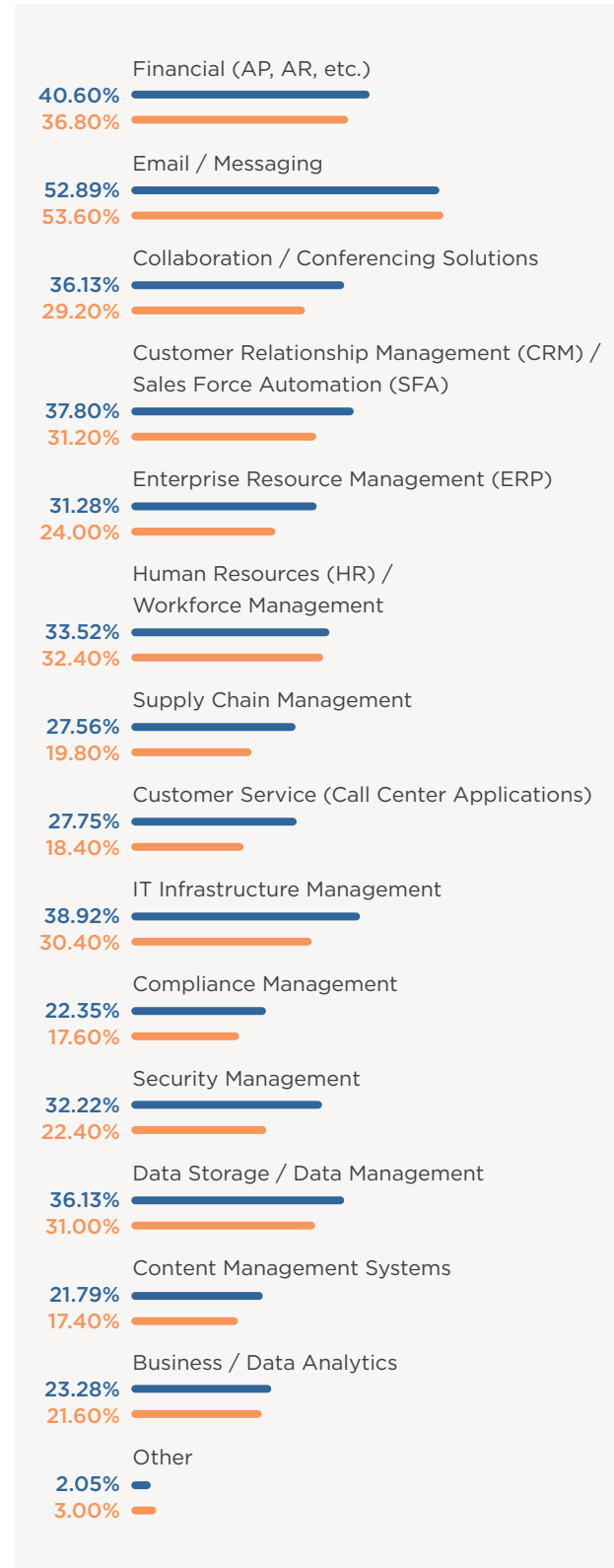### The U.S. and U.K. are largely deploying the same SaaS applications.

On both sides of the Atlantic, organizations are moving to the cloud by deploying similar types of SaaS applications. When given a choice of 14 common types of SaaS applications, the top 2 for the U.S. and U.K. were the same – Email/ Messaging and Financial are either deployed in a public cloud now, or will be deployed in one in the next 12 months.

In the U.K., HR software – containing some of the most sensitive personal data about employees – was the third-most chosen option, while in the U.S., it was IT infrastructure management; both regions included CRM/SFA software as their fourth-most implemented.

More than half of respondents are moving or have moved their email/messaging applications to SaaS models.

Financial (AP, AR, etc.)
40.60%
36.80%

Email / Messaging
52.89%
53.60%

Collaboration / Conferencing Solutions
36.13%
29.20%

Customer Relationship Management (CRM) / Sales Force Automation (SFA)
37.80%
31.20%

Enterprise Resource Management (ERP)
31.28%
24.00%

Human Resources (HR) / Workforce Management
33.52%
32.40%

Supply Chain Management
27.56%
19.80%

Customer Service (Call Center Applications)
27.75%
18.40%

IT Infrastructure Management
38.92%
30.40%

Compliance Management
22.35%
17.60%

Security Management
32.22%
22.40%

Data Storage / Data Management
36.13%
31.00%

Content Management Systems
21.79%
17.40%

Business / Data Analytics
23.28%
21.60%

Other
2.05%
3.00%

▶ U.S.   ▶ U.K.

SPANNING
by EMC

SaaS Data Risks

The U.S. and U.K. have suffered many of the same data losses – and share the same fears.

Organizations in both the U.K. and the U.S. have faced SaaS data loss. Both are primarily turning to the SaaS providers for backup and restoration of data. In general, American IT professionals are more confident than their U.K. counterparts in their organizations' ability to keep cloud data secure.

SaaS data loss affected respondents on both sides of the pond – from similar sources. In the United States, the top four sources of data loss in the past 12 months were:

▶ Accidental deletion (43 percent)

▶ Migration to a SaaS provider (33 percent)

▶ Accidental overwriting of correct information with incorrect information (27 percent)

▶ Hackers and/or hacktivists (25 percent)

Just 23 percent reported no SaaS data loss in the last 12 months.

In the U.K., data loss was from similar sources:

▶ Accidental deletion (40 percent)

▶ Migration to a SaaS provider (31 percent)

▶ Accidental overwriting of correct information with incorrect information (26 percent)

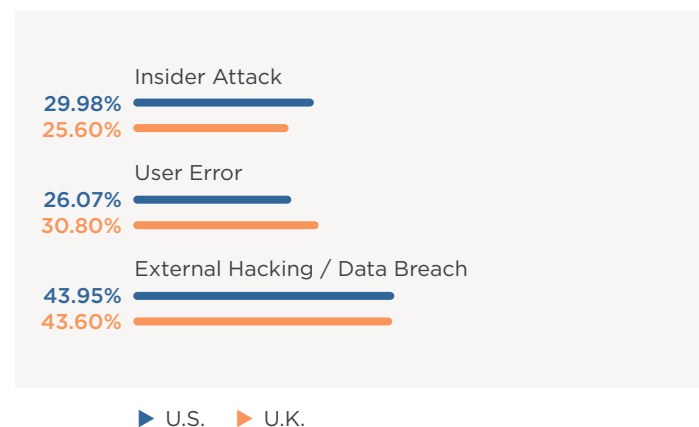▶ Hackers and/or hacktivists (20 percent).

Just 21 percent had no data loss.

When it comes to data loss risks, the majority of respondents cite insider attacks and user error at the top of the list.

On both sides, the greatest cloud data concerns originate from within – 56 percent of U.K. respondents cite "insider attack" or "user error" as their greatest fear, while 55 percent do so in the U.S. 44 percent of both British and American respondents cite "external hacking" or "data breach" as their greatest fear.

Q: **When it comes to protecting your cloud-based data and avoiding data loss, which is your greatest concern?**

Insider Attack
29.98%
25.60%

User Error
26.07%
30.80%

External Hacking / Data Breach
43.95%
43.60%

▶ U.S.   ▶ U.K.

SPANNING
by EMC

SaaS Data Protection

The U.S. is much more confident in its ability to secure its cloud data.

80 percent of American respondents strongly or somewhat agree with the statement, "I am confident in my organization's ability to secure cloud data." At the same time, nearly half (45 percent) of British respondents answered similarly.

So what is driving their confidence? The primary source of data backup and recovery for both was reliance on SaaS vendors – 49 percent in the U.S., and 42 percent in the U.K.
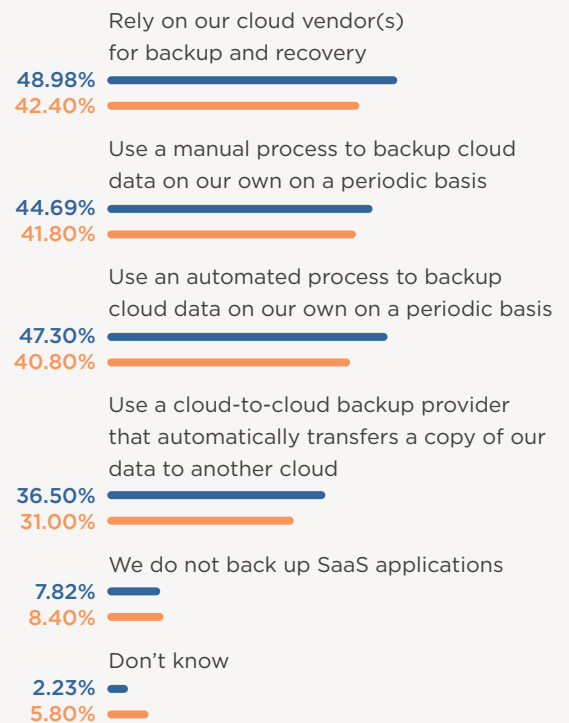
Awareness of standalone SaaS backup solutions is growing.

Some 78 percent of U.S. respondents, and 73 percent in the U.K., are aware of standalone services that allow them to backup and restore SaaS information separate of the provider/application. Yet, only 37 percent in the U.S. utilize them, and 31 percent in the U.K.

Today, 41% of U.K. and 44% of U.S. companies manually back up their SaaS applications.

Q: What is your organization's strategy over the next 12 months for backup and recovery of SaaS applications?

Rely on our cloud vendor(s) for backup and recovery
48.98%
42.40%

Use a manual process to backup cloud data on our own on a periodic basis
44.69%
41.80%

Use an automated process to backup cloud data on our own on a periodic basis
47.30%
40.80%

Use a cloud-to-cloud backup provider that automatically transfers a copy of our data to another cloud
36.50%
31.00%

We do not back up SaaS applications
7.82%
8.40%

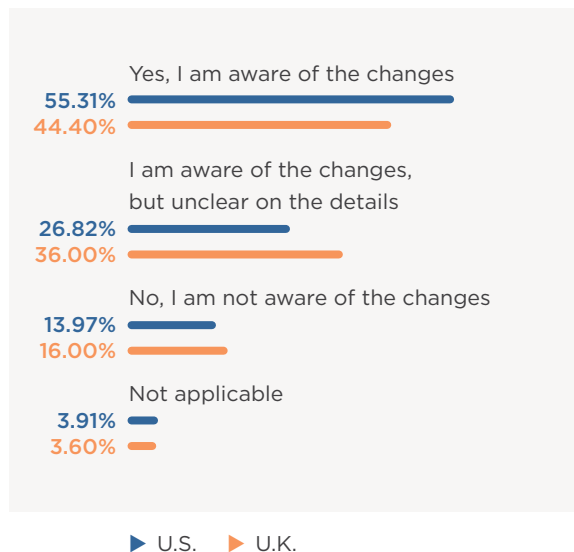Don't know
2.23%
5.80%

▶ U.S.   ▶ U.K.

SPANNING
by EMC

Data Sovereignty

The U.K. is taking a more cautious approach than the U.S.

Respondents in both nations are aware of the impending changes in Safe Harbor rules – 82 percent in the U.S., 80 percent in the U.K. – although many are not aware of the particulars.

Just 36 percent of those in the U.K. who are responsible for their organization's SaaS purchases are "unclear" on the details of the proposed changes. This may be true because the greatest change proposed in the new Safe Harbor agreement, the declaration that E.U. data must stay within the E.U., likely affects the U.K. more than counterparts in the U.S. That said, 27 percent of American respondents are still "unclear" on the details.

Q: Are you aware of the changes in Safe Harbor rules requiring all European data to remain in the EU?

Yes, I am aware of the changes
55.31%
44.40%

I am aware of the changes, but unclear on the details
26.82%
36.00%

No, I am not aware of the changes
13.97%
16.00%

Not applicable
3.91%
3.60%

▶ U.S.   ▶ U.K.

> "
> Being a UK-headquartered company, it is critical that we ensure that the aspects of our data are managed within the European Economic Area and governed securely. This was a critical driver for our company choosing Spanning Backup. Now, we are assured our data remains in the UK data center, where it can be safely protected, backed up and restored."
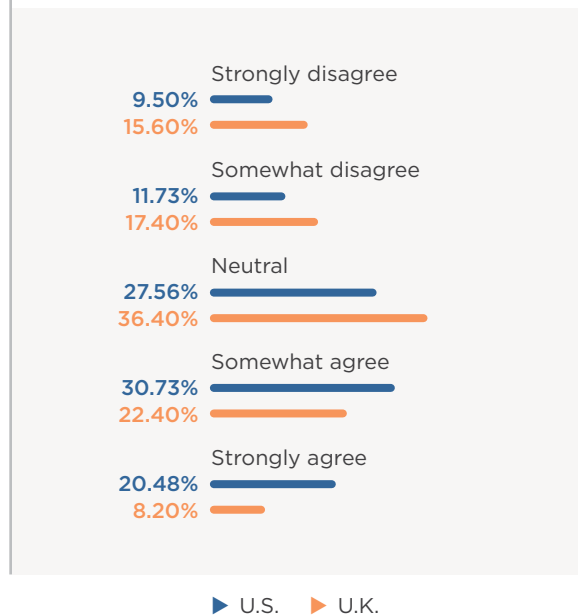
GARRY LENGTHORN
Director of IT Services, SThree PLC.

SPANNING
by EMC

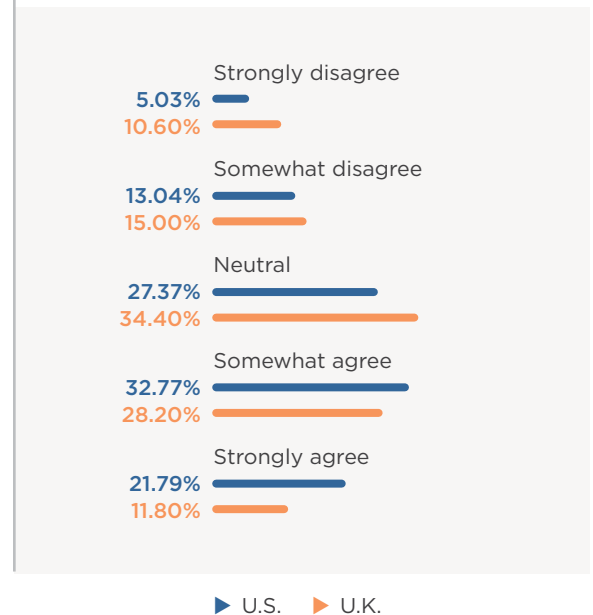## Compliance is seen as costly and not as a fix for privacy.

Respondents from both countries agree that the new privacy regulations are creating a costly compliance burden (50 percent U.S., 40 percent U.K.) – yet most still believe that storing data in a primary cloud vendor's E.U. data center will ensure 100 percent compliance with data and privacy regulations (72 percent U.S., 66 percent U.K.).

Q: How strongly to do you agree or disagree with the following statements?

The existence of EU regional data centers will resolve the issue of data being accessed by agencies like the NSA or GCHQ

Strongly disagree
9.50%
15.60%

Somewhat disagree
11.73%
17.40%

Neutral
27.56%
36.40%

Somewhat agree
30.73%
22.40%

Strongly agree
20.48%
8.20%

▶ U.S.   ▶ U.K.

I am comfortable that the new Safe Harbor Agreement will pacify our EU data privacy concerns

Strongly disagree
5.03%
10.60%

Somewhat disagree
13.04%
15.00%

Neutral
27.37%
34.40%

Somewhat agree
32.77%
28.20%

Strongly agree
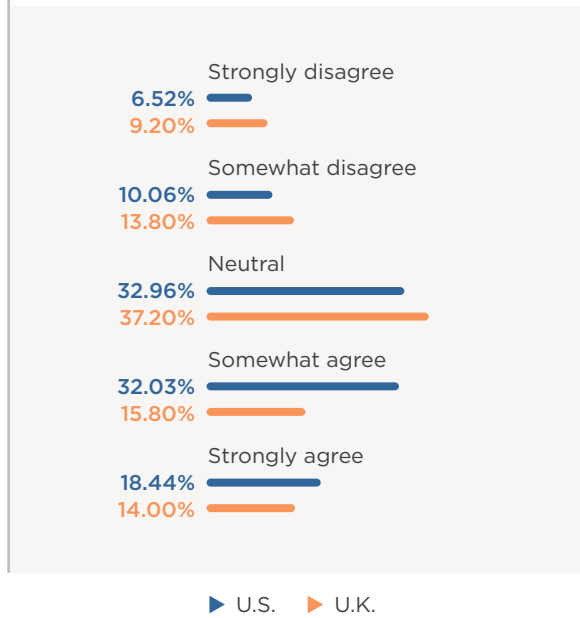**21.79%**
11.80%

▶ U.S.   ▶ U.K.

While both sides are moderately confident in the privacy capabilities of the updated agreement, British respondents still fear the long arm of American surveillance. A whopping 69 percent of them either are neutral on, somewhat disagree or strongly disagree with the statement, "The existence of E.U. regional data centers will resolve the issue of data being accessed by agencies like the NSA or GCHQ." (Americans also fear surveillance by their own government, although not to as great an extent: 49 percent responded similarly).
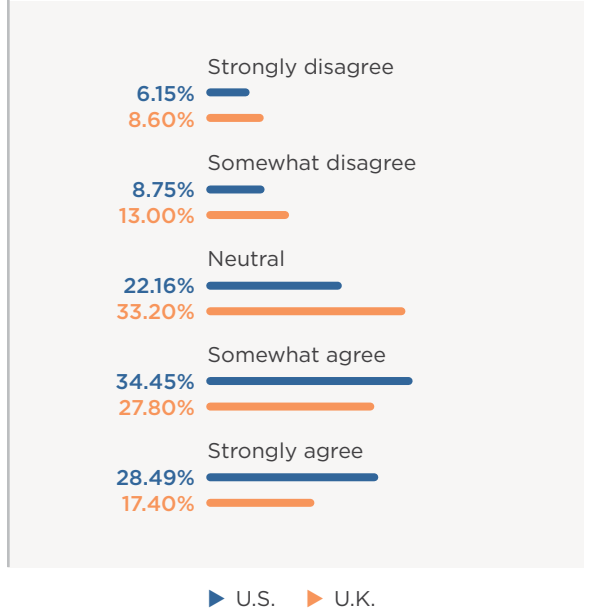
Similarly, in the U.K., 60 percent are neutral on, somewhat disagree or strongly disagree with the statement, "I am comfortable that the new Safe Harbor Agreement will pacify our E.U. data privacy concerns."

This is only true of 46 percent from the U.S. The British skepticism could stem from a variety of sources – including the nation's already-tenuous relationship with the E.U.

The changing EU data privacy regulations are creating a costly compliance burden

Strongly disagree
6.52%
9.20%

Somewhat disagree
10.06%
13.80%

Neutral
32.96%
37.20%

Somewhat agree
32.03%
15.80%

Strongly agree
18.44%
14.00%

▶ U.S.   ▶ U.K.

I am confident in my organization's ability to secure cloud data

Strongly disagree
6.15%
8.60%

Somewhat disagree
8.75%
13.00%

Neutral
22.16%
33.20%

Somewhat agree
34.45%
27.80%

Strongly agree
28.49%
17.40%

▶ U.S.   ▶ U.K.

SPANNING
by EMC

Overall Conclusions

On both sides of the Atlantic, organizations of all sizes, across industries, are putting more of their critical enterprise applications – and thus, employee and customer data – in the cloud. While compliance, data governance and disaster recovery are key drivers for SaaS data protection, other issues will affect how data is managed and where it is stored in the coming months as further decisions are made around data sovereignty and the Safe Harbor agreement.

The security of SaaS data is critical – and Americans (80 percent) are more confident than British respondents (45 percent) in their organization's ability to secure cloud data. This confidence may shift, however, as organizations continue to see SaaS data loss incidents occur – almost 80 percent of all respondents experienced some sort of SaaS data loss. And, while 78 percent of U.S. respondents, and 73 percent in the U.K., are aware of standalone services that allow them to backup and restore SaaS information separate of the provider/application, only 37 percent in the U.S. utilize them, and 31 percent in the U.K.
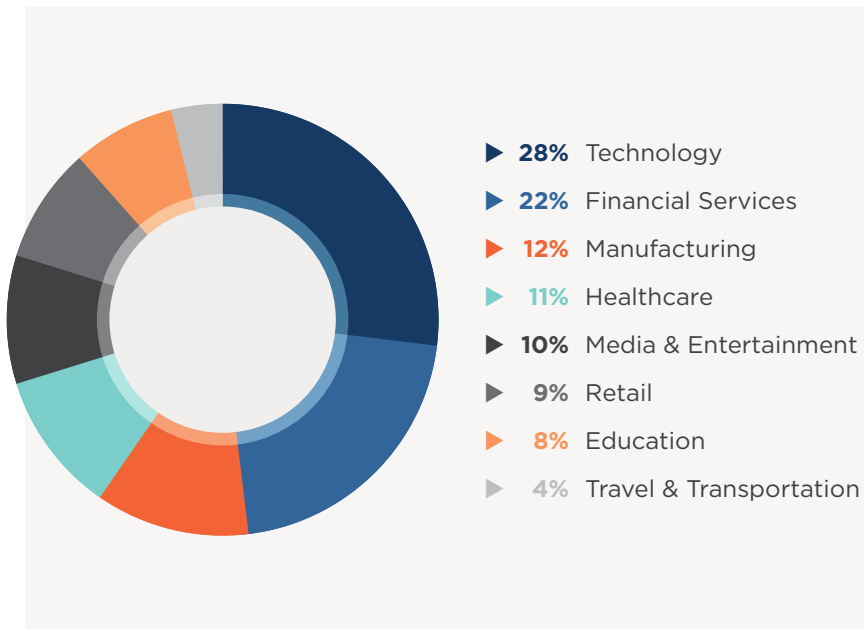
Adoption of SaaS data protection solutions is still in the early phases yet there are plenty of reasons for these organizations to find better ways to make sure their business-critical data is always available and recoverable in case a data loss event occurs.

SPANNING
by EMC

Survey Methodology

[Spanning by EMC](#) commissioned the survey, which was completed by 1,037 respondents. Of the respondents, 500 (48 percent) were based in the United Kingdom, and 537 in the United States (52 percent). A full 100 percent of the respondents "have influence or decision making authority on spending in the IT department" of their organization.

Respondents were asked to select between two specific roles: "IT Function with Oversight for SaaS Applications" (75 percent U.S., 78 percent U.K., 77 percent overall); "Line of Business/SaaS application owner" (39 percent U.S., 43 percent U.K., 41 percent overall); the remaining identified as "other."

In the online survey, respondents represented the following industries:

▶ **28%** Technology
▶ **22%** Financial Services
▶ **12%** Manufacturing
▶ **11%** Healthcare
▶ **10%** Media & Entertainment
▶ **9%** Retail
▶ **8%** Education
▶ **4%** Travel & Transportation

SPANNING
by EMC

About Spanning by EMC

Spanning, an EMC company and a leading provider of backup and recovery for SaaS applications, helps organizations to protect and manage their information in the cloud. The company provides powerful, enterprise-class data protection for Google Apps, Salesforce, and Office 365.

Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of companies and millions of users around the world. Learn more at www.spanning.com.

SPANNING
by EMC