A Sense of Security

"The security of the data on a cloud platform is something that can keep you awake at night."

Jim Albert, CIO at Bankers Financial Corporation

Even as cloud and managed services grow increasingly central to business strategy and performance, challenges remain. The biggest sticking point for companies seeking to capitalize on the cloud is data security. Keeping data safe is an issue in any computing environment, and it has been a focus since the earliest days of the cloud revolution. Understandably so: a lot can go wrong when you allow valuable information to live outside the firewall. Recent revelations about government snooping, along with a steady stream of well-publicized data breaches, only add to the uncertainty. Managing these concerns, along with related questions around choosing the right cloud vendor, is an essential part of any cloud migration.

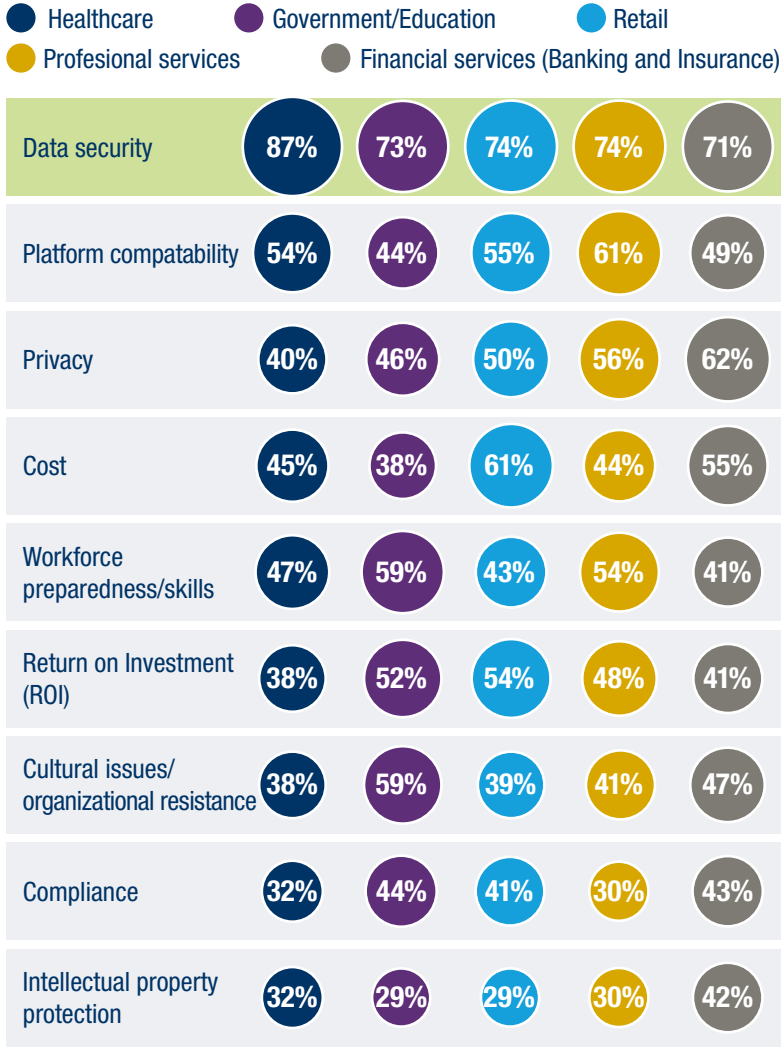
Our survey of 350 business and technology executives from diverse industries across the United States reveals that data security remains the top concern for companies as they move into the cloud—76% of respondents say it influences their migration strategies. Related issues also raise red flags, with just over half of surveyed executives saying data privacy concerns influence their strategies and one-third citing intellectual property protection. As Jim Albert, CIO at Bankers Financial Corporation in St. Petersburg, Florida, puts it: "The security of the data on a cloud platform is something that can keep you awake at night."

windstream®
smart solutions. personalized service.

OXFORD ECONOMICS

Concerns influencing cloud migration strategies

% who say the following concerns are influencing their migration strategies "to quite an extent" and "to a great extent"



Some industries, motivated by regulatory compliance and the nature of their business, place an even greater premium on data security than others. For example, healthcare providers are more likely to consider data security a top concern—87% say it influences their migration strategies, compared with retail (74%), professional services (74%), government and education (73%), and financial services (71%). And attitudes vary with job function, too. C-level executives are more likely to report a strong concern with data security than their less-senior colleagues, with CIOs especially focused on data security as an influence on cloud migration strategy. Getting lower-level management more attuned to security needs, then, would seem to be a good idea.

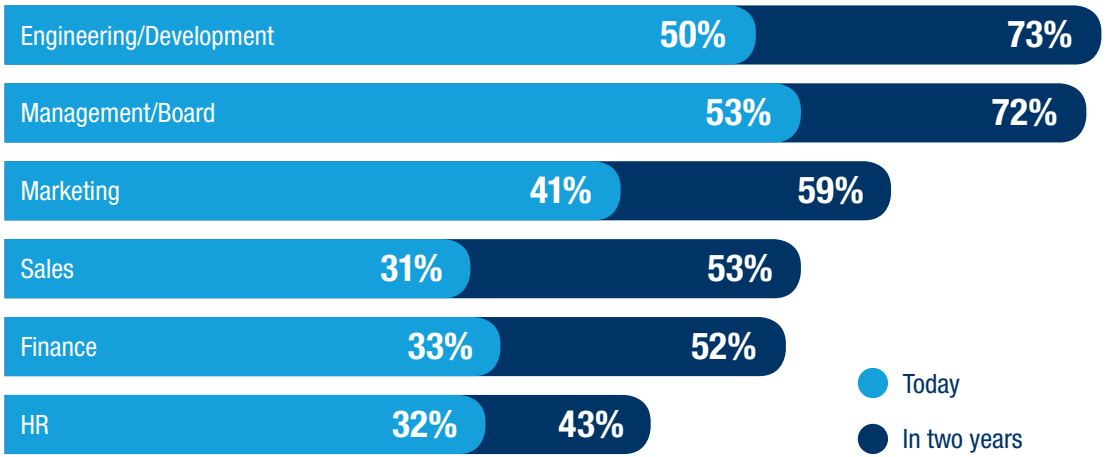
Yet as important as security concerns are, they may be somewhat misdirected. As cloud vendors continue to up their game, companies should be asking themselves if their own abilities to protect data are keeping up with those of cloud providers. In any case, finding the right vendor and integrating their services into a coherent, overarching security strategy are essential steps along the path to value in the cloud.

Security matters

Communication and collaboration are core values of business today. Yet these activities by their nature involve some level of data-security risk. With cloud a key driver of the ascendant data-sharing culture, and a growing share of data headed into the cloud, companies need to make security strategy a priority.

Putting more information into the cloud

% who say functions are in the cloud, today and two years from now



First do no harm

Healthcare organizations put the highest emphasis on data security of any industry we surveyed. That idea resonates with Kevin Buchanan, Director of IT infrastructure at Randolph Hospital, a $100 million-plus primary healthcare provider located in Asheboro, North Carolina. The health system has turned to the cloud for several specialized applications, including radiology and diagnostic imaging, but it must move carefully.

“We have a lot of risk associated with HIPAA compliance,” he says, referring to the massive federal healthcare law. “The Office of the Inspector General has issued millions of dollars in fines for organizations that have had data leakage.”

Randolph Hospital is now looking to migrate its electronic health records, as well as disaster recovery and business continuity, into the cloud. “Today, business is all about risk mitigation, transference, or acceptance,” says Mr. Buchanan. “One of the questions we have to constantly ask is whether we can lower our risk by running an application in-house or in the cloud.” To address the questions around risk, Mr. Buchanan is focusing on detailed due diligence and addressing potential legal issues up front. Randolph Hospital has also established a clear checklist of requirements, and carefully examines whether a provider can meet its standards across multiple criteria, including security and issues covered in service-level agreements.

Well over three-quarters of our survey respondents expect cloud and managed services to facilitate collaboration—83% say it will allow them to collaborate among business units in two years, and 80% say it will allow them to collaborate with partners. And the sensitivity of shared data has never been higher; among the many functions moving quickly into the cloud over the next two years, engineering and development, along with management and board operations, will see the highest rates of growth. The stakes for data security have never been higher.

But no system, internal or cloud-based, is totally secure. Acknowledging that uncomfortable fact can change the way companies think about the cloud. So what can companies do? Jack Whitley, Senior Vice President of E-Commerce at retailer Replacements, Ltd., in Greensboro, NC, says strong security starts with a data-centric view and understanding where data resides, how it travels, and what vulnerabilities and risks the ecosystem presents. In addition, an enterprise must have mechanisms in place to measure results and tie things back to metrics.

Putting cloud security to work

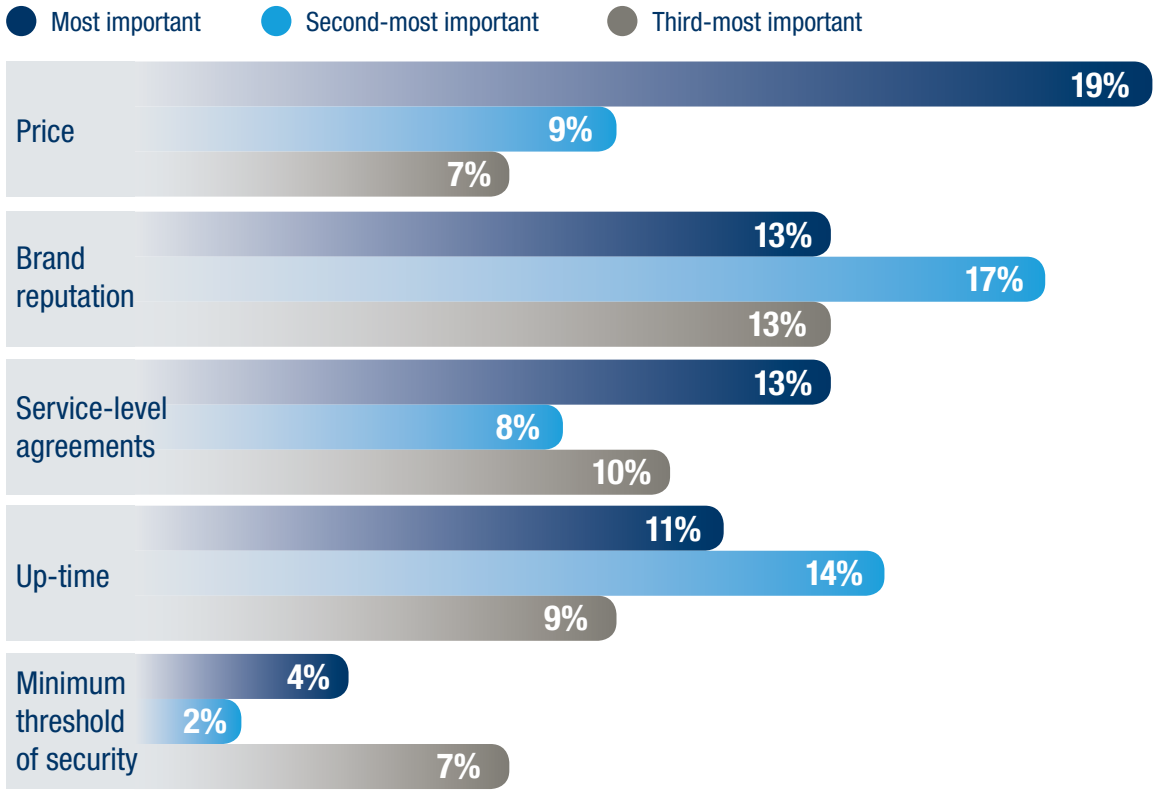
For all the focus on protecting data, many companies are not pursuing the security agenda in a logical or systematic way. While survey respondents clearly recognize the importance of security as they move data and processes to the cloud, a sizable number are not emphasizing their concerns when choosing service providers. Barely half of respondents rank a minimum threshold of security as an important or very important quality in a cloud vendor, putting security behind issues such as scalability, price, portal capabilities, and several others.

This seeming indifference to security could be a result of firms not assessing their own needs in terms of vendor performance. Just 38% of the sample say they have clear expectations of vendor performance, and 39% say they have performed a cloud readiness assessment. Remarkably, nearly one-quarter report that they have no formal processes in place to manage the quality and integrity of cloud services. Furthermore, most companies do not emphasize strong security with vendors—in fact, only 4% indicated that it was the most important issue.

Our research shows that higher-performing firms position security at the center of their cloud initiatives. The most profitable companies in the survey pool are more likely to cite a minimum threshold of security as a core issue—10% say it is the most important quality differentiating a service provider from others, while no firms with flat or negative profit margins say so. More-profitable companies are also more likely to view a vendor's transparency into operations and performance as a key consideration.

38% say they have clear expectations of vendor performance. 23% have no formal processes in place to manage the quality and integrity of cloud services.

How important are the following qualities in a service provider?



Size and security

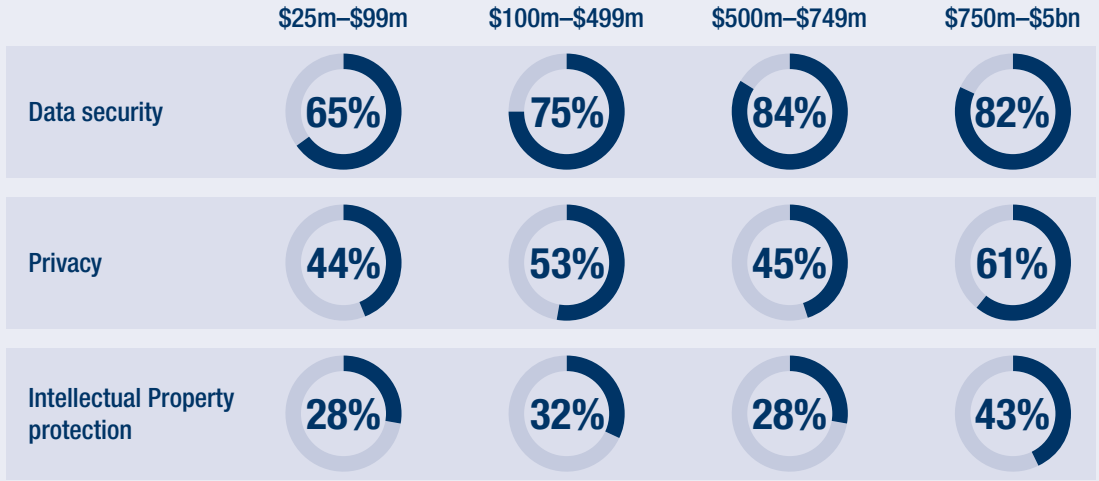
Companies across regions and industries agree that data security is their top concern influencing migration strategies, but significant differences exist in the ways large and small organizations think about cloud security and adopt systems. Among the largest organizations we surveyed (those with revenue between $750 million and $5 billion), 81% rank data security as a top concern when migrating to a cloud. At the smallest companies (those with revenue between $25 million and $99 million), the figure drops to 65%. Likewise, 43% of large companies rated compliance as a top-tier issue, compared with 33% of executives at small firms. Large enterprises are also more likely to cite intellectual property protection as a top concern (43%, compared with 28% of respondents at small firms).

Larger companies also have different priorities when it comes to choosing a service provider. While companies of all sizes are most likely to say scalability is an important quality in a cloud service provider, fully 84% of the largest companies say so. The largest companies are also more likely to say portal capabilities, additional services, and transparency into operations and performance are among the three most important qualities differentiating a service provider from others.

Of course, not all organizations are created equal. In many instances, larger organizations have more complex business and IT environments that require broader and deeper security. But the takeaway is that many organizations—particularly smaller firms—are not focusing enough on security issues.

Concerns influencing cloud migration strategies

% of respondents who say the following concerns are influencing their migration strategies "to quite an extent" and "to a great extent"



Conclusion

The cloud—like all IT systems— represents a certain level of risk. That means companies must build their IT frameworks around robust and comprehensive security, and select vendors with security in mind. Although many cloud providers deliver protection that is superior to what organizations develop internally, it is vital to map a cloud security strategy to overall IT security plans. This involves identifying potential vulnerabilities, choosing a vendor that is equipped to provide high-grade security, and ensuring that the cloud provider supports data protection across its lifecycle.

In order to reap the full benefits of the cloud, organizations must view security as a fundamental element to any and every cloud initiative. As Charles Zieres, Vice President of Technology at Preferred Hotel Group, a Chicago-based global hospitality company, puts it, "Security must come first."

About the research

This think piece is part of a large-scale research program built on a national survey of 350 business and technology executives and a series of executive interviews. To view our briefing paper and interactive infographic, visit our **project landing page**. For more project news, check out **cloudvaluepath.com**.

OXFORD ECONOMICS

windstream®
smart solutions. personalized service.