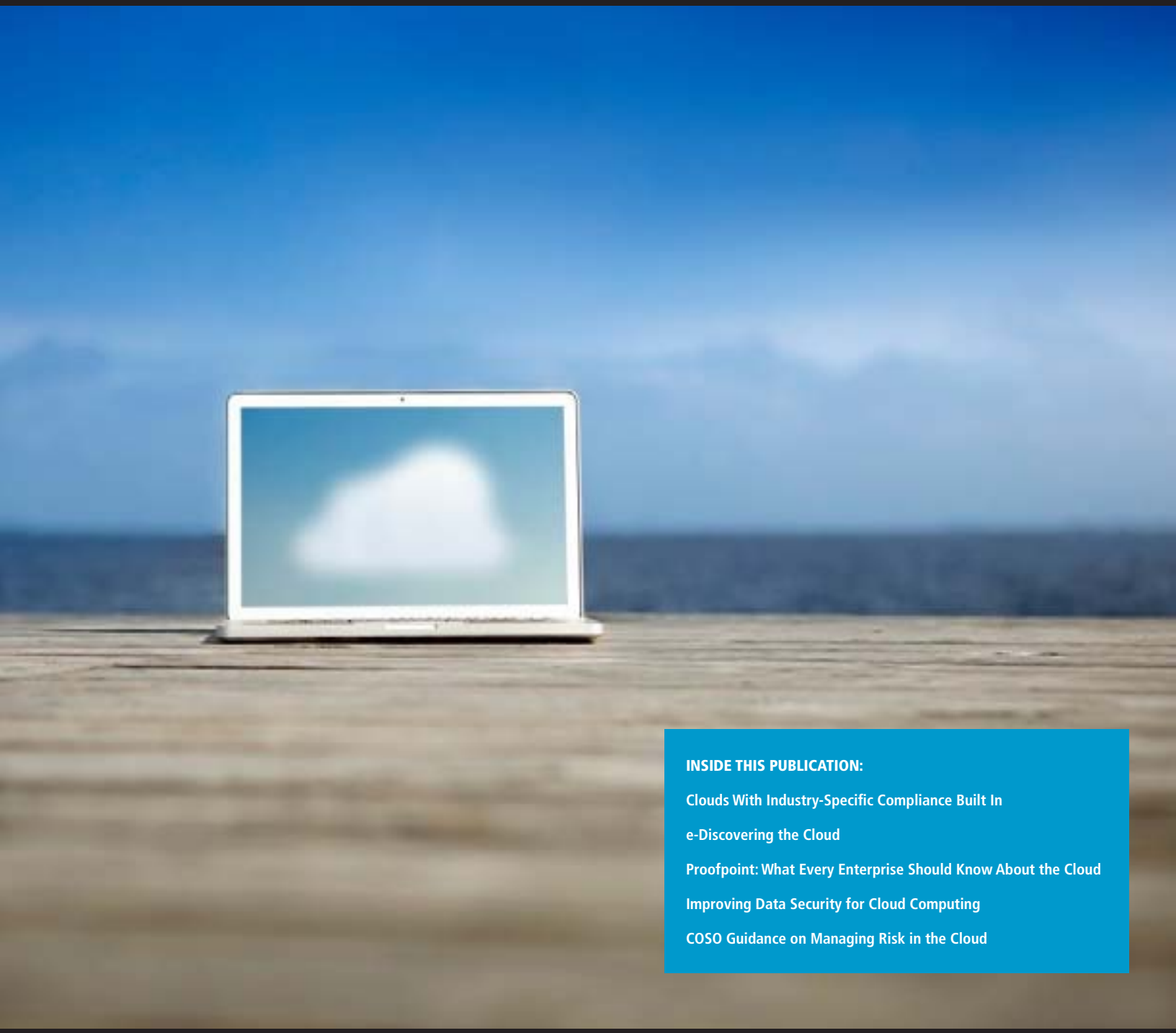
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Talking to the Cloud

Managing Risks and Improving Data Security

An e-Book publication sponsored by proofpoint

COMPLIANCE WEEK

Founded in 2002, Compliance Week has become *THE* premier GRC resource for public companies and the organizations that support them.

Compliance Weeks' magazine, Website, electronic newsletters, databases, and live and virtual events are leveraged by tens of thousands of financial, legal, audit, risk, and compliance executives.

Our mission is to help our subscribers comprehend and comply with the constantly evolving global regulations and standards to which public companies must adhere, while focusing on critical regulatory and compliance issues related to financial reporting, regulatory enforcement, corporate governance, enterprise risk management, and related global issues.

proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information. More information is available at www.proofpoint.com.

Inside this e-Book:

Clouds With Industry-Specific Compliance Built In

By Todd Neff

The arguments for industry-specific cloud computing are becoming more compelling.

Take the pay-as-you-go cost advantages and expand-as-you-need flexibility the cloud affords, and add layers of industry-specific processing, security, and compliance. Indeed, ever since a couple of high-profile industry-specific cloud providers emerged in 2011, such as the NYSE Technologies' Capital Markets Community Platform and SITA's ATI Cloud for the air-transport industry, industry-specific clouds –also known as community clouds–have continued to proliferate.

But it has been quieter than was the case with the initial pulse of public cloud update a few years ago, said David Linthicum, an independent cloud consultant and InfoWorld blogger. He suspects there's a reason for that. "At the end of the day, we're building what are in essence enterprise applications, just in a way that can be consumed over the Internet, and I think people are realizing it's no big whoop."

> "What makes the cloud attractive is that it's more a utility model. It has the potential to bring costs down dramatically."
>
> Brian Bodor, Partner, Pillsbury Winthrop Shaw Pittman

So they're not tabloid fodder. But community cloud offerings do offer things a public cloud can't, not least of which is to handle tough industry-specific security and compliance requirements. As Mark Wright, NYSE Technologies' vice president of product management put it, "We take great pride in being a very un-public cloud." Community clouds like that of NYSE Technologies come with assurances that cloud-stored data will remain safely in a specific country, region, or even data center. They are housed either in private clouds—server farms owned and controlled by the entity offering the community cloud service—or they provide secure gateways into the clouds of hired-gun providers. And they are often tailored to satisfy specific, existing business needs.

Nasdaq OMX's FinQloud, launched late last year, is one example. FinQloud's main pitch is dealing with SEC 17a-4 record retention rules. Rather than securities broker-dealers having to store seven years of transaction data, they can send it off to FinQloud. Customers enter through a secure NASDAQ gateway, and NASDAQ servers hold the encryption keys. But the data itself resides on the Amazon Web Services cloud. NASDAQ officials say the service saves clients 80 percent in data-storage costs.

Compliance issues have pushed financial industry-specific cloud far from the fingers of the public Web, says Alex Tabb, a partner with capital markets research and advisory firm Tabb Group.

"They are for all intents and purposes segregated from the rest of society—no one in capital markets is going to put this kind of important, very strategic, confidential information anywhere near where people can get access to it," Tabb says. Compliance issues, he adds, remain a top concern among financial players looking at any sort of cloud solution.

NYSE Technologies' Community Platform resides entirely in the secure confines of NYSE data centers, in which clients have been comfortable for decades. Once inside, investment banks can crank out regulatory reports, hedge funds can test and validate strategies, and financial firms of all sizes can test custom applications.

Wright says customers are looking for a range of services. Some seek straight infrastructure as a service (IaaS) on which to set up their own private clouds. Others make use of software bundles NYSE has developed to quickly build out, say, a new trading solution. Others focus on disaster recovery, or communications compliance, or SEC 17a-4 record storage, he says. Client firms may still be wary of a wholesale outsourcing of their servers, Wright says, but for things like record retention, "Can you unload that for me?" is a common refrain.

The list of financial industry cloud players is growing—Bloomberg Vault and Thomson Reuters Elektron being among the notable entrants. Linthicum says he's consulting with several financial firms developing community cloud services. Part of the challenge for community cloud shoppers, Tabb says, is figuring out which service best aligns with their goals. Smaller firms are paying close attention to community clouds, he says, seeing them "as a way of getting away from the very expensive infrastructure they need —they can just go to the cloud and pay based on what they use."

But bigger players are just as interested, Wright says. "There's a trend toward bigger shops and more aggressive moves," he says. "Clients have known for years that they need to rethink their cost structure. They need to consider managed services more broadly. What can they push out of their shop to save money? They can't do it all themselves."

The Nasdaq OMX model of picking a specific battle represents a common community cloud theme, says Mike West, vice president at distinguished analyst at Saugatuck Technology.

He cites the example of Pixar's RenderMan On Demand cloud offering. Rendering digital animation is processing in-

tensive, the costs of high-end servers contrasting with the "feast or famine" nature of filmmaking. IGT Cloud is another example of cloud-based software as a service (SaaS). It gives casino operators cloud-based access to hundreds of games in IGT's game library.

"Here's a model that I think makes a lot of sense for a lot of industries," says West.

Community clouds could make themselves attractive in other ways. There could be community cloud platforms that help retailers develop PCI- and financial-regulation-compliant systems, including shared databases for things like fraud detection, West says.

So where else are these community clouds? The financial industry is the hotbed, Linthicum says, but healthcare players are also increasingly interested. "Manufacturing doesn't have the money. Retail doesn't have the money," he says. "I think healthcare really doesn't have the money, but they have to do it to survive."

Easing the Transition

Transitioning to the cloud can be tough for these institutions, though. While cloud-based options like CareCloud and Optum Health Care Cloud exist, an institution may be running a major electronic health record like Meditech or Epic in-house in addition to multiple tangential systems and data warehouses.

"That's kind of the untold story in the cloud world," Linthicum says. "Most are pushing back on the cloud not because it's too risky or because of compliance issues, but they don't have the money."

Community clouds are also a hot topic among governments, particularly now that one of the biggest compliance-related issues has been removed from the equation, says Brian Bodor, a partner with law firm Pillsbury Winthrop Shaw Pittman in Washington D.C.

Amazon's GovCloud and others have found ways to ensure that government data stays in the United States, Bodor says. In Amazon's case, the offering also meets federal encryption requirements and complies with U.S. International Traffic in Arms Regulation (ITAR) requirements. That's good news for governments and agencies facing budget shortfalls and for whom capital investment is often trickier to budget than operating expenses, he adds.

"What makes the cloud attractive is that it's more a utility model," Bodor says. "It has the potential to bring costs down dramatically." ■

THE CLOUD IN A NUTSHELL

Industry-specific, a.k.a. community clouds, can involve levels 1-4, and sometimes, as is the case with NYSE Technologies, all four. Sagautuck Technology explains the different levels below.

Level	What Is It?	What Is In It?
Level 4	Cloud Business Service and Operations	Cloud Strategy, Business Process Outsourcing, Managed Services, Systems Integration
Level 3	Cloud Business Solutions	Software-as-a-Service (SaaS), hosted offerings, vertically purposed solutions
Level 2	Cloud Platforms & Hubs	Platform-as-a-Service (PaaS), other platforms, e.g., Analytics, Mobility, Social Networking, Integration, Security
Level 1	Cloud Infrastructure	Infrastructure-as-a-Service (IaaS), e.g., Computer/Storage, and Private Clouds
Level 0	Cloud Technologies	Basic Hardware, Software, Middleware Networking

Source: Saugatuck Technology.

e-Discovering the Cloud

By Todd Neff

A Fortune 20 company was all set to move its e-mail and collaboration systems to the cloud. The business case was obvious: It would be cheaper, more scalable, and easier to manage. The chief information officer was about to pull the trigger.

Only one problem: The company hadn't considered the move's implications on e-discovery. Where would the data be stored? How quickly could it be accessed, analyzed, and removed for delivery to the opposing litigant? When would e-mails and other data be deleted? How could they prove that documents had not been manipulated?

Barry Murphy, principal analyst with the consulting firm eDJ Group and a contributor to *eDiscovery Journal*, raised some of these questions. While the cloud is still in the company's plans, it has scaled back and slowed the migration. e-Discovery concerns "prevented the IT team from going out and saying, 'Here's our mail—just manage it for us,'" Murphy says.

Just as the varieties of cloud are diverse—private, public, and hybrid; involving infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS)—so too are the cloud's implications on e-discovery. There are two important e-discovery considerations with respect to the cloud. The first relates to dealing with corporate data being stored in the cloud. The second has to do with how vendors harness cloud technology to collect, process, and review data destined for legal proceedings.

If the 500 information managers responding to the Association for Information and Image Management's information governance survey are any measure, how e-discovery plays out in the cloud should be of broad interest. More of those surveyed listed "excess litigation costs or damages resulting from poor recordkeeping" as a top-three information-governance risk than any other concern. At the same time, however, 53 percent remained reliant on manual searchers on file shares, e-mail, and physical paper records, said Doug Miles, head of market intelligence for the AIIM.

Also, he said, for all the popularity of the cloud, Corporate America does not appear to be condensing its sensitive data into it. Nearly half of AIIM survey respondents said they wouldn't—or probably wouldn't—move to the cloud for their records, with 38 percent saying they're waiting for more mature security and reliability. Just 16 percent already had their records in the cloud or planned on moving them there soon. "Most analysts would say, 'Everybody's on the cloud already, aren't they?'" Miles said. "Well, no."

The reticence may have something to do with the many fronts of uncertainty inherent in emerging technology. "The question with cloud computing is whether it's going to make e-discovery harder or easier, more or less expensive, and offer more or less control," says Todd Nunn, a partner with law firm K&L Gates. "It can really go both ways."

> "The question with cloud computing is whether it's going to make e-discovery harder or easier, more or less expensive, and offer more or less control."
>
> Todd Nunn, Partner, K&L Gates

Nunn and other experts stressed that companies should build e-discovery needs into service-level agreements (SLAs) before sending their data to the cloud. "You can see it as a train wreck waiting to happen if you don't think about these things in advance," says Michael Lackey, a partner in charge of law firm Mayer Brown's Washington D.C. practice.

Avoid click-through agreements if at all possible, says David Stanton, a partner with law firm Pillsbury Winthrop Shaw Pittman. These are boilerplate, legally binding "contracts of adhesion" that automatically go into force when you click past the fine print without really reading it anyway. Under such agreements, e-discovery has the potential of becoming cumbersome, expensive, or both, Stanton says. The good news, though, is that, "If you're a larger company with a significant amount of data, you can bypass it and call the company," Stanton adds.

In negotiating with a cloud provider, getting answers to a few key questions can help put corporate attorneys at ease, says Michele Lange, director of thought leadership at Kroll Ontrack, a provider of data management and recovery services. First, assess the cloud provider's reputation for integrity, she says. Then ask: Where will the data be located? How can we access it? How will it be preserved? How will it be secured?

Murphy says SLAs should include language as to how

quickly e-discovery-related searches should run and how quickly the data will be available to the legal team. While no cloud provider will offer full indemnification, "If you get sanctioned $300,000 for not producing data quickly enough because the cloud vendor fell and couldn't do it, you can build in some ways to recoup costs," he says.

Other contractual stipulations might include ensuring that e-mail metadata is preserved, specifying copyright ownership of your data, clarifying country locations and cloud-service sub-contracting arrangements, and providing notification of subpoenas, Stanton added.

Sophisticated cloud providers understand e-discovery, are responding, and are already marketing to e-discovery needs, Lackey says. That marketing may not have much behind it, though, warns Stanton.

"You'll see marketing materials that say 'e-discovery compliance' and it doesn't mean anything. They don't know what they're doing," Stanton says. The issue, he says, is that most cloud providers are in the business of getting data in and getting you access to it—and not in getting a lot of data out quickly. There may or may not be a mechanism to extract it. Or if there is a mechanism, it might be an exorbitantly priced add-on, he adds.

There's a good way to avoid this pitfall, Lackey says. "I would have them actually demo the technology. There are a lot of claims out there in the technology space, and a lot of times they don't live up to the hype," he says.

And if your data's already in the cloud? A demo may be the part of the answer here, too. Stanton suggests working quietly with the cloud provider's on-the-ground staff to run a hypothetical e-discovery test case to see what's going to happen if they need to pull e-mails from, say, 15 people.

e-Discovery as a Service

The second part of the e-discovery-in-the-cloud story—vendors using the cloud for e-discovery document processing and analysis—is more straightforward. The appeal of moving e-discovery processing to the cloud using the SaaS model is the appeal of the cloud itself: no hardware or software to buy, no IT infrastructure to maintain, scalability for surprise lawsuits, and, presumably, lower cost. Often, it's an extension of traditional e-discovery outsourcing arrangements. "This isn't anything new despite vendors making it sound like it's new," says Kroll Ontack's Lange.

In the past, though, the processing engines driving e-discovery often ran on dedicated boxes. With the cloud, that process can move to virtualized services of an e-discovery vendor's private cloud or to the public cloud itself.

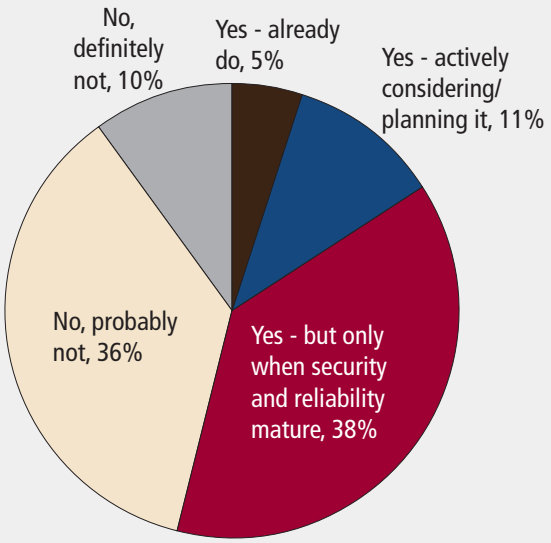
An example of the latter is X1 Discovery, whose software can be leased on demand in Amazon Web Services' cloud. The key, says X1 Discovery CEO John Patzakis, is that the SaaS provider has good data connectors into target cloud sites. "It's no different than where you have a solution that connects into a Sharepoint or Documentum repository," Patzakis says.

Also central to technologies like those of X1 Discovery and Kroll Ontrack's Verve is the intelligent, cloud-based filtering of huge numbers of documents across many virtual servers using predictive-coding logic. It's saving countless hours of attorney time already, and that's only the beginning.

"It's not a question of whether e-discovery will primarily live in the cloud," says Lange. "It's a question of when." ■

MOVING TO THE CLOUD?

Respondents to the AIIM information governance survey were asked if they would consider adopting a Cloud/SaaS system for recordkeeping. Below are their responses.



Source: AIIM.

What Every Enterprise Should Know About the Cloud

Today, it is clear that IT organizations are moving quickly to take advantage of the cost and manageability benefits of the cloud. But many do so without engaging critical stakeholders that must manage demanding use cases including e-Discovery and regulatory compliance. Involving these stakeholders in the due diligence process is critical to ensure that cost and management benefits are not achieved at the expense of data protections that must satisfy the rigors of litigation and regulatory inquiry.

Two important trends in the enterprise are operating at cross purposes:

» Enterprises are investing heavily in the cloud. They're using infrastructure from a broad range of cloud vendors, and they're replacing on-premise applications with Software-as-a-Service (SaaS) applications. By moving to the cloud, enterprises hope to increase operational agility while lowering IT costs overall.

» Enterprises are also attempting to increase control and achieve greater efficiency around e-Discovery and regulatory compliance. Instead of continuing to operate reactively to e-Discovery and regulatory inquiry, they are looking for tools that enable internal process improvement. The cost savings can be substantial, and the reduction in risk can help to avoid costly sanctions and damaged reputations.

But some enterprises are finding that their investment in cloud-based technology can be at odds with objectives for greater efficiency and control. The cloud can make IT operations fast and nimble, but it doesn't necessarily make information easier to discover or practices easier to defend. On the contrary, cloud computing can make information searches more complex, time-consuming, and difficult. Today, the majority of cloud providers would be unable to satisfy the stringent security, privacy, and data access requirements of corporate counsel and other stakeholders responsible for managing legal risk exposure.

IT departments need to engage legal and compliance stakeholders in due diligence of cloud service providers, so that new cloud initiatives don't expose the organization to e-Discovery or regulatory risk.

The Cloud Challenge: Total Cost of Ownership and Efficiency Versus Information Risk

The uptake of cloud-based technologies is undeniable. Gartner recently predicted that by 2016, 80 percent of organizations will move to a cloud model for enterprise information archiving, up from 30 percent in 2011.[1] The reasons are clear: opportunity for significant cost savings, fewer IT hassles, and greater operational agility. Enterprises can launch cloud services within minutes or hours, crunch data for business analysis, clinical trials, or other compute-intensive projects—sometimes with an annual cost per user that is cheaper than buying a cell phone. Many have experienced an overall cost of ownership that is 40 to 60 percent lower than the cost of managing an on-premise system.[2]

The second trend is enterprises seeking greater control and efficiency over critical processes including legal discovery and response to regulatory inquiry. Today, many organizations continue to respond to e-Discovery by relying upon outside service providers to search, collect, and preserve information from sources such as back-up tapes, PST files, and imaged hard drives. Service providers must painstakingly hunt through mountains of information—for a price that typically ends up running several hundreds of dollars per gigabyte.

The Conflict: Data Protection in the Cloud

Some enterprises have discovered that their investment in the cloud raises a new set of concerns over how they can improve control and lower cost around critical e-Discovery and compliance processes. Cloud computing makes IT operations fast and nimble, but it doesn't necessarily make information easier to discover, review, or report. In some cases, cloud computing can make the search, collection, and review of information more complex, time-consuming, and difficult.

IT Departments Are Ill Prepared

IT has traditionally used on-premise systems to identify and collect large volumes of stored data for legal or regulatory purposes; they could influence the hardware, software, and storage investments to ensure that capacity was available to meet requirements. This process is not always cost effective or timely but it allows IT to respond when issues arise.

With cloud-based solutions, the situation changes drastically. There are a lot of questions that need to be asked to make sure your data is protected and easy to access. When large data exports are required, does your provider have a Service Level Agreement (SLA) and a response time that will be acceptable to your stakeholders? Have you insisted on reviewing audited SSAE-16 certifications to understand underlying cloud service operations and procedures for recovery when data outages occur? Did you consider whether the cloud provider has an established process to recover historical data that has been corrupted? Is it possible that your data could be co-mingled with another customer's in an unprotected multi-tenant infrastructure? How will you retrieve data if the cloud provider goes out of business?

1 2012 Gartner Magic Quadrant for Enterprise Information Archiving

2 Proofpoint study, based upon analysis of over 50 archive customers that had migrated from on-premises systems from 2010 to 2013.

proofpoint

Signing up with a cloud service provider that lowers capital expense can turn into a financial nightmare if the service provider is unable to protect your information and allow for easy access when that information is required.

Assessing the Data Protection of a Cloud Service Provider

Investing in cloud-based solutions requires that IT, legal, and compliance teams collaborate to assess cloud service in these three key areas:

- Data Preservation
- Data Collection
- Data Integrity and Authentication

Table 1: Assessing Data Protection Capabilities of Cloud Vendors

REQUIREMENT	COMMON SITUATION	PROOFPOINT SOLUTION
Data Privacy	Virtually all cloud providers have some chance of inadvertent third-party access or disclosure due to data comingling and access controls.	Rigorous safeguards to protect data integrity including SAS 70 – Type II, SSAE-16 and FISMA certification. Proofpoint's unique and patented DoubleBlind™ Key Architecture (DBKA) ensures separation of the key from the data, leaving the customer in control of the keys. Proofpoint never has ability to access customer data.
Data Location	Many cloud providers cannot provide location assurance.	Proofpoint provides assurance that data is always maintained in the jurisdiction specified by the customer (e.g. US, Canada, or EMEA).
Data Security Protection	Virtually all cloud providers access customer data "in the clear," increasing the potential for breaches and lapses in security.	DBKA, SSAE-16, FISMA – for archiving service, not just data center (unique in industry), ongoing audited security protocols are part of Proofpoint's core business.
Data Integrity	How many copies of the data does the provider store and how often does it make ongoing integrity checks?	Data stored in paired but geographically distributed data centers. Ongoing data fingerprint check ensures that messages can be recovered.
Data Accessibility	Some cloud providers do not provide 24/7 data access.	Search SLA–data is always accessible for customer use, with fully automated, audited processes for defensibility.
Data Recovery	Some cloud vendors charge hefty fees to export data and leave the service. This can lead to a sub-optimal customer experience and product roadmap.	Ongoing self-service provided to customers for data export; optional professional services available.

Conclusion

Through the collaboration and joint due diligence of IT and legal experts, enterprises can take full advantage of cloud computing services while remaining confident that they can meet all the requirements of ESI preservation and e-Discovery.

Proofpoint Enterprise Archive™ offers the most advanced discover and compliance features and the highest performance in an easy-to-use solution (see Table 1 above.)

Visit www.proofpoint.com/archivedemo to see the Proofpoint Enterprise Archive™ solution in action.

About Proofpoint, Inc.

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information. More information is available at www.proofpoint.com.

proofpoint™

Improving Data Security for Cloud Computing

More challenges face companies looking to mitigate data security risk

By Jaclyn Jaeger

The advent of cloud computing and mobile devices has, of course, dramatically changed the way employees access, use, and share information, yet the related security risks continue to frustrate IT professionals.

In fact, a "Global Study on Mobility Risks" conducted by the Ponemon Institute reveals the degree to which mobile devices are circumventing enterprise security and policies. According to the survey of more than 4,000 IT practitioners in 12 countries, 77 percent said the use of mobile devices in the workplace is important to achieving business objectives, but 76 percent also believe these devices put their companies at risk.

"We are going through a massive transformation in our industry," said Mark Benioff, CEO of Salesforce.com, at an RSA Conference in San Francisco. This new workforce is "more open, transparent, and collaborative."

At the same time, there are no easy solutions to solve the security risks, even while pressure mounts to mitigate those risks. "We're being required to offer more services, mobility, and access while at the same time dealing with more requirements around governance and compliance," said Symantec CEO Enrique Salem at the conference.

A "lockdown mentality" is not the answer," said Salem. "We need to stop saying 'no' and partner with our user community. This new world cannot be a choice between social versus secure; it has to be both," said Salem. The new world of doing business means enabling interconnectivity, as well as allowing for "strong governance, compliance, and controls."

That push for access to social media platforms and mobile apps is driven by a young generation that has never been tied to a desktop system. Salem described how the "digital native" generation, in particular, has forever changed the way companies conduct business. Typically born in the 1990s, digital natives have never known a time before the Internet or mobile devices.

Digital natives readily turn to their mobile devices, social networking sites, and the cloud to solve problems, rather than obtaining information from a single source, such as a search query. "This is the future of business," said Salem.

While security problems still abound, great progress is being made toward getting them solved. Salem offered a list of three questions companies in every industry must think about to move forward:

- How do we manage online identities when our employees maintain dozens?
- How do you protect information when the workforce shares information freely?
- How do we keep track of a substantially higher volume of online activity?

"If we can't answer these questions, it will be a barrier to the new world of business," said Salem. He described the need for an "advanced persistent protection" plan made up of four essential pillars:

- Reliable early warning systems that allow you to understand when a new threat is potentially going to attack;
- State-of-art protection, one that recognizes threats without affecting the corporate infrastructure;
- Fast remediation, solutions that can move faster than the threat can spread across the company; and
- A response plan that includes enforcement officials that can help with an ultimate solution.

Companies still have a long way to go, however, when it comes to adopting necessary security controls and enforceable policies. According to the study, only 39 percent have the necessary security controls to address the risks, and only 45 percent have enforceable policies.

Part of the problem is that employees don't always follow the controls and procedures. In fact, 59 percent of respondents report that employees circumvent or disengage security features, such as passwords and key locks, on corporate and personal mobile devices. During the past 12 months, 51 percent of those companies experienced data loss resulting from employee use of insecure mobile devices, including laptops, smartphones, USB devices, and tablets. "It's clear that employees are deliberately disabling security controls, which is a serious concern," said Larry Ponemon, chairman and founder of the Ponemon Institute.

And the continued migration to mobile devices will only make matters worse. "Tablets and iOS devices are replacing corporate laptops as employees bring-their-own-devices to work and access corporate information," said Tom Clare, senior director of product marketing management of security provider Websense, which sponsored the study. "These devices open the door to unprecedented loss of sensitive data. IT needs to be concerned about the data that mobile devices access and not the device itself."

The study indicates that companies often don't know how

and what data is leaving their networks through non-secure mobile devices, which increase rates of malware infections. Fifty-nine percent of respondents reported that over the last year, their companies experienced an increase in malware infections as a result of insecure mobile devices in the workplace, with another 25 percent unsure if they have or not.

"As mobile devices become more pervasive and more employees bring their own smartphones and tablets to work, IT is being challenged like never before," said John McCormack, president of Websense, a data security firm. "They need to immediately protect data, and they need to establish and enforce security practices and policies."

Traditional static security solutions such as antivirus, firewalls, and passwords are not always effective at stopping advanced malware and data theft threats from malicious or negligent insiders. "You can be a super well-prepared company for yesterday's threats with a great security posture looking backward, and yet you can be completely unable to defend against these new targeted attacks," says Kevin Epstein, vice president of product marketing at Proofpoint.

New Security Tools

To prevent security threats, Christopher Young, senior vice president at Cisco Systems described the need for more effective firewalls that can track data as it enters and leaves a company's systems. Authentication of data also needs to be altered, so that it is as close to single sign-on as possible, but flexible enough to work across a variety of platforms, added Salem.

Companies already have available the tools they need to achieve greater visibility. "Today we can access standard language that is directly embedded in routers and switches that automatically enforces our policies," said Young, who also spoke at the RSA event. By doing so, the network can determine several factors, including:

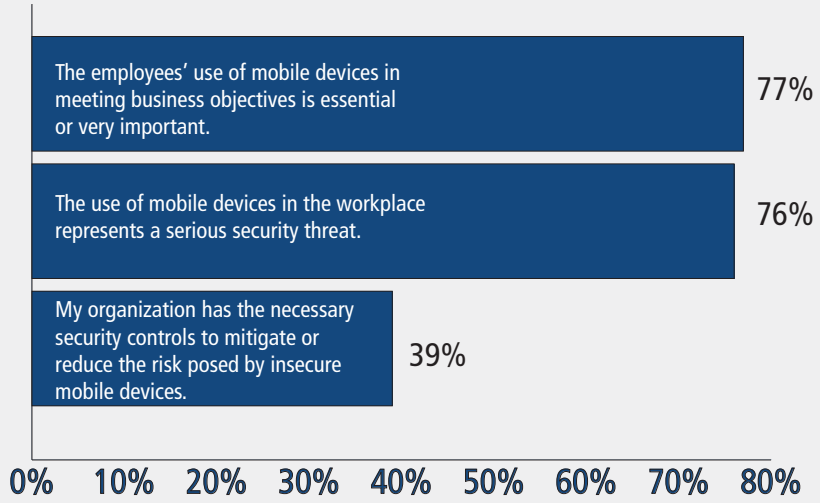
- How is that device connected—via Ethernet or wireless?
- What's the device: a PC, iPad, iPhone?
- What is the posture of that device: Is it infected, or is it clean?
- Where is that device connected from, and when?

Administrative burdens on users also must be reduced. Data that leaves the cloud should automatically be tagged, and cloud audit trails need to be set up and monitored, said Salem. Employees' access to accounts also should be disabled after they leave the company.

"In a world where users are bring their own devices to work and where user names and passwords, even the strong ones, are easily compromised," Young added, "our only way forward as an industry is to deliver increasingly granular, context aware, and forced control via the network." ■

MOBILE DEVICE RISK

Below is a chart from the Ponemon Institute study that shows respondents' perceptions about the use and risks of employees' mobile devices (strongly agree & agree responses combined):



Source: Ponemon Institute.

COSO Guidance on Managing Risk in the Cloud

By Jaclyn Jaeger

Companies working to assess and mitigate the risks that result from cloud computing are getting some much needed help.

The Committee of Sponsoring Organizations (COSO) published guidance on the topic in the paper, "Enterprise Risk Management for Cloud Computing." The guidance leverages the principles of COSO's *Enterprise Risk Management—Integrated Framework* document to help management and boards better understand the risks and opportunities presented by cloud computing.

"When you engage a third-party cloud service provider, you ultimately are inherently taking on some of their risk," says Warren Chan, co-author of the paper and a principal at Crowe Horwath. What this publication provides is an "adaptation of the well-established COSO 2004 ERM framework" so that senior management can clearly understand the risks associated with their cloud decisions and the top questions they need to ask, he says.

The paper provides detailed descriptions of the top risks associated with cloud computing, including:

Legal and compliance risks: Cloud service providers can create legal liabilities for their clients if they neglect or fail to fulfill their responsibilities. Additionally, the physical location of data—sometimes obscured in cloud computing arrangements—can raise concerns about legal ownership, availability, and privacy if the data is moved across state or national borders.

Uncertainty about where data resides raises questions about what laws the company is subject to in running its business transactions in the cloud. The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act, and a web of complex state, federal, and country-specific data privacy and protection regulations can apply to data that physically resides in the relevant jurisdiction. The COSO paper recommends that companies review contract terms to ensure compliance with applicable data protection laws.

Cloud service provider viability: Many cloud service providers are new to the business. As a result, companies that enlist their services "might have to face operational disruptions or incur the time and expense of researching and adopting an alternative solution, such as converting back to in-house hosted solutions," should the provider struggle, the paper stated.

"The cost of switching providers is a hassle," says Ron Woerner, a professor and director of cyber-security studies at Bellevue University's College of Science and Technology. Companies should understand the risks of transferring their services and data from one provider to another, and how to most easily achieve that, he says.

Reliability and performance issues: "System failure is a risk event that can occur in any computing environment but poses unique challenges with cloud computing," COSO says.

Just days following the publication of COSO's guidance, for example, Amazon's cloud computing service suffered widespread outages, disrupting hundreds of companies that depend on Amazon every day for data storage.

Some of the questions companies should ask include: Does the cloud service provider have backups of each data center? Does it have power generators available? What is the history of services outages? "A lot of businesses haven't considered these sorts of questions when going to a cloud provider," says Woerner.

How much risk the company is willing to take on in such situations depends on the types of data being moved to the cloud and each company's management team. "You have to find alternatives based on your particular risk profile and the level of comfort your specific situation requires," says Chan.

Management Considerations

Well before choosing a cloud service provider, the COSO paper stresses that deciding whether to move data to the cloud at all requires an in-depth evaluation by management. This includes an evaluation of both the internal environment—the state of business operations, IT costs, and the backlog of IT projects—and external environment, including laws and regulations and competitors' use of cloud computing.

As management and boards contemplate the company's cloud computing position, some central questions to consider include:

- What is management's overall view of outsourcing functions?
- Does the organization anticipate rapid growth that might require using cloud solutions?
- Is the organization in a mature market that might require using cloud computing to save costs to remain competitive?
- What is the capability and maturity of the organization's current IT function?
- Are the organization's operational functions and processes formalized enough to allow for a change in the underlying technology platform?
- Who should be involved in the evaluation process, and who makes the decisions?

When deciding to engage with a cloud service provider, negotiation is important. The contracts of most cloud service providers are generally geared toward a mass market, says Chan. The preferred position for most cloud providers is to offer a one-size-fits-all standard solution that requires a minimum amount of tailoring for each customer. "The same formula is going to be used in their contracts," he says.

At minimum, management should demand a right-to-audit clause in each contract. Management should further require that the cloud service provider publish either bi-annually or annually their Service Organization Control (SOC 2) reports, which are audit requirements designed to assure users that a cloud service provider has an effective control system in place to effectively mitigate operational and compliance risks. Preferably, cloud contracts should include a right-to-audit clause.

"Unfortunately, there are a fair number of cloud service providers that do not publish SOC reports and do not grant right-to-audit clauses," Chan says. The risk here is that if you engage a cloud service provider that doesn't allow you to audit them and doesn't publish SOC reports, "you're somewhat functioning in the dark regarding what controls are in place and how good those controls are," he says.

Cloud customers should also be alert for pricing change type clauses in their contracts, Chan adds. When or how often can the provider institute a price hike—annually, bi-annually, or is it not stated?

ERM Measures

A contract cannot prevent all risks, however, so enlisting a cloud services provider may mean making changes, or accepting a different level or set of risks, to the company's business operations. "The framework put forth in COSO's 'Enterprise Risk Management—Integrated Framework' has established a common language and foundation that can be used to construct an effective cloud governance program tailored specifically for a given cloud solution," the COSO paper stated.

Performing a risk assessment while engaging the services of a cloud provider is not as simple and straightforward as performing a risk assessment on your organization's own IT systems, says Jim Hietala, vice president of security for the Open Group. "It's important not to overlook that," he says.

For companies that already have risk-management programs in place, cloud computing is one more risk to think about, says Chris Harding, who leads the Service-Orientated Architecture Work Group and the Cloud Computing Work Group at the Open Group, a forum of customers and suppliers of IT products and services. The challenge is how to plug that risk into existing procedures, says Harding.

Even if management has no interest in cloud computing, companies should still have controls in place to prevent and detect employees' unauthorized use of cloud services. "It comes down to policy and education of the workforce," says Hietala. For example, the company may choose to limit employees' use of Dropbox or Google's IDrive, downloadable applications which allow for the unsecured sharing of documents across the Internet.

Before long, most companies may not be able to avoid the cloud. Cloud computing is projected to be a $140 billion industry by 2014, according to technology research firm Gartner. Most every company will use some type of cloud service moving forward, says Woerner. "The idea is to determine what fits best in the cloud, and what doesn't fit," he says. ■

ROLES AND RESPONSIBILITIES

The following excerpt from the COSO paper defines roles and responsibilities of management in respect to cloud computing:

Board of Directors:

- Be aware of cloud computing trends and understand management's perspective on the impact of cloud to the industry and its business model
- Be aware and have oversight of transformative IT projects such as cloud services
- Understand how management is balancing risks with the benefits of cloud as part of its business and technology strategy
- Leverage internal audit resources for assurance that cloud initiatives are in alignment with the organization's risk appetite and controls philosophy

Chief Audit Executive or Internal Auditor:

- Perform periodic audits to evaluate the design and effectiveness of the blended control environment in which controls and processes are shared with the CSP
- Audit the CSP or review SOC reports to verify the effectiveness of CSP controls relied upon by the organization
- Perform periodic compliance audits of data residing on external clouds to verify compliance with data classification polices
- Audit CSP spend and contractual compliance
- Evaluate cloud governance

Source: COSO.

Rise above on-premise archiving solutions.

Learn how Proofpoint cloud-based archiving is more secure than on-premise solutions, with 10X faster searches and easier management.

Only Proofpoint cloud-based archiving and governance solutions address the growing need for **greater security**, **performance**, **scalability** and **cost-effectiveness**.

Visit us at: www.proofpoint.com/archive

proofpoint