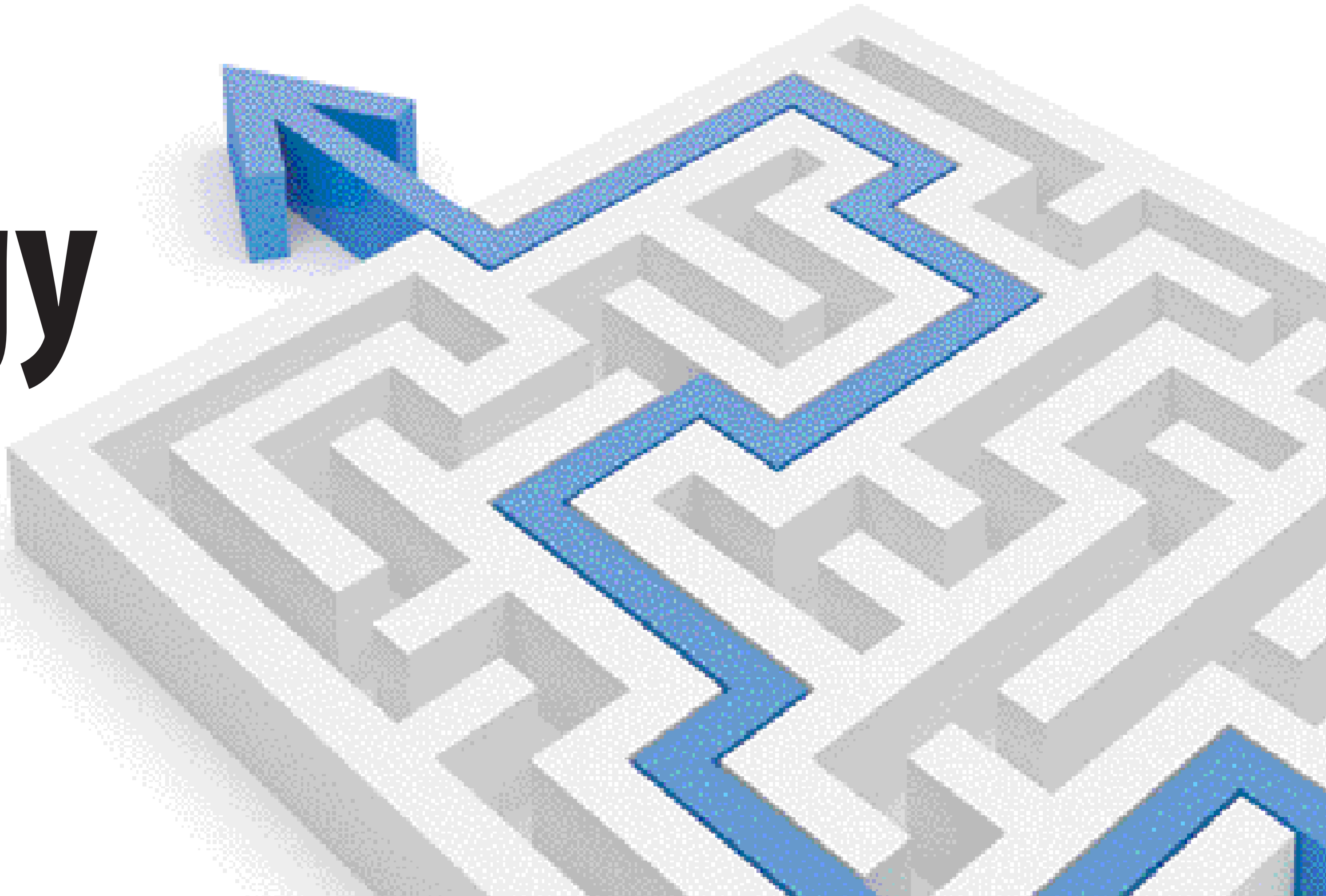
InformationWeek
Government reports
reports.informationweek.com

October 2014 $99

Next

Time to Reconsider Enterprise Email Strategy



As we pull out of a difficult time in our nation's financial history, government agencies struggle to meet information technology demands. Agencies must focus on the cloud and a strong information governance program to avoid the sort of attention recently focused on the IRS.

By Patrick Oot

Report ID: S8201014

InformationWeek Government reports

TABLE OF CONTENTS

ABOUT US

InformationWeek Reports' analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption of best practices gleaned from experience.

OUR STAFF

Lorna Garey, content director; lorna.garey@ubm.com
Heather Vallis, managing editor, research; heather.vallis@ubm.com

Find all of our reports at reports.informationweek.com.

Patrick Oot
InformationWeek Reports

Patrick Oot is a partner in the Washington, D.C., law offices of Shook, Hardy & Bacon LLP. Mr. Oot is a nationally recognized expert in e-compliance, digital investigations, electronic discovery, and information governance. He advises global financial services organizations, pharmaceutical companies and technology corporations on litigation and compliance matters. Prior to joining the firm, Mr. Oot was senior special counsel at the US Securities and Exchange Commission. He is also the co-founder of the nonprofit think tank the Electronic Discovery Institute. Mr. Oot can be reached at oot@shb.com.

EXECUTIVE SUMMARY

Cost, time, and risk. It's the demand trifecta vying for the attention of both technology professionals and attorneys charged with balancing the expectations of their clients and business units with the hard reality of the current financial and regulatory climate. Sometimes, organizations assume high levels of risk as a result of their inability to meet the costs involved in data protection. In other instances, it's time that's of the essence, as with a data breach.

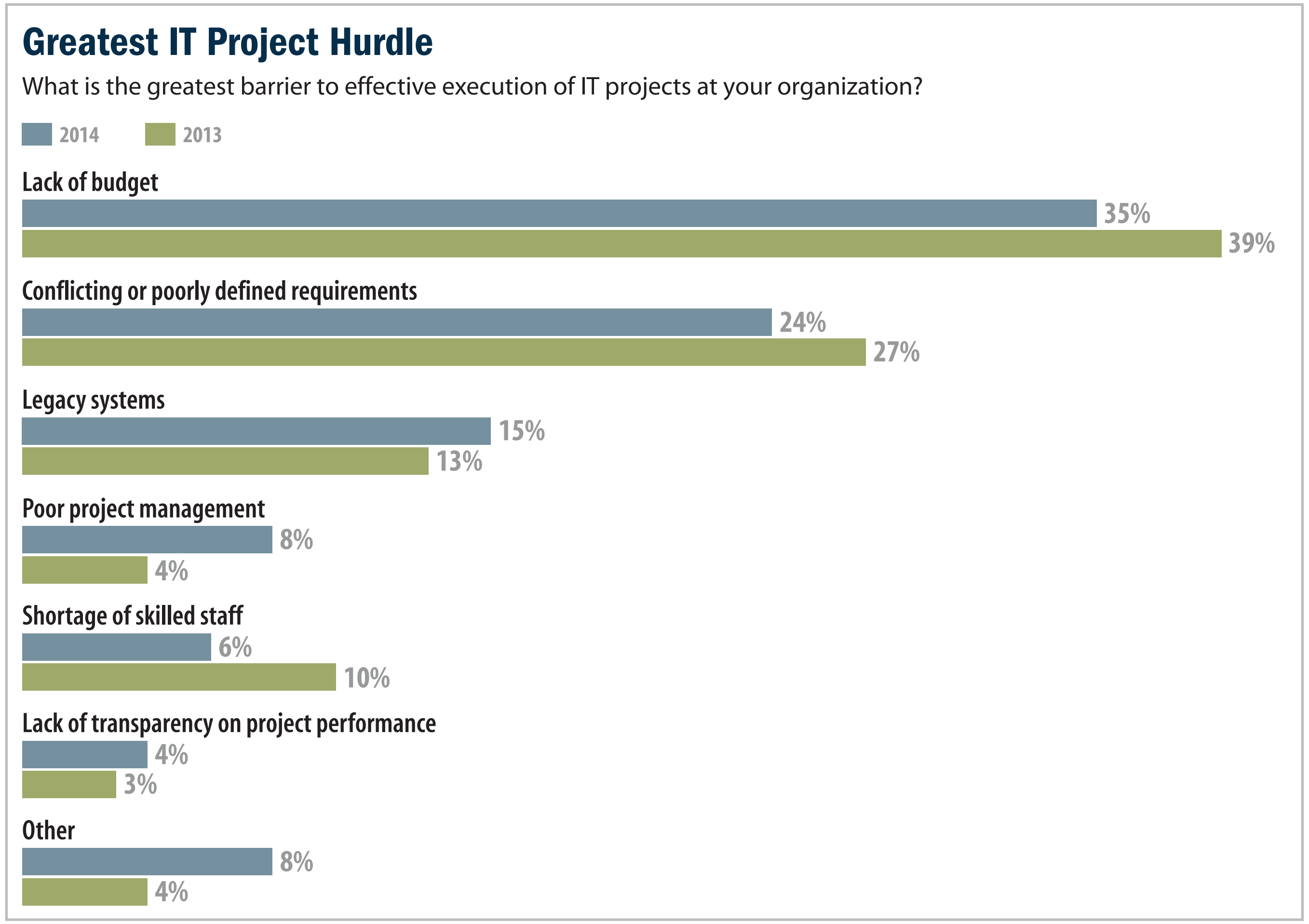
However, we must do better at information governance. The fact is, hard drives fail all the time, and modern technologies provide opportunities to balance the cost-time-risk equation. Finally, efficiently meeting e-discovery and Freedom of Information Act challenges takes more than dependable storage; you need governance. Here's how to develop a strategy.

Lost Email Brings Heavy Scrutiny

Talk about a hot seat. The hard drive disaster that led to former Internal Revenue Service official Lois Lerner's grilling by Congress over missing emails was not only painful to watch, it could have been avoided. Preserving email and other digital government records ought not to be a challenge in the era of inexpensive cloud storage and robust on-site archiving systems, yet as the IRS incident and other instances make painfully clear, evidence that auditors, investigators, and congressional committees expect to be easily accessible often is not. Even when the data is preserved in its raw state, lack of proper metadata classification of records can make evidence difficult — and expensive — to produce, even when an agency is motivated to do so.

In case you missed the excitement, the IRS learned in February that two years' worth of email messages belonging to Lerner, a key witness in a politically charged inquiry, and six additional IRS employees were lost. Long before the investigation, in mid-2011, Lerner experienced an irrecoverable hard drive crash,

Figure 1



Base: 123 respondents in June 2014 and 155 in June 2013
Data: InformationWeek Federal Government IT Priorities Survey of federal government technology professionals
R7830714/4

at the exact location where she archived important emails. The local file containing her pre-2011 email stores was gone.

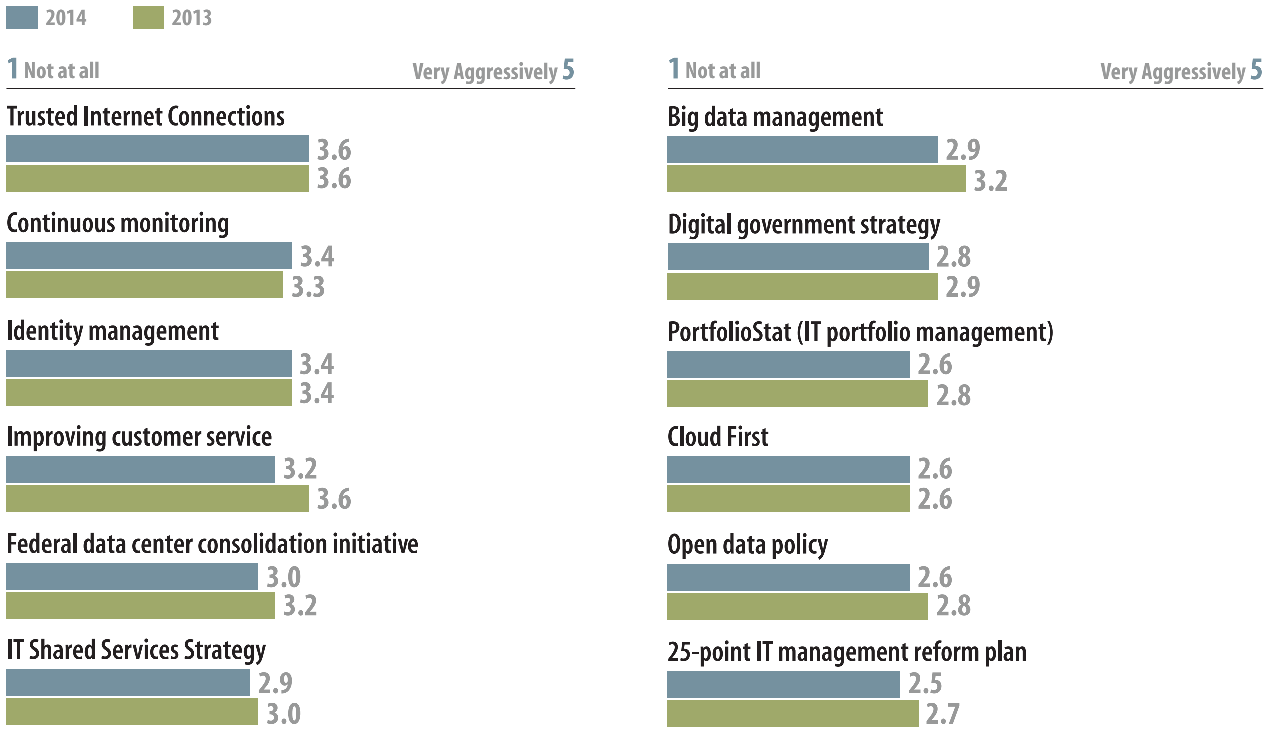
On Sept. 9, the Permanent Subcommittee on Investigations of the Committee on Homeland Security and Government Affairs issued a report summarizing its bipartisan investigation into problems with how the IRS processed applications for exempt status under Section 501(c)(4) of the tax code. I previously summarized the technology-related issues in a Law Technology News article. Essentially, IRS employees were limited to 500 MB of mailbox storage on the agency's Microsoft Exchange servers. That tight size limitation forced users to store important emails in PST folders on their local laptop or desktop PC hard drives, which are susceptible to crashes and mechanical failures. According to testimony from IRS Commissioner John Koskinen, appropriations earmarked for information technology were cut year over year, leaving no funds for system maintenance and storage upgrades.

To remediate the loss, more than 65,000 Lerner emails were produced from a mish-

Figure 2

Pursuit of Federal IT Initiatives

Using a scale of 1 to 5, where 1 is "not at all" and 5 is "very aggressively," to what degree is your agency pursuing the following federal IT initiatives?

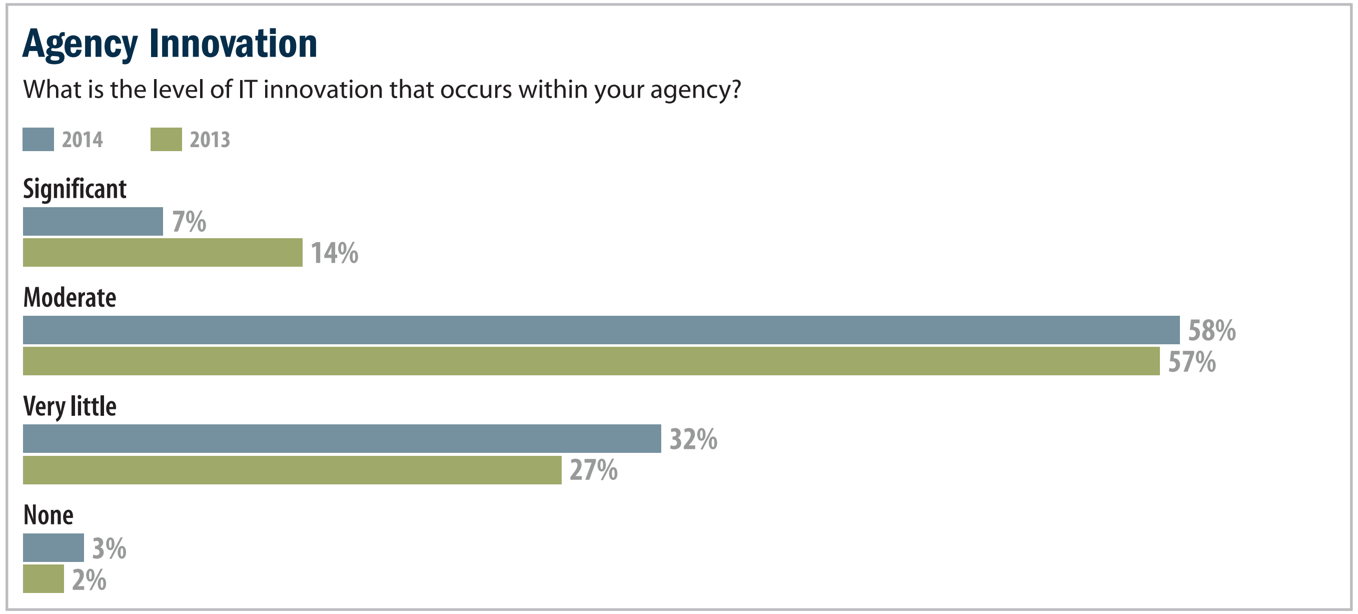


Note: Mean average ratings
Base: 123 respondents in June 2014 and 155 in June 2013
Data: InformationWeek Federal Government IT Priorities Survey of federal government technology professionals

R8030714/5

Previous Next
Table of Contents

Figure 3


Agency Innovation

What is the level of IT innovation that occurs within your agency?

Base: 123 respondents in June 2014 and 155 in June 2013

Data: InformationWeek Federal Government IT Priorities Survey of federal government technology professionals

R8030714/23

mash of sources — servers and devices, as well as emails that other employees retained from Lerner in their own email storage locations. The IRS retains daily disaster recovery tapes on a six-month cycle, but these tapes didn't reach back to the missing time period and most likely duplicate what is in more accessible media. The IRS has been in perpetual document-production mode ever since, at a cost to taxpayers of between $16 million and $18 million, according to a letter from Koskinen to the subcommittee.

The IRS's problems don't stop there. While the congressional inquiry continues, the agency faces Freedom of Information Act litigation from Judicial Watch, a self-described "conservative, nonpartisan foundation." The lawsuit requests that the district court compel the IRS to produce records of all communications regarding the processing of applications for tax-exempt status. On July 20, Judge Emmet G. Sullivan appointed Judge John Facciola, a noted e-discovery expert, to preside over the highly technological issues in the case. In a Sept. 17 motion to the court, attorneys for Judicial Watch requested that the IRS search an unidentified emergency backup system, which Judicial Watch attorneys call a component of the continuity-of-government program and that they say contains copies of the emails. The motion also states that the "Inspector General for Tax Administration is looking into whether some of these backup tapes may include the missing emails."

As of now, it's unclear if this secondary disaster recovery system even exists. If it does, Facciola might then consider whether an unintentional hard drive crash that occurred long before the FOIA request is enough reason to order a burdensome and expensive search. If anything, the Judicial Watch matter might be an opportunity to consider cost-shifting in the FOIA litigation. If the DR system does exist, a discussion of who should pay for the restoral might be warranted.

Both the IRS and Judicial Watch have their perspectives, as you might imagine.

There's no reason the situation had to come to this. It's not that agency IT teams and the firms that support them don't get the criticality of data protection. In InformationWeek's 2014 Federal Government IT Priorities Survey, disaster recovery and business continuity planning came in at No. 2 on a list of 32 IT initiatives, rated by importance and current leadership focus, behind only security. Data records management was No. 3. Meanwhile, advances in cloud storage and internal data protection products and practices mean IT has the tools to protect government data. What's often lacking is the money to follow through.

News flash: The media don't care if your agency's IT budget was cut. Simply put, it comes down to a few basic questions: How is your organization set up for litigation response, information security, and compliance? Can you meet court-imposed deadlines? Is your data secure? Do you retain the information you're required to retain under statute? IT professionals and attorneys must understand current requirements on data systems — or risk front-page attention, and not the kind that they want.

FAST FACT

35%

of respondents to our 2014 Federal Government IT Priorities Survey say lack of budget is the greatest barrier to effective execution of IT projects at their agencies.

Policy Matters

If you have lived the reality of stuffing a laptop into an overhead bin every few days, you're probably familiar with the perils of a failed spinning hard drive. Some believe hard drive failures are rare, perhaps because of the advent of solid state drives, which should help the problem going forward. In reality, disk failure appears pretty commonplace. Interestingly, some hard drive models crash more often than others. A September report by cloud backup provider Backblaze, analyzing the performance of 34,881 hard drives, revealed that some fail at a rate as high as 24.9%.

Regardless of which side of the political spectrum you fall on, the IRS situation shines a spotlight on the problems with disparate and ad hoc storage information systems, both from a user perspective and for legal teams once conflict arises. Local PSTs on hard drives that are prone to failure are clearly not the ideal storage medium for email sent by or received from key executives. However, when an organization lacks resources, making the case for better email management might be difficult — especially when appropriations limit overall information technology expenditures.

True analyses of cost, risk, and time might lead an organization to prioritize information governance programs to, hopefully, avoid a $16 million investigative goat rodeo. Such an initiative takes a combined effort from information technology professionals, records administrators, and attorneys in the office of general counsel. An enterprise information governance agenda, combined with a litigation response program, might act as a good road map for efficiency and response.

If you doubt the need for policy, think about this: IBM estimates that, every day, 2.5 exabytes of data is created globally. It's no wonder that everyone's talking about big data, or that the government is experiencing growing pains in terms of managing the deluge. Even when data is preserved in its native state, lack of proper classification of records can make evidence difficult (and expensive) to produce, even assuming an organization is motivated to do so.

Agencies must focus on the concept of *information governance* — that is "structures, policies, procedures, processes, and controls implemented to manage information at an enterprise level, supporting an organization's immediate and future regulatory, legal, risk, environmental, and operational requirements."

If you're looking to launch an information governance program, email systems are a good place to begin because email tends to be the most problematic in litigation. Bring data owners into this conversation. Retaining too much can be costly. Don't retain enough and you may end up in the crosshairs of congressional inquiries or discovery sanctions. Fortunately, the National Archives and Records Administration is addressing the retention issue, as I'll discuss. Failing to appropriate sufficient money to underpin email retention programs will make responding to inquiries and litigation not only problematic; it can create a massively expensive Humpty Dumpty project to piece together materials that would be accessible had they resided on centralized, searchable, and accessible systems.

Courts Concur: Crashes A Fact Of Life

Courts have routinely excused document production based on the failure of information systems. The current Federal Rule of Civil Procedure 37(e) provides a safe harbor "for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

For example, in Multifeeder Tech Inc. v. British Confectionery Co., US Magistrate Judge Tony N. Leung ruled that the "Court is keenly aware that wiping and encryption software are commonplace; computers crash; computers are reformatted; computers are repurposed; and data and metadata are destroyed and rendered unrecoverable both intentionally and inadvertently. The discovery rules do not accomplish justice if they are construed as a cudgel for punishing litigants who continue to use their computers to conduct business and take appropriate precautions to preserve ESI. Prudent and good-faith measures should be considered when misplacement and deletions occur. Imperfection and spoliation are not synonymous."

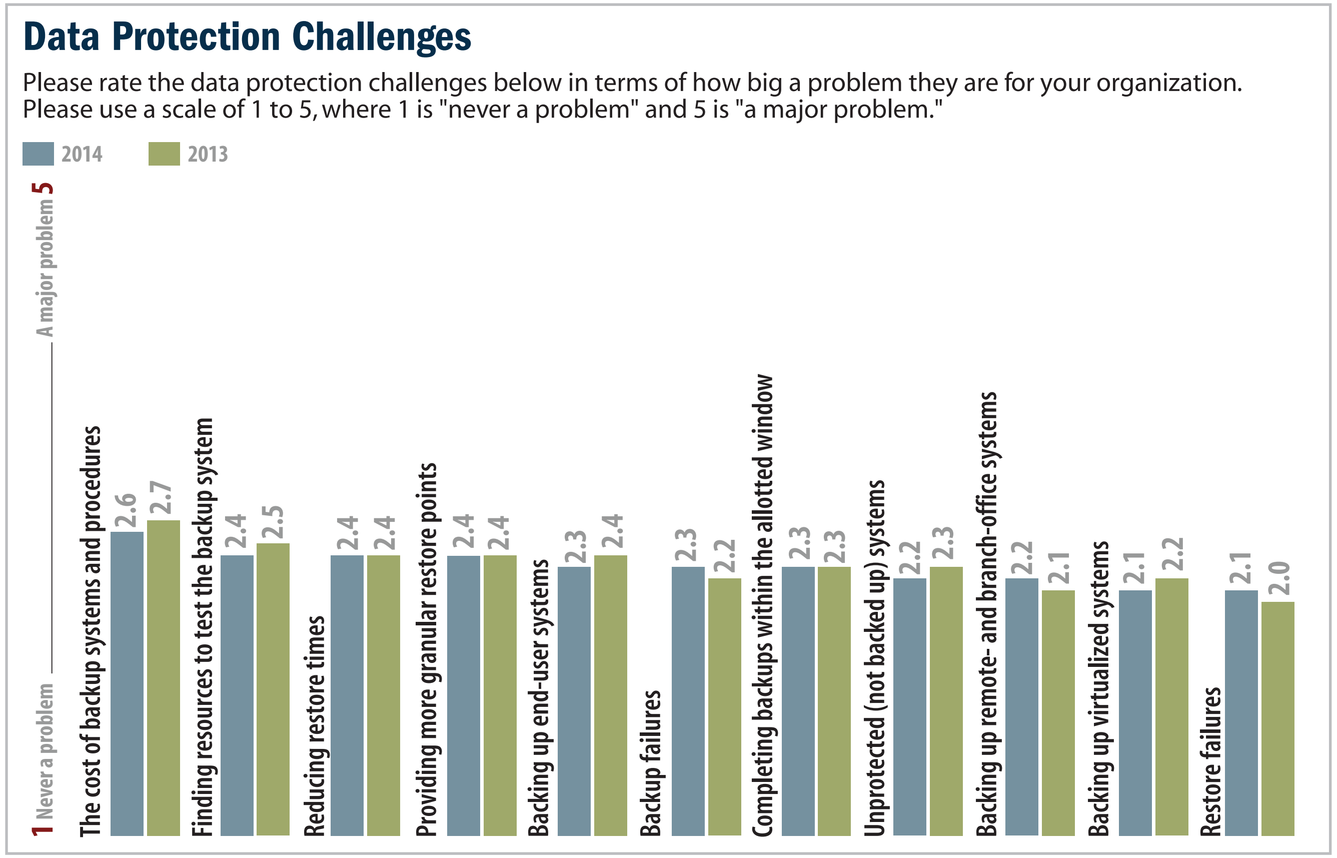
Courts have also addressed a party's inability to produce data as a result of a computer hard drive crash. For example, in Government Benefits Analysts Inc. v. Gradient Insurance Brokerage Inc., US Magistrate Judge David Waxse, an often-cited jurist with e-discovery expertise, ruled that "Plaintiffs also contend that they have provided some documents that coincide with the oral agreement between the two parties. However, Plaintiffs also note that they did not originally produce all documents based on their objections. Moreover, Plaintiffs state that responsive documents dating back to January 1, 2005 do not exist because of a hard drive crash. The Court cannot compel Plaintiffs to produce documents they claim do not exist when the Court has no evidence to the contrary."

However, don't take these rulings to mean you needn't worry about retention. Regardless of how courts view hard drive failures, both congressional requests and public perceptions influence expectations around how email should be managed.

In-House Vs. Cloud

InformationWeek 2014 Backup Technologies Survey shows both private and public sector organizations have room for improvement in data protection. Among 437 respondents, the top method is to back up directly to tape. Just 36% say they're very satisfied with their current backup systems. Among Government IT Priorities respondents, only 10% say they're very aggressively pursuing big data management, down from 13% in 2013. Inadequate funding is a major reason; 35% say lack of budget is the greatest barrier to effective execution of IT projects at their agencies. That's the No. 1 response, landing 11 points ahead of the No. 2 answer, conflicting or poorly defined requirements.

Figure 4



Note: Mean average ratings
Base: 437 respondents in May 2014 and 502 in March 2013
Data: InformationWeek Backup Technologies Survey of business technology professionals

R7930614/22

If moving to more stable information management systems for capturing and preserving email is a priority, there are two main routes.

The first option is setting up internal email archives that staff can readily search for responsive materials. Archives also help avoid failures that result from unreliable local storage. Many federal agencies have already deployed or are seeking to deploy email archives to house all messages to and from their employees. According to a recent federal solicitation, the Federal Housing Finance Agency Office of Technology and Information Management has a requirement to purchase Symantec Enterprise Vault software licenses and maintenance support services to implement an email archiving system. Similar systems offered by CommVault, EMC, HP Autonomy, IBM, and Proofpoint, among others, can also provide enterprise-class email management — and let you avoid some of the pitfalls experienced by the IRS with local email storage.

Another option is for agencies to harness the cloud.

On Dec. 9, 2010, then-US CIO Vivek Kundra launched "Cloud First," a 25-point plan to reform federal IT management. While adoption was slow at first, additional guidance was released on Feb. 24, 2012, to help government agencies better procure information services in the cloud. Allison Stanton, director of electronic discovery at the Department of Justice, has played a key role in advising parties litigating for and against organizations that consume cloud services. In an article she co-authored, Stanton identified several agencies moving to the cloud, including the Department of Agriculture. In addition, Microsoft has recently announced in news releases that both the US Department of Veterans Affairs and the US Environmental Protection Agency selected Office 365 as new cloud-based platforms for email management. Symantec and other email archiving providers also offer cloud-based versions of their software.

Bottom line: Cloud-based email platforms provide inexpensive enterprise-level storage in the cloud and the ability to search and export data much more cost effectively than information stored on individual machines.

It's unfortunate that agencies continue to resist cloud use. Cloud First landed at No. 10 among 12 federal IT initiatives, in order of how aggressively respondents are pursuing these mandates. Just 32% of Government IT Priorities respondents are implementing, or planning to implement, public cloud services.

Get Moving Or Risk Drowning In Data

Like many large companies, federal agencies bear the burden of managing and maintaining large volumes of email communications. Because email messages are records only when their content (including attachments) meets the definition of a record under the Federal Records Act, records managers at federal agencies must segregate organizational records from transient email and apply retention schedules appropriate to the content.

Also like enterprises, many agencies experience an "over-preservation conundrum." In response, the National Archives and Records Administration (NARA) has addressed the issues and risks with journal-based broad email retention. It acknowledges that current email archiving systems "may not be capable of grouping related records in accordance with record-keeping requirements or maintaining the records in a usable format for their full required retention periods; It may make it difficult to identify permanent records and temporary records and carry out proper disposition at the end of their retention periods, be that transfer to the National Archives for permanent records or destruction of temporary records."

As a result of the growing email problem at federal agencies, NARA developed the Capstone approach as part of its continuing efforts to evaluate how agencies have used various email repositories to manage email records. This approach was developed in recognition of the difficulty of practicing traditional records management on the overwhelming volume of email that federal agencies produce.

Under the Capstone approach, NARA recommends targeted, role-based retention based on identifying email accounts according to the work of the user. NARA says that Capstone can substantially reduce the records management burden on individual users by basing email records retention on the mailbox owner's role rather than on the content of each record, and by automating email capture and management according to the simplified, role-based Capstone retention periods.

Capstone is just a start. Both governmental organizations and large corporations might consider launching a holistic IT and legal initiative that includes the people, process, and technology to promote an information governance program.

The Crystal Ball: Defensible Tech Plus Information Governance

My high school chemistry teacher always told his students that hindsight is 20/20. No one appreciates a Monday-morning quarterback. That said, had Congress appropriated more money for email management systems, maybe the IRS could have standardized on a method to retain email for key executives instead of forcing reliance on local storage. Or perhaps that's just wishful thinking. Government procurement life cycles can take as long as two years in some instances — I should know, experienced this in my former position as senior special counsel at the Securities and Exchange Commission.

If we turn back the clock to two years before Lerner's hard drive failed, we find ourselves in 2009. At that time, some of us might remember that our dedicated public servants from both the executive branch and Congress were managing the financial crisis. Spending money on email systems was probably not on the top of anyone's list. Even so, as the recovery is in full swing, perhaps now is the time to think about information governance at your organization.

Soroosh A. Asady contributed to the research and development of this article. Mr. Asady is working under the Electronic Discovery Institute Fellowship Program and is law student at Syracuse University College of Law. He can be reached at saasady@syr.edu.

Like This Report?
Share it!
Like Tweet
Share

Previous

Table of Contents

MORE LIKE THIS

Want More Like This?

InformationWeek creates more than 150 reports like this each year, and they're all free to registered users. We'll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you'll find:

2014 Backup Technologies Survey: Data protection perceptions seem unconnected from reality for our 437 respondents, as 36% say they're very satisfied with their backup systems even as just 23% are extremely confident in their recovery capabilities.

Future of FedRAMP: Agencies have a wider array of platform options than ever, yet progress is still slow. The problem? Cultural resistance to cloud. Here's how FedRAMP and a hybrid model can help.

Gov Cloud: Executive Initiatives, Enterprise Experience: Cloud computing has been endorsed by everyone from the president on down as a key way to make government IT more efficient and responsive. Planning a move should be on every agency's to-do list..

PLUS: Find signature reports, such as the InformationWeek Salary Survey, InformationWeek Elite 100 and the annual State of Security report; full issues; and much more.