

The Total Cost of Email

Putting a price tag on your email environment

You can't afford to ignore email archiving, security, internal policy or regulatory requirements, but can you afford to keep paying for them as multiple systems on top of your email system? When you add up the full price tag for your email environment, from server to software and risk management to staff costs, it becomes clear why running everything in-house can mean spending far more of your budget on maintenance than on innovation.

CALCULATING THE TRUE COST OF EMAIL

Your IT budget is probably going to be reviewed over the next year, so now is the time to look at where you can generate savings without making compromises. To do that, you need to understand exactly how much your current infrastructure is costing you for services that may not add competitive advantage to your business – and to consider how key applications can be charged back to the rest of the business, if that’s an option.

Email is often taken for granted, with senior executives simply seeing email flowing to and from the organization without any understanding of the complexity involved. Ensuring email is always free from spam or malware and that it is not a vector for social engineering attacks or leakage of confidential data is as critical as making a permanent record for compliance or litigation protection. The growth of mobile messaging devices now means that working hours are no longer 9 to 5, as users will often check email in the evening or on weekends, leading to an increasingly low tolerance of any form of downtime.

Organizations have tended to add to their email infrastructure in an organic fashion as new threats or regulatory requirements have arrived. They very rarely step back and analyze the total cost to the business of running their email.

Understanding how much your current email system costs, and how that all adds up, is the key to making changes and to providing a better service for your users. It is only when you understand the risks your organization faces and the costs of your mitigation products that you can perform a true cost-benefit analysis. And breaking out the costs of a typical email solution can be quite surprising – especially when it’s a business-critical service that is taken for granted, and for which the IT department is paying. It’s not just the initial capital costs that are an issue; it’s also the ongoing operational expenses.

Although industry estimates that the cost of managing any on-premises software can be up to four times the initial purchase price, for email storage it’s closer to seven to one. A complex and fragmented environment also introduces risk, and risk has a financial impact on the organization in the event of failure.

BUILD-IT-YOURSELF EMAIL INFRASTRUCTURE	
YOUR BILL:	
EMAIL ARCHIVING:	
ARCHIVING SOFTWARE	\$\$\$
ARCHIVING HARDWARE	\$\$
ARCHIVING BACKUP	\$\$
ARCHIVING STAFF	\$
ARCHIVING STORAGE	\$\$
EMAIL SECURITY:	
ANTI-VIRUS SOFTWARE/SERVICE	\$
ANTI-SPAM SOFTWARE/SERVICE	\$
DENIAL OF SERVICE SOFTWARE	\$\$
DLP SOFTWARE	\$\$\$
SECURITY HARDWARE	\$\$
SECURITY BACKUP	\$\$
SECURITY STAFF	\$\$
EMAIL CONTINUITY:	
BACKUP SOFTWARE	\$\$\$
BACKUP HARDWARE	\$
(2 OF EVERYTHING)	
CLUSTERING SOFTWARE	\$\$
CLUSTERING APPLIANCE	\$
POLICY MANAGEMENT:	
POLICY PLANNING TOOL	\$
DISCLAIMER SOFTWARE	\$
BRANDING SOFTWARE	\$
OTHER:	
MAINTENANCE	\$\$\$
POWER & COOLING	\$\$\$
DATA CENTER RENT	\$\$
STAFF TRAINING	\$
SUPPORT CONTRACTS	\$\$
TOTAL BILL	\$\$\$\$\$\$\$\$\$\$

IRON MOUNTAIN EMAIL SERVICE	
	
YOUR BILL:	
PER EMPLOYEE	\$
TOTAL BILL	\$\$
THANK YOU FOR SHOPPING	

Upfront Capital Investment

Many of the costs of your email infrastructure are sunk costs, especially the initial capital outlay of buying the appropriate hardware. Few businesses can cope with a single email server, and adding policy management, archiving and risk management tools means adding systems to run them on. Email is increasingly a business-critical service with low user tolerance for outage, so an email server may need to be clustered, or even set up to work over a WAN connection to a disaster recovery center. Consider that risk management and regulatory requirements don't diminish in a failover situation. As a result, a large number of the additional services around the email server itself will also need to be clustered using their own high availability configuration. Failover hardware needs to be part of any implementation – and also needs to be regularly tested.

Migration Costs

Hardware and appliances have a finite lifetime, requiring constant repurchasing and migration every three to five years. Consider an archive in a commercial environment that requires seven years' worth of email to be retained. During this period, there may be up to three separate cycles with each one involving a hardware purchase and the migration of an increasing volume of data, with each migration introducing the risk of data loss or corruption. Add in a share of the data center costs – for space, power and cooling. You'll find that these costs quickly dwarf your initial hardware investment and that they'll vary with changes in energy prices.

Ongoing Costs

Then there are upgrades to support new features, installation of software patches, and integration with other systems. With the latest email server releases you're going to need hefty 64-bit multi-core machines with plenty of memory. If you're using a virtual infrastructure, you'll need to be sure you have appropriate resources in your compute fabric that can be prioritized for email, along with the right virtualized storage technologies. Adding extra servers or rolling out upgrades takes time – time that key IT staff could be spending on more strategic projects and time that delays the ROI of the project. Plus, you'll have to budget overtime costs for migrating between mail servers outside regular business hours, as any downtime could severely impact existing business processes and affect business revenues.

High as they are, hardware costs are only a small part of the bill for running your email environment. Software adds further burdens to strained budgets, not just for the email server software and client licenses, but also for the overlapping patchwork of risk management and policy tools required to keep email running smoothly (and, of course, many of those need their own hardware).

You'll need to invest in good anti-virus, intrusion prevention and anti-spam tools to protect your desktop PCs and keep users safe from malware, phishing, application exploits and unwanted advertising. That doesn't just mean spending money on licenses; these all need regular updates that your staff may need to test and then stage on production servers. You can avoid that by investing in expensive managed appliances that filter email connections at the edges of your network, though again this means paying subscription and management fees, as well as additional licensing. You'll also need to make sure that your network is protected from denial of service attacks to ensure that email remains available at all times. The more point products that are introduced into an environment, the more potential there is for misconfiguration or device failure.

Regulations and Compliance

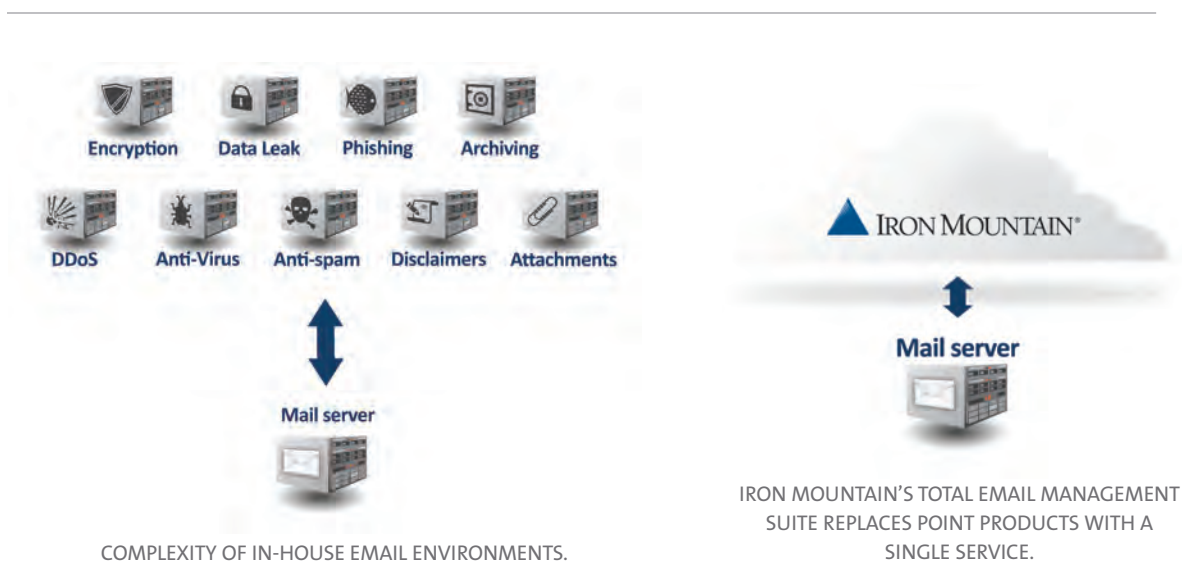
Regulatory requirements add to the costs associated with email. Messages need to be archived and have appropriate disclaimers attached. The regulatory rules that apply will vary from message to message, so you'll also need to implement a rules-based information lifecycle management (ILM) policy. ILM can be expensive and can also require significant amounts of storage hardware to deal with the explosion of information that's flowing in and out of your network. Drivers for archiving go beyond just regulatory requirements; many organizations are retaining emails for internal governance and litigation protection. There's also the additional cost of implementing the appropriate search and audit tools for eDiscovery, or just for unlocking the business value in historical email. And then there's the ever-increasing storage you need to put in place, as the number and size of messages and file attachments just keep on growing. Attempting to discover emails when they are stored as .pst files distributed across remote workers' laptops can be an expensive and time-consuming task.

Protecting Company Information

Data loss prevention (DLP) is an additional cost that's becoming more and more important, not just for regulatory compliance, but also for customer confidence; key business information needs to be protected and so does customer data. Adding DLP to an existing email solution means investing in and integrating additional hardware, software and business processes. You'll need to set aside time for developing and maintaining any DLP rules that you intend to use. In fact, integrating multiple tools with your email environment means careful planning so that the email service isn't interrupted by an installation or any problems it might cause.

Cost of Support

Ongoing subscriptions and regular updates for all of these tools add up. It's also challenging to manage just how many licenses you'll need. You can find that you've over-licensed and that it's next to impossible to be reimbursed by your suppliers. Service and support add to the price, and you'll need to keep track of your support agreements with your suppliers, as well as any service-level agreements. Downtime is expensive, too, and choosing the wrong support contract or SLA can turn into a bad investment. Because you probably won't get all the tools you need from a single vendor, your IT team will have to manage multiple purchase agreements, licensing configurations and renewal dates, as well as multiple interfaces, configurations, policies, reporting tools, patch schedules and support contacts.



The time it takes to deal with tasks that keep the IT department operating means that many companies devote the majority of their IT budgets to maintenance rather than innovation. According to a CIO magazine survey, maintenance represents 60% of the budget for the average business.¹ But the best-performing businesses have reduced that to just 35% and plan to bring it down as low as 20%, freeing up budget that can be used to develop IT solutions that give the business a competitive advantage.

Of course, the costs of email aren't limited to the IT department. If you haven't implemented tools to manage regulatory compliance, then your business could well be left facing expensive litigation – or handling the PR fallout from a significant data loss or security breach. You'll also need to make sure that your end users stay productive and are not swamped with spam and phishing messages, struggling with awkward, rarely used tools or waiting for unresponsive servers (or for backup tapes to be delivered and loaded when they need to access archived messages). Email is the lifeblood of the modern business, and it needs to be kept flowing – cost-effectively.

THE COST SAVINGS OF CLOUD SERVICES

Subscribing to cloud-based services can make quite a difference to your bottom line. Not only will you significantly reduce ongoing capital expenditure, you'll bring down operational expenses as well.

There's no need to worry about over-licensing, as you'll pay a per-user subscription that can adapt to the changing headcount requirements of your organization. Because it's based on the number of users, the subscription model also means it's easier to charge back service costs to business units.

As part of Iron Mountain's Storage-as-a-Service portfolio, Total Email Management Suite, *powered by Mimecast*[®], has a low entry barrier with no procurement costs and fast ROI because you get applications and services that are ready to run. And, with all of the hardware running at Iron Mountain's secure data centers, there's no need to invest in hardware or data center space. You simply connect your existing Microsoft[®] Exchange server to Iron Mountain – and that can take as little as one day.

A well-designed cloud service will scale automatically, giving you all the performance and storage you need for your email archives, security and management, and you don't need to worry about planned or unexpected downtime. Instead of multiple point products that duplicate features or leave you unprotected in some areas, with Total Email Management Suite you get a single service, a single interface and unified reports. Upgrades and updates are transparent, and you don't need to employ dedicated support staff for the service.

Shifting the email load to the cloud means that your IT team can focus on delivering the business services and innovations your company needs, while your Storage-as-a-Service team handles the everyday functions.

Find out more: www.ironmountain.com/digital/email.

¹ CIO Magazine, State of the CIO 2008

ABOUT MIMICAST

Mimecast delivers SaaS-based enterprise email management for archiving, discovery, continuity, security and policy. By unifying disparate and fragmented email environments into one holistic solution that is always available from the cloud, Mimecast minimizes risk and reduces cost and complexity, while providing total end-to-end control of email. Founded in the United Kingdom in 2003, Mimecast serves 2,500 customers worldwide and has offices in Europe, North America, Africa, the Middle East and the Channel Islands.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE:IRM) helps organizations around the world reduce the costs and risks associated with information protection and storage. The Company offers comprehensive records management and data protection solutions, along with the expertise and experience to address complex information challenges such as rising storage costs, litigation, regulatory compliance and disaster recovery. Founded in 1951, Iron Mountain is a trusted partner to more than 90,000 corporate clients throughout North America, Europe, Latin America, and Asia Pacific.

For more information, visit the Company's Web site at www.ironmountain.com.

Portions © 2009 Iron Mountain Incorporated. All rights reserved. Iron Mountain, the design of the mountain and Iron Mountain Digital are registered trademarks of Iron Mountain Incorporated. The reproduction of this white paper is limited to distribution by Iron Mountain Digital only.

Additional copyright and other rights worldwide in this white paper are the property of Mimecast Limited and those may only be reproduced with Mimecast Ltd.'s permission. Mimecast is a registered trademark of Mimecast Limited. All other trademarks and registered trademarks are the property of their respective owners.



IRON MOUNTAIN®
120 Turnpike Road
Southborough, Massachusetts 01772
(800) 899-4766

Iron Mountain Digital is the world's leading provider of Storage-as-a-Service solutions for data protection and recovery, archiving, eDiscovery and intellectual property management. The technology arm of Iron Mountain Incorporated offers a comprehensive suite of solutions to thousands of companies around the world, directly and through a worldwide network of channel partners. Iron Mountain Digital is based in Southborough, MA.