



## E-mail Service Delivery

### Overview

E-mail is critical to the success and operation of most organizations. Without e-mail, organizations are less efficient and can't compete against larger, and more established firms.

Computer users are critical to the success of an organization's security platform. E-mail threats such as spam, viruses, and phishing specifically target users and their end point devices. Hand held devices put data 'on the move' and the same users that are critical to the success of an organization's security framework now present security related risks.

E-mail systems require on-going IT management and monitoring. Not only must e-mail hardware and software be periodically upgraded, these same systems must be patched on a regular basis.

### Security response

IT departments are responding to known security threats by implementing traditional security measures:

- *Employee awareness* - security education and training.
- *Anti-malware* - anti-virus, anti-spam, anti-spyware, and anti-pop up software.
- *Patch management* – keeping software and firmware patched and up-to-date.

### Messaging risks

Organizations must also deal with messaging risks, risks related to transmitting information:

- *Confidentiality* - e-mail attachments can include confidential information such as customer lists and pricing that should not be sent to recipients outside of the organization.
- *Clear text* – sensitive information can inadvertently be sent in clear text.
- *Traffic* – e-mailing large documents creates bottlenecks and uses up valuable network bandwidth.
- *Compliance* – meeting regulatory requirements related to information as it is collected, stored, archived, and secured.

### Internet based utility computing

In addition to the above security responses, many small to mid-size organizations are re-evaluating the need to keep e-mail services in-house vs. using outsourced e-mail service delivery. Providing services internally requires a combination of hardware, software, staffing, and environmental resources. In addition, security time must be allocated to manage e-mail related services.



Internet based utility computing is a process where an organization purchases services on an as needed basis. Much like paying for electricity usage when needed, an organization can outsource e-mail services including the e-mail server, software, storage, protection, and related labor services.

Utility based e-mail services are generally delivered over the Internet using a web browser. Advantages of using an external service provider for e-mail include:

- Equipment - use of service provider's security appliances
- Protection - spam and virus filtering provided by service provider
- Internal resources - reduced internal storage and bandwidth
- Updates – any upgrades are provided by the service provider
- Labor – patch management provided by service provider
- Management – services are monitored and managed 24x7 by service provider

Utility based computing provides services on an as needed basis with flexible on demand storage space, e-mail services, e-mail filtering, etc. The external service provider manages e-mail security and message compliance including message archiving, encryption, and policy enforcement.

Compared to managing functionality in-house, external services provide advantages in cost and effectiveness. The total cost of ownership for an internal e-mail system can be as much as \$50 per seat per month (includes hardware, software, and labor) while an external solution is much less.

According to recent surveys, almost one-half of respondents plan to deploy outsourced e-mail service solutions for e-mail security, web security, or message compliance. The benefits of utility based e-mail services include:

- Time savings – internal e-mail solutions require more IT department time to manage and maintain e-mail servers. Outsourcing e-mail to utility based solutions better deploys internal resources to strategic projects.
- Risk management – organizations that outsource e-mail service delivery transfer their risks to the outsourced services provider.
- Enhanced reliability – external full-time e-mail providers can provide enhanced service at a lower cost.
- Simplicity – external e-mail providers help simplify the internal network infrastructure.

### **Service delivery considerations**

IT managers should take professional care and due diligence when evaluating external service providers:

- Service levels - your organization should determine if the outsourced provider has professional, high performance infrastructures that can guarantee levels of performance delivery.



- Support – user and technical support must be determined up front. Will first level user support be provided by their staff or yours?
- Redundancy - external service providers should have redundant solutions that allow systems to continue operating even during single component failure.
- Contingency plans – business continuity and disaster recovery plans must be updated and tested on a regular basis.

### **Summary**

While outsourcing isn't for every organization, many firms have found that outsourcing e-mail can be a simple, reliable, and cost effective solution. By using utility based outsourced e-mail services, internal IT staff has additional time to focus on higher level business initiatives. In addition, outsourcing helps organizations meet regulatory requirements while simplifying the IT infrastructure. A variety of solutions may be purchased on an as needed basis:

- Spam filtering – reduces phishing threats that lead to information disclosure.
- Message security – e-mail security, Transport Layer Security (TLS) encryption, and policy management for inbound and outbound messages prevents eavesdropping, tampering, and message forgery.
- Message discovery – message archiving and e-discovery.

Assessments help organize identify, manage, and reduce their e-mail and compliance related risks.

### **Publication and Author Information**

Jim Kelton is Managing Principal of Altius IT ([www.AltiusIT.com](http://www.AltiusIT.com)), an IT security audit, security consulting, and risk management company based in Costa Mesa, California. Mr. Kelton has over 30 years of experience in the Information Technology industry and is recognized as a security expert. He is certified by the Information Systems Audit and Control Association (ISACA) as:

Certified Information Systems Auditor (CISA)

Certified in Risk and Information Systems Controls (CRISC)

Certified in the Governance of Enterprise IT (CGEIT)

He sits on the Board of Directors of the following associations and organizations:

- Association of Professional Consultants (APC)
- International Association of Professional Security Consultants (IAPSC)
- Technology Professionals Association (TPA)