

***e*B2Bcom**

Email Management: Are you in control

October 2003

Opening Remarks

Andrew Ferguson – Vice Chair AITSF

October 2003





Topics

- Some Observations
- Securing your knowledge information – protecting the contents of your Messaging networks
- Costs of Ownership
- eB2Bcom

Why do organisation's need to protect the knowledge information

- **Antivirus and other attacks are a global problem and increasing**
- **Damage and costs are immense**
- **“Leaking” of internal documents is widespread**
- **Companies are liable for employees’ harassment, racial slurs,**
- **Sensitive internal information is vulnerable to malicious dissemination**
- **Sexist e-mail lawsuits**
- **Over 50% of respondents to a Novell survey said they received Flame mail (derogatory or obscene) on a regular basis - some even leaving their jobs as a result.**
- **Files hidden in other formats - eg Word inside multiple Zips**
- **Translation of email Policy into practicality**
- **Difficulty and costs of configuring and administering**
- **Management and reporting**

Corporate Email asset or Liability

- **One of the fastest growing business tools in recent years is corporate email. Organisations worldwide now rely upon email communications as a core part of their dealings with both customers and business partners. Whilst many would argue that its value as a business tool is unquestionable, there is another view that is hitting many large organisations – email needs management and policy control in order to avoid becoming a corporate liability.**
- **As an asset to the business, email is enabling true global communications, improving the management of customer relationships and empowering employees, giving the potential to dramatically increase productivity. It has become the ‘life blood’ of the organisation, relied upon for the majority of communications at all levels.**
- **Conversely the rush by many organisations to capitalise on this "communications revolution" and to be perceived as cutting-edge has encouraged the development of systems that give little thought to management policy, the efficient use of resources or the very real risk of breaches of confidentiality and security. In many ways email has become a bandwagon that is out of control, and as such is a true corporate liability.**

The Threat from Within

- **There is little point in enhancing communications if the required information isn't easily accessible to those who need to communicate it. From company telephone lists and corporate policies, through to customer databases and business plans, an organisation's most sensitive information is often easily accessible to its staff. As a result it is now possible for employees to simply take sensitive company data and despatch it around the world via email, either maliciously or unconsciously.**
- **The problem is exacerbated by the increasing need for organisations to share information in publicly available directories. However, access to this information needs to be controlled and only given to certain individuals within an organisation or key partners, in order to protect electronically stored assets and adhere to the Data Protection Act and increasingly to Federal & State Privacy laws.**
- **For example a US airline recently admitted that a computer software glitch inadvertently included subscribers' email addresses in an electronic bulletin. The company has been doing a lot of apologising to unhappy subscribers ever since.**
- **It is clear therefore that there is a requirement to set in place policies and controls to ensure that sensitive information is only available, and communicable, to those who have a genuine requirement for it.**

Email & corporate liability

- **Many organisations are beginning to recognise the potential liability of email, illustrated by the explosion of corporate disclaimers that are often larger than the email itself. There has been much deliberation over when an email becomes a contractual obligation. Indeed organisations are becoming so concerned about the business consequences of employee email that they have instigated "email compliance" policies, physically checking every mail to leave the organisation for business sensitive information.**
- **The problem is not limited to information, we are seeing the emergence of test cases where an organisation is held liable for spreading, either knowingly or not, computer viruses. There is also much concern about "flame-mail" - a derogatory, obscene or in appropriate email message. Over 50% of respondents to a Novell survey said they received these on a regular basis - some even leaving their jobs as a result. Litigation can be expensive;**
- **The management of an organisation must be prepared to take responsibility for the mis-use of email systems, and put measures in place to identify any areas where organisational or email policies, or the rights of the individual, are being flaunted.**

Quantifying the Problem

- **Chevron paid \$2.2m to settle sexist e-mail lawsuit**
- **Greatest threat to intellectual property is trusted insiders; 70% of security breaches come from inside (ASIS 2000)**
- **80% of companies in UK have no e-mail/Internet policy; 68% of directors believe they are exposed to legal risk (TSO 1999)**
- **34% of IT professionals in US blame e-mail as biggest cause of IT support problems (Support.com 2001)**
- **By 2004, economic value of Internet crime expected to increase 1000% (Gartner 01/01)**
- **Western Provident 1m pounds damages over Norwich Union defamatory e-mails**
- **Claire Swire e-mail re-forwarded to 20m people (Dec 2000)**
- **Melissa, Love Bug, etc e-mail propagated viruses. Infected millions of PC's and networks world-wide, \$m's cost to business and government**
- **Whitehouse web site e-mail bombed, May 1st 2001, Hacked by Chinese**
- **Hacking has become 'cool' and a tactical weapon**

Security & Policy at the Boundary

- To date, this need to recognise and control the content of email has only been partially addressed with keyword searching of the header and content of the email. It is a well-accepted that is easily overcome by using code words, or simply by putting information within an attachment. This is compounded if the email is encrypted.
- A new generation of email technology now takes control by allowing systems managers to define "concepts" that they do not want to be communicated internally or to the outside world. Using sophisticated artificial intelligence software the contents of an email, and its attachments, can be automatically scanned for any breach of confidentiality or policy even if the contents are encrypted. When an email that contains the 'forbidden' concepts is identified, it can be automatically routed to a pre-defined reviewer and prevented, if appropriate, from leaving the organisation
- Significantly, instead of attempting to gain control of corporate email at the desktop, new generation software adopts a more pragmatic approach by managing email at the "information portal" on the boundary between the organisation and the outside world (or between departments within an enterprise) Clearswift's Deep Secure technology is a very good example of this new technology. This approach offers the benefits of configurability and policy setting at a server level, allowing the definition and management of email policy from a corporate perspective regardless of desktop set up.
- By taking this approach organisations can realise substantial maintenance savings and, perhaps more importantly, demonstrate in a court of law a proactive stance in implementing policy that allows higher levels of monitoring and control.

Boundary Protection for Messaging

- **The Boundary Messaging gateways provide**
 - assured network separation (in some cases on Evaluated platforms)
 - virus scanning to protect the information knowledge content
 - document fingerprinting to control information release
 - macro control
 - Spam and spoof control
 - security label checking to control knowledge release
 - content filtering to checking content
 - Document and information release policy checking
 - Support for encrypted messaging on a desktop to desktop basis not just gateway to gateway

The Problems

Inadvertent or Intentional:

Legal, Ethical
& Regulatory
Liability

Confidentiality

Productivity

- Inappropriate employee communications
- Disclosure of internal sensitive information
- Viruses
- Spam
- Downloads (music files, images etc.)
- Espionage
- Hacking

Lost

Brand, reputation, customer confidence,
intellectual property, ideas

Informality / lack of privacy / Permanence / Easy distribution / “Send now, think later” culture

Complacent communication

Cost of Ownership

- **Global Study looking at TCO of Messaging networks across range of industries (Global 1000 companies)**
 - Banking & Financial Sector 20%
 - Government 10%
 - Retail 10%
 - Insurance 10%
 - Transportation 10%
 - Healthcare 10%
 - Education 10%
 - Others 20%

Study Numbers

- **Enterprises**

- 38% of organisations surveyed had in excess of 25K Mailboxes
- 15% have between 15,000 to 25,000 mailboxes
- 46% have less than 15,000 Mailboxes

- **Service Providers/Outsourcers**

- 25% of those surveyed have in excess of 5Million Mailboxes being managed
- 15% of Service providers have between 1M to 5M
- 60% have less than 500,000 email subscribers

Total Cost of Ownership Enterprise Messaging

Avg. Cost/User	Lotus Notes	MS Exchange
Acquisition	\$ 145.93	\$ 148.40
Maintenance	\$ 29.43	\$ 32.72
Installation & Configuration	\$ 17.94	\$ 41.15
Administration	\$ 93.04	\$ 25.54
Downtime	\$ 20.73	\$ 69.72
1 st Year Training	\$ 1.39	\$ 0.70
Follow-on Year Training	\$ 0.77	\$ 0.42
TCO – 1st year	\$ 279.03	\$ 285.51
TCO – 3 Year Average	\$ 220.84	\$ 217.93

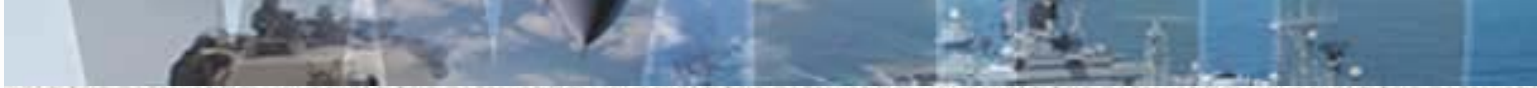
Source: Radicati

Total Cost of Ownership for Outsourced Messaging

Avg. Cost/Subscriber	Critical Path	iPlanet	Microsoft
Usage Scenario	50% Basic; 25% Knowledge Worker; 25% Consumer	40% Basic; 60% Knowledge Worker	20% Basic; 80% Knowledge Worker
Acquisition	\$ 0.83	\$ 1.22	\$ 23.59
Maintenance	\$ 0.14	\$ 0.28	\$ 0.83
Physical Space	\$ 0.00003	\$ 0.00036	\$ 0.019
System Integration	\$ 0.009	\$ 0.33	\$ 3.08
Installation & Configuration	\$ 0.01	\$ 0.013	\$ 0.21
Administration	\$ 0.08	\$ 1.01	\$ 8.58
Downtime	\$0.0006	\$ 0.03	\$ 0.28
1 st Year Training	\$ 0.001	\$ 0.018	\$ 0.48
Follow-on Year Training	\$ 0.0004	\$ 0.0145	\$ 0.46
TCO – 1 st Year	\$ 1.31	\$ 3.61	\$ 42.80
TCO – 3 Year Average	\$ 0.79	\$ 2.55	\$ 26.92

Outsourced Messaging

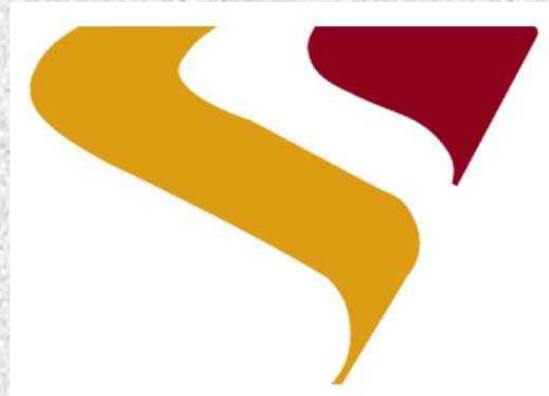
	Critical Path	iPlanet	Microsoft
Hardware platform	Sun E220, SunE420, SunE4500	SunE420R SunE450	Compaq HP
Usage Scenario	50% Basic; 25% Knowledge Worker; 25% Consumer	40% Basic; 60% Knowledge Worker	20% Basic; 80% Knowledge Worker
Planned Subscriber Capacity	10,600,000	390,000	55,600
Actual Subscriber Capacity	3,740,000	107,500	9,733
Avg. # of msg. servers	14.6	3.3	12.6
# of CPUs/Server	4	4	4
Avg. RAM capacity	3.8 GB	3.3 GB	2.9 GB
Avg. Disk sub-system capacity	6.8 TB	2.2 TB	5.3 TB
Avg. # of directory servers	2.7	2.3	4.3
Avg. # of routers	0.6	1.7	3.5
Avg. # of switches	1.4	2.3	7.5
Avg. # of load balancer devices	2.4	3	4
Avg. # of firewalls	0.6	2	3
Initial physical space allocation	34.8 sq. m	10 sq. m	40.2 sq. m
Incremental space over 12-18 mos.	5.6 sq. m	14.1 sq. m	106.4 sq. m
Full-time Admin. staff	2.5	1.8	3.8
Help-desk staff	0.9	2.7	5.6



"Nurse, get on the internet, go to SURGERY.COM, scroll down and click on the 'Are you totally lost?' icon."

eB2Bcom Credentials:

- **Founded 1996**
- **Australian-owned SME**
- **Software solutions for Secure Messaging, Trusted Gateways, Secure Information sharing and Identity Management**
- **Consultancy expertise in Messaging Benchmarking, DSD i-RAP security audits, Identity Management & Meta Directories**
- **Blue chip successes**
- **Portfolio of technology**
- **Focus is Defence, Intel, Police, Govt, Finance and e-Health**
- **Management experience in eCommerce**
- **Small, with SI partnerships**
- **Highly focussed on growth technologies and C4ISR**



eB2Bcom

**enabling electronic Business 2 Business
communications**

sales@eb2b.com.au

www.eb2b.com.au

October 2003

