

E-mail Management

By Joanna Goodman

Contents

EXECUTIVE SUMMARY	1
PART ONE	
E-mail management: Identifying the Issues	5
CHAPTER 1	
E-mail management: The business drivers	7
Compliance and corporate governance	7
Spam, viruses and other inbound threats	8
E-mail abuse and other outbound threats	9
E-mail overload	9
Disaster recovery	9
Improving customer service and business processes	9
Corporate e-mail: Regulation and legislation the UK	10
CHAPTER 2	
The challenge of managing unstructured data	13
Managing inbound and outbound threats	13
Controlling the volume	14
Archiving, search and retrieval	16
Instant messaging, VOIP and other messaging applications	17
CHAPTER 3	
E-mail, information strategy and architecture	19
Deciding how much to outsource	19
Filing and classification	20
Knowledge management	22
Roles and responsibilities	23
Disaster recovery and business continuity	24
CHAPTER 4	
Governing e-mail usage with policy, technology and training	27
The need for an acceptable e-mail usage policy	27
Establish a policy and support it with technology	27
Key security issues	27
Monitoring and surveillance	28
Retention and disposal	28
E-mail content	28
Personal use of e-mail and internet	29
Educate everyone	29

Enforce the policy	30
Good practice guidance	31
CHAPTER 5	
The interface between internal and external communication	33
Key communication challenges	33
E-mail disclaimers	33
Guiding user behaviour	35
Educating users	36
Leading by example	37
Addressing e-mail stress and e-mail addiction	38
CHAPTER 6	
Tools and tactics for successful e-mail management	39
Avoid common e-mail management mistakes	39
A strategic approach adds value	40
When to use e-mail – and when to avoid it	41
Regular user consultation – education pays dividends	42
Alternative technologies	42
Ten steps to effective e-mail management	44
PART TWO	
Expert Guidance on E-mail Management in Practice	
CHAPTER 7	
Complying with the law	47
E-mail in context	47
The liability	48
Monitoring	50
Complying with data protection for employees	51
Retaining e-mail	51
The policy	52
Archiving and storage products	53
CHAPTER 8	
E-mail management in practice: The triple helix of people, policies and technology	55
Introduction	55
Challenges	55
The three steps to success	56
Examples of good practice	56
Technology	57
People	58
Policies	60

CHAPTER 9	
E-mail storage, retention, retrieval ... and destruction	63
Introduction	63
Needs assessment	63
Considerations when selecting a system	65
E-mail policies	66
What e-mails must be archived – and for how long?	67
Conclusions	68
CHAPTER 10	
Getting e-mail under control	69
Deploying a business classification scheme	70
Implementing a corporate File Plan	71
Training and change management	72
Top tips for effective e-mail classification	72
CHAPTER 11	
What's the matter?	75
A filing dilemma	75
So why bother with matter centricity?	75
DMS implementation	75
The upgraded system	76
Matter-centric e-mail management	77
Logical workspaces	77
Practice management	77
Remote access	78
A unified content environment	78
CHAPTER 12	
E-mail management – it's not easy	79
CHAPTER 13	
Taming the beast: Regaining control of e-mail	81
E-mail: The killer application	81
What? More problems	82
Why have it?	84
So, take control	84
CHAPTER 14	
Building a solid framework for e-mail best practice in the construction industry	87
The challenge: a remote and mobile workforce struggling with e-mail overload	87
The solution: a partnership approach to best practice	87
Mesmo's 'e-mail charter'	88
Educating users	89

Reinforcing the message	89
The outcome: better online time management and reduced e-mail stress	89
Next steps	89
CHAPTER 15	
Traditional brewer creates a SPECIAL e-mail charter	91
The background	91
The role of leadership	92
A SPECIAL charter	92
The outcome: a better understanding of e-mail and communication	93
Next steps	93

Executive summary

E-MAIL HAS rapidly become the most significant communication channel for businesses and individuals, and has transformed the workplace. Most organisations depend on e-mail to communicate with their customers, partners and suppliers. E-mail underpins key operational processes, including administration, purchasing, sales and marketing. Key negotiations and business-critical transactions are conducted by e-mail. E-mail is also the default communication channel for individual users. It's the only application that touches every single department, role and function in an organisation, so it has become the framework for internal communications, underpinning working relationships, collaboration, knowledge and information sharing and social interaction.

It follows, therefore, that for some time e-mail management has been a hot topic in business circles. This report aims to encapsulate some of the latest thinking, expert guidance and best practices that help successful organisations avoid the dangers of unstructured data, and leverage what has become the critical business tool to drive efficiency and productivity and maximise business opportunity and success. This requires a comprehensive strategy, led from the top and involving the entire user population, with the purpose of incorporating good e-mail management and best practice into the information infrastructure of an enterprise and its corporate culture.

Chapter 1 examines the key drivers for implementing an enterprise-wide e-mail management strategy. The ubiquity, immediacy and popularity of e-mail, as well

as the growth in attachment size due the proliferation of multimedia formats, have led to e-mail overload, with corporate e-mail servers handling huge numbers of messages every day. Furthermore, our tendency to spend more and more time communicating online has been encouraged by rapid technological developments, particularly in peer-to-peer applications such as instant messaging, BlackBerry and similar PDA devices and Voice over Internet Protocol (VOIP).

Typically, nearly half the e-mails that an organisation receives are unwanted, so spam filtering and virus protection is crucial to prevent e-mail volume from spiralling out of control, and to limit the threat to an organisation's information infrastructure presented by deliberate and inadvertent e-mail misuse. The fact that business-critical and confidential data is commonly transmitted between internal and external stakeholders drives the need for security measures including message encryption and user authentication.

Regulations covering e-mail are also increasing exponentially and compliance has become a key issue. Organisations' potential liability is complicated – and increased – by the fact that e-mail transcends international boundaries. The fact that e-mail is legally discoverable has been highlighted by Enron and other high-profile cases, increasing organisational awareness of its potential dangers, which range from embarrassing to terminal. These are outlined in Chapter 1 and covered in more detail by barrister Stephen Mason in Chapter 7.

Chapter 2 addresses some of the challenges of managing the unstructured

data that organisations have to deal with every day. The growth in e-mail volume and increased compliance requirements, particularly in the financial, legal and healthcare sectors, means that almost all businesses invest in e-mail management technology, including applications that automatically scan and analyse the content of inbound and outbound messages, apply rules that minimise corporate liability and threats, control e-mail misuse and fulfil retention, archiving, search and retrieval requirements. Decisions regarding the choice and combination of applications, and whether (and how much) to outsource depend on the business profile of the organisation and its compliance and operational requirements, as well as the volume and nature of the messages it handles. In Chapter 9, content management expert Jon Helfet provides further detailed guidance on these issues.

It's also crucial to support automation with strategies, rules and processes for organising the different categories of information contained in e-mail messages, which often represent key business records, as well as providing arrangements for business continuity in the event of an e-mail system failure. Chapter 3 explores the way that e-mail management fits into an organisation's overall information architecture, covering filing, classification, e-mail lifecycle and knowledge management. It's also important to define the roles and responsibilities involved in a comprehensive, enterprise-wide e-mail management programme. Additional expert guidance on these issues is provided by business classification consultant Jeff Morelli in Chapter 10.

Chapter 4 explores e-mail policy – the procedural framework that drives which e-mails are retained, how and when they

are purged and how they fit in with the larger array of information managed by the organisation. Experts agree that all organisations should establish an acceptable usage policy that needs to be signed by all employees. In addition to retention, storage, search and retrieval, a corporate e-mail policy should also cover agreed processes on security, monitoring and surveillance, as well as human factors such as personal use of e-mail, acceptable content of messages and user behaviour. The policy needs to be enforced by processes, technology and user training. In Chapter 8, top e-mail consultant Dr. Keith Nicholson reinforces this view and presents a three-step approach to policy development and enforcement.

Chapter 5 concentrates on the essential purpose of e-mail as the application that underpins internal and external communication. It presents some of the key communication challenges associated with corporate e-mail, and demonstrates that formal and informal user education, supported by ongoing internal communications, help to maintain an organisation's e-mail usage policy by influencing online behaviour and embedding best practice. This is illustrated by Dr. Monica Seeley's e-mail charters and workshops, featured in the Shepherd Construction and Young's case studies (Chapters 14 and 15).

Chapter 6 presents a selection of practical tools and tactics for successful e-mail management, including how to avoid common pitfalls, the benefits of taking a strategic approach and ways to address common administrative and technological considerations and add value to your business. It goes on to explore alternative technologies, pointing out that e-mail is not always the best communication medium for every message, and ends with

a ten-step quick reference guide to effective e-mail management.

Part 2 comprises a selection of articles comprising the latest thinking and guidance from recognised experts, as well as recent examples of good e-mail management featuring a selection of well-known organisations in a variety of business sectors. The majority of these have been commissioned especially for this report; the rest are drawn from recent experience of successful e-mail management in practice.