



Using Classification to Manage Email Policy for the Enterprise

Whitepaper

Release 2.0 (May, 2007)

Classify-Manage-Control

Information in this document is subject to change without notice. The names of the companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written consent of Titus International Inc.

Titus Labs Inc. may have patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document.

© 2006-07 Titus Labs Inc.

Microsoft, Windows, Windows 2000, Windows XP, Windows Server 2003, Microsoft Group Policy, Microsoft Group Policy Management Console, Microsoft Windows Rights Management Services are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

At Titus Labs we work to help businesses better manage and secure valuable corporate information. Our focus is on building policy management solutions that make it easier for IT administrators to protect and manage corporate correspondence including email and documents.

For further information, contact us at (613) 820-5111 or email us at info@titus.com

<http://www.titus-labs.com/>

Table of Contents

EXECUTIVE SUMMARY.....	4
THE EMAIL POLICY CHALLENGE.....	4
HOW CLASSIFICATION CAN BE USED	5
<i>Government Classification</i>	5
<i>Financial Industry Classification</i>	7
<i>HIPAA and the Health Industry</i>	10
<i>Military Classification</i>	12
TITUS LABS MESSAGE CLASSIFICATION	14
<i>Classify</i>	15
<i>Manage</i>	16
<i>Control</i>	17
MESSAGE CLASSIFICATION ENTERPRISE EDITION.....	18
MICROSOFT WINDOWS RIGHTS MANAGEMENT SERVICES	18
<i>The Power of Classification with Microsoft RMS.</i>	19
CONCLUSION.....	19
ADDITIONAL READING	20

Executive Summary

This paper discusses issues related to the use of email within large organizations. While email has become an indispensable tool of modern communications, its misuse has also been at the center of ethical and legal breaches across diverse organizations. In response to these breaches, regulators have stipulated a wide range of measures that must be taken to ensure security, privacy, and accountability. This paper provides IT professionals and executives with an overview of issues and the regulatory responses across a number of sectors. It describes classification-based strategies to comply with requirements to manage email effectively. It also discusses the role of classification in managing email from an operational perspective.

The Email Policy Challenge

Over the past decade, email has become virtually ubiquitous. Organizations of all sizes and types rely on it to communicate with clients and customers, partners and suppliers and for the massive amounts of collaborative information exchange between employees that are the lifeblood of information-based work. Even in the face of newer technologies such as instant messaging and VoIP, email remains the killer application of the Internet, intranets and extranets. In 2005, the average corporate user sent and received 84 messages per day, requiring over 10 megabytes of storage space and including every sort of information from proprietary intellectual property to client or customer records. Yet email remains primarily an unmanaged medium. While governments, corporations and other organizations have invested heavily in protecting themselves against the threats posed by inbound email, such as spam, viruses, worms and trojan horses, little thought has gone into the risks posed by outgoing and internal email. These risks are potentially

dramatic and include loss of proprietary information and violation of record retention and privacy laws. Email is a weak link in organizational security.

In addition, email is a vast store of unstructured information that cannot easily be mined for enterprise advantage. Because of its prevalence for exchanging ideas and information within the organization, stored email holds approximately 70% of intellectual property generated within the organization. Yet this potentially rich store of business intelligence is effectively a data landfill if it cannot be searched / sorted and mined in ways that make it useful to the knowledge worker.

How Classification can be used

Email classification is a technique for adding metadata and visual labels to email. If applied judiciously, they offer an effective strategy for managing and controlling email.

The following sections describe ways in which message classification can be used in several large, complex and mature public and private sectors.

Government Classification

Government agencies and departments have historically faced higher expectations than other organizations in the handling of information. Governments hold sensitive information in the public trust and are ultimately answerable to the public. As such they face stringent safeguards on the handling and safeguarding of that information. Over the past several years, government regulations have been catching up with the realities of electronic communications and data storage.

In the United States, the Freedom of Information Act requires that federal agencies disclose their records to anyone making a written request. The speed and economy of

email often makes it the preferred means of delivery, carrying risks that the wrong information might be sent or the wrong recipient addressed.

Because email has become so prevalent for interdepartmental communications, security of communications has become a serious concern.

The Federal Information Security Management Act (FISMA) places the onus squarely on agencies and their partners to develop information security risk assessments and mitigation strategies. As part of FISMA compliance, agencies and departments should implement ways to track the contents of all outgoing emails.

Classifying emails by applying labels and metadata presents an obvious opportunity for governments' efforts to manage and control electronic communications. Through the use of security procedures and server-based content scanning which complement email labelling, government can ensure that private or confidential information is protected from unintended or illegal disclosure, while ensuring citizen's timely and cost effective access to public records and personal information under fair disclosure legislation.

Some governments have specifically required various forms of email classification for their departments.

In the United Kingdom, the Government Protective Marking Scheme (GPMS) requires that broad classes of government-generated information, including email, be marked with an appropriate security marking and handled appropriately.

The Australian government has taken a more pointed approach to government email.

Amendments to the Australian Defense Signals Directorate's Communications

Technology Security Manual require that all email originating in federal agencies carry

markings in compliance with its Electronic Mail Protective Marking Policy. These markups establish a maximum-security classification and accompanying caveats for the message.

Financial Industry Classification

Over the past several years, insider trading, misrepresentation of the prospects of securities and other irregularities in the financial services industry have led to more stringent laws governing their behavior.

Financial services companies face a wide range of regulations that impact information technologies in general and email in particular. In the United States, for instance, the Financial Modernization Act, also known as the Gramm-Leach-Bliley or GLB Act, aims to protect the privacy of customer information held by financial institutions. GLB stipulates stiff penalties and extends to electronic data including email in transmission and in storage.

Regulations from the Securities and Exchange (SEC) restrict forward-looking statements at certain times and enforce quiet times associated with registration filings. Other SEC rules stipulate that a wide range of records and communications be maintained and readily accessible for examination for significant periods of time, including interoffice memoranda and communications.

The National Association of Securities Dealers (NASD) and the New York Stock Exchange impose additional record keeping regulations with specific requirements for the management of electronic data. The NASD also places restrictions on how investment offerings are marketed and sold.

The Fair Credit Reporting Act places the responsibility for maintaining the privacy of personal credit information squarely on credit bureaus.

In situations where financial services companies have divisions or groups that could be put into an ethical conflict by sensitive customer information, such as where the possibility of insider trading exists, particular care must be taken to ensure that email systems protect ethical walls.

The cost to financial service organizations for non-compliance with these regulations can be severe. For example, in 2002 the SEC, in conjunction with the NYSE and NASD, fined Deutsche Bank Securities Inc., Goldman, Sachs & Co., Morgan Stanley & Co. Incorporated, Salomon Smith Barney Inc., and U.S. Bancorp Piper Jaffray Inc. over \$8,000,000 for failing to preserve emails for three years. These fines also underlined the importance of maintaining a demonstrable system for managing and retrieving archived emails.

While there is no standard definition of a reasonable amount of time to disclose business records or business communications when required under these regulations, 36 to 72 hours is generally considered fair. Companies that fail to produce records promptly can face severe fines. In 2004 Bank of America was fined \$10,000,000 for failing to turn over emails from senior managers that potentially implicated the firm in trading on unreleased research by its own analysts. Whether deliberate or not, failure to comply carries harsh consequences. Considering that a company of 20,000 employees could be required to archive over 4.5 billion emails over the next seven year period, it is clear that effective management techniques are required to quickly locate and retrieve the one or two emails that a regulator may want to review.

The Sarbanes-Oxley Act (SOX) was passed in 2002 in response to highly publicized cases of corporate fraud related to financial reporting, including those of Enron and WorldCom. SOX makes officers of public corporations personally responsible for misrepresentations of financial information. It requires that safeguards be put in place to ensure the accuracy of financial reports. These include security of electronic data against unauthorized access or change, both during transmission and in storage. SOX also requires monitoring of the users who access financial data. These restrictions have a significant impact on the ways in which publicly traded companies treat email. Ensuring that email systems and practices meet the requirements of the legislation involves protection of sensitive email from tampering and unauthorized access. These restrictions stretch from sender to recipient and into the enterprise data store.

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) provides broad protection of personal information held by private organizations and stipulates that this information must be made available on demand to the individuals it relates to.

Classification labels can be used to effectively manage and control email and meet a variety of challenges faced by financial institutions. Classifications can be used to enforce internal ethical walls by preventing sensitive information from being shared inappropriately. For instance, an email classification label such as “Mergers and Acquisition Dept Only” used in conjunction with Safe Recipient List technology (available in Titus Labs Message Classification) can help ensure that sensitive information is restricted to groups of users with “need to know”. Used in conjunction with an optional digital rights management system (such as Microsoft RMS), email can

be properly protected based on its classification, ensuring that only certain users have rights such as “View”, “Forward”, “print” etc.

Classifications can also be used to help with proper retention of information. For instance, classification can be used to ensure sensitive emails are not inadvertently deleted while still under one or more legal embargos. For example, email classification labels such as “Financial Information” or “Legal Information” can be read by server-based email archiving systems, which can ensure that the emails are retained for the desired period.

Finally, classification metadata attached to email provides effective and timely searching and retrieval in compliance with requirements to disclose information to regulators on demand. For example, where email has been labeled based on a project such as “ABC Merger”, all emails related to the project can quickly be pulled from an archive.

HIPAA and the Health Industry

Email has the potential to improve efficiency and reduce costs in health care delivery. For example, patient records can be quickly and efficiently shared between general practitioners, specialists, hospitals and insurers. Classification and security are paramount to enabling this efficiency within stringent legislative frameworks.

The Health Insurance Portability and Accountability Act (HIPAA) encourages the secure use of email for communications not only for collaborative access to patient records, but billing and administrative functions as well. HIPAA places great emphasis on the privacy and security of patient records. HIPAA specifically allows patient records to be shared by health care professionals to facilitate patient care. It forbids the sharing of these same records with third

parties such as insurers, without the consent of the patient. HIPAA's restrictions on the use of patient information can extend to government departments, pharmaceutical companies running hosted trials and employers that provide group health care plans.

There have been many cases of organizations being fined for failure to maintain electronic records securely. For example, the pharmaceutical maker Ely Lilly faced sanctions when a clerk accidentally sent email reminders to over 600 trial participants using the TO field rather than the BCC field, thus exposing their identities. In another incident, a former employee of Kaiser Permanente posted 140 patient records on a public website.

Email classification can protect against inadvertent leaks of patient information. By implementing a system that requires doctors, nurses, clerks and others to classify & label messages before they can be sent, a health institution can ensure that these sensitive records can be used in accordance with the requirements of HIPAA for effective collaborative diagnostics while preventing their unauthorized disclosure to insurers or other third parties. Many employers with group health insurance face similar requirements and can also realize benefits from classification systems.

HIPAA is not the only legislation that organizations with activities related to human health must be aware of. Parts 210 and 211 of the Food and Drug Administration's Current Good Manufacturing Practice regulations require that records relating the manufacturing within pharmaceutical firms be maintained and that these firms can prove that prescribed practices were followed. Classification of emails related to manufacturing practice is an important link in the chain of proof required under parts 210 and 211.

Military Classification

Military requirements for secure communication are as old as the military itself. In the modern world, however, these needs are significantly complicated. The post 9/11 context of terrorist threats and the military's response heighten the urgency to safeguard military secrets. At the same time, military entities have evolved into large, multi-branch organizations that must collaborate internally across geographically dispersed departments, with allies and with private sector partners such as closely coupled defense contractors. Email is an essential tool for facilitating communication within this distributed military environment, yet it also presents the challenge of containing electronic information within its intended perimeter of authorized users. Once released to an unauthorized recipient, an email can spread quickly, do instant damage and cost lives. In order to protect military communications, many military organizations are mandating that messages be classified before being sent. Classification requires that an electronic label, such as "Secret" be applied to emails. Based on such labels, the disposition of the email can be controlled. Classification is a key component of email security in the military, but simple labeling does not provide the flexibility to facilitate effective, secure communications. Multiple criteria, such as releasability markings or program information can further restrict the possible distribution of a message. Further, the ability to assign classifications to emails must be managed in a secure, centralized way. For example, the ability of a user to assign a Secret classification to a message may be revoked when a user is transferred to another project or department. Products such as Titus Labs Message

Classification allow the classifications or labels available to a particular user to be dynamically controlled by administrators.

When classification at the client is combined with corresponding logic on the mail server, military organizations can prevent the transmission of sensitive email outside a secure perimeter of authorized users. By preventing recipients from lowering or removing the classification of an email, forwarding and replying are similarly restricted.

Message classification in the military context is essential, and the traditional requirement to physically stamp paper correspondences has been extended to electronic messages. These organizations use sophisticated, multi-level email labels to specify security levels, releasability markings and legitimate recipients for emails that are used on complex programs involving multiple branches, private sector suppliers and allies. Prevention of security breaches is paramount for the military and centrally controlled administration of policies that define who can do what and when is an essential email classification requirement. The ability to force the user to classify messages is essential to preventing downstream breaches in the security perimeter as the message is passed from user to user.

Regardless of the industry or sector, the importance of managing email goes far beyond regulatory requirements. Consider that by some estimates, as much as 75% of an organization's intellectual property is contained its email system, much of it is in the format of casual communication between individuals. A sound email classification strategy, deployed in combination with a content management system can enable the

organization to capture, analyze and retrieve intelligence such as market insights, product or service ideas and more.

Titus Labs Message Classification

The Titus Labs approach to email management builds on the principle of end-user classification. This strategy is based on the following insights:

- The end-user or knowledge worker is the person best able to determine the proper classification and handling of email, including security, project based and retention classification labels. Server based content scanning technologies will never be able to match the knowledge worker in terms of proper classification of email.
- That the threat from trusted parties is not only malicious abuse of email, but also accidental misuse. For example, surveys have shown that up to 39% of workers have received accidentally misaddressed email that was not intended for them. Typical accidents include dragging the wrong attachment into an email, clicking Reply to All rather than Reply to, and relying on Autocomplete features to select recipients. Safe Recipient Lists and perimeter security technologies based on classifications can prevent inadvertent disclosure of sensitive information in these situations.
- That a well-designed and centrally defined classification system can be an effective mechanism for added security awareness, and mitigating user-originated mistakes. By enforcing classification policy at the point of email origination, users are forced to pause and consider both the sensitivity of an

email and the implications of mishandling it. Since an estimated 90% of mishandled emails are the result of hurried, careless mistakes, encouraging vigilance on part of users is an effective form of prevention. This vigilance also ensures that employees are accountable for their actions because they must make a conscious decision when making the classification.

Based on these observations, Titus Labs has developed a three-step approach to email policy management that recognizes the weaknesses in server-based content scanning technologies, provides effective security awareness and control, and scales with the enterprise.

Classify

A solid classification system, placed in the hands of knowledgeable end users, is a critical first step in the process of developing effective checks on email usage. Email creators are the subject-matter experts with the most useful insights into the nuances of the material they are writing. Enforced classification at the desktop serves to ensure that users: a) consider the ramifications of sending sensitive information through the email system, b) double-check recipients, and c) verify sensitivity of email attachments. It also helps ensure that email archived for regulatory or business intelligence purposes are categorized into an effective knowledge management and retrieval schema.

Titus Labs Message Classification™ supports classification labels for Microsoft Outlook and Outlook Web Access (OWA), as well as auxiliary mail interfaces in other Microsoft Office tools. Classification labels are embedded in message headers, away from intentional tampering. Labels can optionally be inserted as visual indicators on the first

line of the message, as automated abbreviations in message subjects, and optionally in the last line of the message, raising awareness among recipients. Users can be forced to make explicit classification selections before a message can be sent, ensuring that they make conscious decisions about the disposition of sensitive emails. Further, email classifications can be maintained across all retransmissions, such as forwarding, replying and replying to all. Multiple classification labels allow refinement of message handling. For example, a primary label might be “Unclassified” or “Confidential”, while a secondary label might specify a retention period.

Manage

An effective classification system is a sound basis for management. Systems such as archiving, content and document management systems all benefit from the classifications added to message headers by the Titus Labs solutions. Once the classification metadata has been added to the email it can be used to sort / search for specific information more quickly in archiving or document management systems.

Management of the classification system itself is also an important aspect of a successful system. Effective, secure and centralized administration of classifications deployed to the desktop requires centralized, flexible and secure control to ensure scalability to hundreds or thousands of users. Titus Labs provides powerful administrative management by building on proven Microsoft Active Directory and Group Policy technologies. From the centralized Group Policy console, labels can quickly be added to the users’ selections. Force selection can be turned on for all, or a selected group of users. Users can be added and removed from email policies on an individual or group basis.

Rights can be fine-tuned according to a user's clearance and needs. For example, a financial analyst working on a merger might be able to send and receive email correspondence related to "Mergers and Acquisitions", but not be able to send or receive correspondence related to "Mutual Funds Dept". Upon leaving the project, the analyst's rights can easily be revoked.

Control

Message classification and management are the basis for effective control.

Classification, applied in a controlled way by appropriate users, adds intelligence to email messages. Through the use of classification and a third party server based content scanning engine, corporations can ensure that private or confidential information is protected from unintended or illegal disclosure. For example, email administrators could define that email classified as "Confidential" could not be sent outside the company or could only be sent to trusted partners. In addition, Titus Labs' Safe Recipient List and "Trusted Domain" technology provides for recipient checking before email can be sent to ensure email distribution on a "need-to-know" basis.

Used in conjunction with an optional digital rights management system (such as Microsoft RMS), classification can provide additional control over the distribution and viewing of email.

Classification labels can also be used to provide effective archiving and retrieval in accordance with regulations such as Securities Exchange Commission disclosure rules, and permit sophisticated analysis and retrieval of the business intelligence within email messages.

Message Classification Enterprise Edition

Titus Labs Message Classification Enterprise Edition™ adds several advanced classification features not available in the base Titus Labs Message Classification client. The Enterprise Edition Safe Recipient List technology is used by forward-looking organizations to verify email addressees against rights policies. In the event that a user has included recipients to an email other than those permitted by a specific classification, Message Classification Enterprise can block transmission of the message and prompt the sender to remove unauthorized addressees before permitting distribution. Flexibility is achieved by allowing the administrator to apply safe recipient lists at the group or individual level.

Enterprise Edition builds on proven and scalable Microsoft Active Directory and Group Policy technologies to provide dynamic label lists that are available on a user or group basis and can be updated each time a user starts Outlook. This functionality is particularly important in environments where rights requirements change frequently, such as those where temporary teams are pulled together for frequent, short-term projects.

Microsoft Windows Rights Management Services

Windows Rights Management Services (RMS) is a digital rights management tool that provides additional protection for sensitive email. RMS applies persistent usage policies that are embedded directly in a message or document and stay with it wherever it is used. These rights can, for example, prevent an unauthorized user from opening an email that is sent to them in error, or can prevent a recipient from forwarding a sensitive email.

The Power of Classification with Microsoft RMS.

Titus Labs' trusted classification approach integrates seamlessly with RMS to provide enhanced security based on classifications. Rights policies defined within RMS can be assigned to email based on the classifications set at the client. As an example, all "Confidential" email could be automatically protected such that only company employees could view the message. Such a strategy helps ensure that email is protected against violation of privacy and security policies as it moves through the mail infrastructure. This approach can offer significant advantages to organizations such as financial institutions that are faced with requirements to protect correspondence and that may be asked to prove that records are tamper-proof. By combining client-side labeling such as provided in Titus Labs Message Classification and RMS, organizations can effectively secure, manage, analyze and retrieve large stores of unstructured messages.

Conclusion

Email has historically been a weak link in organizational security. While organizations have emphasized protection against threats posed by inbound messages, little has been done to protect against risks based on outgoing emails. Over the past several years, regulation of email management and security has been significantly enhanced in response to criminal activity, security breaches and terrorist threats. Organizations in a wide range of sectors, including the government, finance, health and the military, need to respond to more rigorous requirements. Classification is founded on the belief that the knowledge worker is the most appropriate person to classify email for security, retention and project bases. Classification at the desktop encourages users to exercise appropriate care and

caution when sending email, while putting effective knowledge management tools in the hands of the subject matter experts creating messages. By building management and control infrastructure on top of end-user classification, advantages extend from enhanced security and regulatory compliance to creation of rich, practical pools of business intelligence.

Additional reading

- <http://www.hhs.gov/ocr/hipaa/>
- http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf
- <http://banking.senate.gov/conf/grmleach.htm>
- http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp
- <http://www.dsd.gov.au/library/infosec/acsi33.html>
- <http://www.microsoft.com/windowsserver2003/techinfo/overview/rm.mspix>
- <http://www.microsoft.com/windowsserver2003/techinfo/overview/rmscompliance.mspx>