

SECURE ELECTRONIC COMMUNICATION: BEYOND THE COMPLIANCE CRISIS

White Paper
October 2005

Table of Contents

Executive Summary	3
Drivers for Secure Electronic Communication	4
Compliance	4
Summary of Requirements of Selected Regulations	4
Data Protection and Privacy	5
Essential Information to Form the Basis for Policy and Infrastructure	5
Opportunities for Business Improvement	6
Stronger Business Relationships	6
Better Decision Making	6
Enhanced Operational Efficiency	6
Revenue Growth	6
Technology Enablers of Secure Communication	7
Sun Java Communications Suite	8
Capabilities for Communication Security and Privacy	8
Integration with Sun Identity Management	9
Sun Compliance and Content Management Solution	9
Sun Java System Communications Suite in Action	10
Conclusion	12

Chapter 1

Executive Summary

Recent regulations affecting the security, privacy, and integrity of enterprise information have many organizations scrambling to comply with a multitude of new regulatory requirements. Much of the focus in this struggle has been on electronic communication, particularly on the need to archive e-mail and instant messaging to meet records retention requirements. But in the frenzy to formulate archiving policies, identify best practices for archiving, and implement archiving systems, many organizations are overlooking the larger context — a context which includes business improvement opportunities that have emerged from the compliance challenge.

The fact is that compliance is about much more than archiving — and security is about much more than compliance. The challenge of complying with regulations may be what has brought the issue of secure electronic communication to the fore. But now that it is front and center, organizations have a choice about how they see it: as a difficult, painful, and costly challenge being imposed from outside, or as an opportunity to improve business practices within the organization and thereby improve operations, customer satisfaction, and public image.

This paper will:

- Explore the drivers behind electronic communication security, which include not only compliance specifically but also data protection and privacy in general
- Examine the ways in which regulatory requirements have created opportunities to improve business practices and stimulate business growth
- Discuss the role of the electronic communication infrastructure in creating a secure environment that facilitates both regulatory compliance and business improvement
- Describe the Sun Java™ Communications Suite and related Sun™ solutions for secure electronic communication
- Provide real-world examples of organizations using components of the Sun Java Communications Suite to comply with regulatory requirements and to ensure data protection and privacy

The goal of this paper is to help organizations move beyond the seemingly panicked reaction to regulatory demands and begin to exploit opportunities exposed by these regulatory demands.

Chapter 2

Drivers for Secure Electronic Communication

The recent push to secure electronic communication in organizations is driven to a significant extent by compliance. But compliance is by no means the only driver for secure communication. The need to protect sensitive data and keep private information private is equally critical.

Compliance

Given the widespread recent media attention to laws such as the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley) and the Health Insurance Portability and Accountability Act (HIPAA), it's easy to forget that regulatory requirements — even those that specifically involve electronic communication — have been a part of the business landscape for a very long time. The Securities and Exchange Commission (SEC) Rule 17a-4, for example, which requires financial brokerages to retain certain communication and keep it accessible for a specified period of time, is part of the Securities and Exchange Act of 1934. It was recently reinterpreted to include e-mail and instant messages (IMs) among the forms of communication that must be retained.

One thing that is different about compliance today — and what is likely behind the scrambled effort to respond to regulatory demands — is the sheer proliferation of regulations. Since 1996, at least a half-dozen regulations have been passed that affect the way organizations handle electronic communication. Major examples of such regulations and their requirements vis-à-vis electronic communication security are outlined in the next section of this paper, “Summary of Requirements of Selected Regulations.” Not only are there many regulations to follow, the penalties for not complying are severe. Penalties in the neighborhood of \$2 million are not unheard of in cases involving failure to comply with SEC Rule 17a-4.

Another difference is that the widespread use of electronic communication beginning in the 1990s has complicated record keeping for organizations. No longer are policies and practices for storing and accessing paper records sufficient to comply with regulations. Organizations must also have a strategy in place for storing and accessing records of electronic communication such as e-mail and IMs.

Summary of Requirements of Selected Regulations

The following paragraphs sum up requirements related to electronic communication of just a small portion of recently enacted legislation governing the integrity and security of critical information.

The Gramm-Leach-Bliley Act (GLBA): Directed specifically at financial institutions, GLBA requires that institutions ensure the security and confidentiality of customer personal information (including, by implication, personal information included in electronic communication) against internal and external threats.

HIPAA: The portion of this health care regulation that is related to protecting the privacy of patients' personal identifying information requires that health care entities safeguard the confidentiality of patients' health information in any communication with or about the patients.

Sarbanes-Oxley: To protect the integrity of corporate financial information, the law requires public companies to retain every audit-related record (including e-mail and instant messages) for seven years. Another requirement of the law, which has not yet taken effect, is for real-time disclosure, which will necessitate monitoring of e-mail contents for relevant information.

These are just a few examples. Other recent laws that affect the way companies manage electronic communication include the Can-Spam Act of 2003 for marketers, the Tread Act of 2000 for the automotive industry, and the USA Patriot Act of 2001. And these examples are limited to the United States. The European Union Data Protection Directive, Basel II, and other international regulations have emerged to impose similar requirements in other countries. In addition, some of the U.S. laws can be applied to companies in other countries if those companies are listed on U.S. stock exchanges or, in certain cases, if they conduct business with companies in the United States.

Data Protection and Privacy

With each day seeming to bring more new headlines about breaches in the security of credit card numbers or other sensitive data, the importance of protecting sensitive data and keeping it private has become painfully clear. Even if there were no laws, regulations, or fines of any kind associated with this issue, the legal liability, loss of customer trust, besmirching of corporate reputation, and other business consequences of failure would be more than sufficient to motivate organizations to take action in the interest of data protection and privacy.

A thoughtfully crafted security policy is the cornerstone of data protection and privacy for any organization, and a strong security infrastructure built on that policy is the key to minimizing the risk of a data breach. Given the increasing reliance on electronic communication today — in everything from shopping for retail merchandise online to exchanging health care-related e-mail with doctors' offices — the security policy and infrastructure must specifically address these types of communication.

Essential Information to Form the Basis for Policy and Infrastructure

Articulating security policy and strengthening the security infrastructure are critical processes that begin with some very basic questions:

- How is electronic communication secured within and outside the organization? What potential exists for a breach in this system?
- How is employee and customer (or patient or citizen) privacy protected with regard to electronic communication?
- How is the integrity of electronically communicated data maintained?
- What policies and procedures have been applied to protect data and maintain the privacy of data across the organization? What is being done to ensure that they are uniformly applied throughout the organization?
- What access points exist to sensitive data or private information in the organization's electronic communication? Are these access points internal or external? How are they vulnerable to being breached?

Answering these questions is the first step in assessing the current state of data protection and privacy in the organization, and taking steps to secure data against unauthorized access. But doing so can be a challenge, especially when you consider the complex and often contradictory demands that can result when government regulation and corporate policy collide. For example, the Sarbanes-Oxley directive to protect data integrity by monitoring e-mail is an apparent contradiction to a corporate policy that protects employee privacy by limiting e-mail monitoring. Working through challenges and contradictions like these is a difficult but essential part of the process when laying the groundwork for effective regulatory compliance and data protection.

Chapter 3

Opportunities for Business Improvement

Improving the security of electronic communication, implementing archiving systems, more effectively managing access to data — all these steps are essential to achieving compliance. But they're not merely the means to comply with regulatory demands. They can also fuel business improvement through the institution of best practices toward stronger business relationships, better decision making, enhanced operational efficiency, and revenue growth.

Stronger Business Relationships

The point is so obvious, it may be easy to overlook: The main reason for an organization to implement policies, processes, and procedures that enable better data protection and privacy isn't simply to comply with laws or avoid getting sued. The main reason for an organization to do these things is to protect its customers, partners, and employees — to ensure the quality of their experience doing business with the organization, and to make sure that no harm comes to them as a result. Looking out for their interests is essential to building strong business relationships over the long term. When users can trust that their sensitive data won't be compromised and that their privacy is consistently protected, everyone benefits. Customers, partners, and employees enjoy a safe, quality online experience, which in turn increases their loyalty to the organization and improves its competitive advantage.

Better Decision Making

When it comes to technology for accessing, archiving, and retrieving electronic communication, the focus today is on compliance. The value goes far beyond that, though. Secure access, archiving, and retrieval aren't just about complying with laws; they're about enabling ready access to information in electronic form — whether that consists of current e-mails and IMs retrieved from anywhere at any time, or long-archived electronic data — and then using it to help drive better, more timely business decisions. Archiving and retrieval are the keys to creating institutional memory — not just to pass an audit, but also to learn from prior experience and apply what's been learned over time to today's decisions.

Enhanced Operational Efficiency

Secure electronic communication can contribute in several ways to operational efficiency. By reducing the risk of spam, viruses, and other intrusions, for example, a secure communication infrastructure limits the potential for business disruption and productivity interruption that such intrusions typically cause. In addition, secure communication can increase efficiency by enabling employees to work productively from remote locations.

Revenue Growth

A secure infrastructure for electronic communication is essential to exploiting new revenue opportunities that are born of extended relationships with partners, vendors, and others across traditional network boundaries. Take financial services, for example. Through secure, reliable electronic communication and data exchanges with partners, a financial services provider can offer more online services to more customers, improving its revenue opportunities. Without the assurance of secure electronic communication, it would be difficult for businesses to form trusted relationships for such purposes — and for customers to want to participate.

Chapter 4

Technology Enablers of Secure Communication

Secure electronic communication protects the integrity of information and guards the privacy of end users, enabling compliance with industry regulations and the achievement of important business objectives, such as stronger relationships and revenue growth. To ensure the security of communication such as e-mail and IMs, organizations must have in place an electronic messaging infrastructure with extensive security and privacy features such as:

User authentication: Ensuring that users are who they say they are is fundamental to secure communication using e-mail or IM.

Message and session encryption: Encryption ensures that e-mail and IMs, as well as the private information and sensitive data associated with them, will not be accessible to unauthorized users.

Virus and spam protection: E-mail and IMs are notoriously vulnerable to the effects of viruses and spam, and the electronic messaging infrastructure must include robust protection against these intrusions.

E-mail and IM archiving: At a time when so many regulations require that organizations store and provide access to electronic records, organizational policies must address the retention of electronic communication as a necessity for compliance. Processes must be instituted to protect the integrity of the data in saved communication, as well as the privacy of the communicator.

Privacy options: With so many opportunities now for instant messaging over public networks, privacy of communication has become an increasingly important requirement. For example, users should be able to control who can see their online status and communicate with them.

Secure access: Tying information access to the identity management infrastructure additionally secures electronic communication through the use of identity-based access policy, centralized user management, and single sign-on (SSO) across messaging and related applications. In addition, providing a virtual private network (VPN) on demand helps ensure convenient access when and where it is needed, without compromising the security of sensitive communication.

Chapter 5

Sun Java™ Communications Suite

The Sun Java Communications Suite for e-mail, calendaring, and real-time communication is expressly designed to secure electronic communication and protect user privacy. Its components — Sun Java System Messaging Server, Sun Java System Calendar Server, and Sun Java System Instant Messaging — are not only tightly integrated with each other, they are also highly integratable with other Sun solutions and third-party solutions. The following summarizes key security and privacy capabilities of the suite.

Capabilities for Communication Security and Privacy

Authentication: The Java Communications Suite employs multiple authentication mechanisms to ensure that users are properly identified and authorized. Java System Instant Messaging, for example, includes an Authentication Framework API that provides alternate authentication and SSO services to facilitate secure integration with third-party portal solutions.

Encryption: The encryption capabilities of the Java Communications Suite include not only client-to-server and server-to-server Transport Layer Security and Secure Sockets Layer (TLS/SSL) for e-mail and instant messaging session encryption, but also message encryption. Support for the Secure Multipurpose Internet Mail Extensions (S/MIME) protocol enables users to sign and encrypt e-mail and IMs to enhance security.

Virus and spam protection: Java Communications Suite capabilities for protection against viruses and spam are constantly evolving to stay a step ahead of these threats to secure communication. As part of this effort, Sun made the Java Communications Suite integratable with a variety of third-party, antivirus and antispam solutions. One example is the Symantec AntiVirus Scan Engine (SAVESE), which enables the messaging infrastructure to remove viruses from e-mails before they ever reach the end user.

Archiving: Java System Messaging Server is integratable with Network File System (NFS)-based storage solutions from Sun and other third-party vendors enabling organizations to easily store, secure, and manage their secure e-mail communication. And Java System Instant Messaging provides an archive application programming interface (API) that enables integration with any third-party archiving and compliance software. The API is fully preintegrated with Sun Java System Portal Server to leverage advanced search and retrieval technology.

Privacy: Extensive, user-controlled privacy options are included in the Java Communications Suite. These options go beyond protecting the privacy of e-mail to include calendar entries and instant messaging activities. Granular privacy controls enable end users to grant differing levels of access to their calendars. And users of instant messaging can exert flexible control over who can see and communicate with them online. For example, a user can create a “working at home” profile that specifies access only to selected team members.

Secure access: The Java Communications Suite can be integrated with the Sun Java Identity Management Suite to further secure electronic communication through identity-based access management, SSO, directory services, identity auditing, and other related capabilities. The Sun Java System Portal Server Secure Remote Access application uses VPN-on-demand technology to enable secure access by users who are connecting to systems from outside the firewall.

Integration with Sun Identity Management

The Java Communications Suite is tightly integrated with Sun™ identity management products, especially Sun Java System Access Manager and Sun Java System Directory Server Enterprise Edition. This bolsters security by enabling secure SSO and a fine-grained access policy for provisioning, down to the level of specific suite features. For example, users can be provisioned to employ only selected features of the Suite, depending on their roles in the organization. This identity-based access policy allows organizations to differentiate secure collaboration capabilities based on user login, workgroup, or role.

Sun Compliance and Content Management Solution

The Sun Compliance and Content Management Solution protects e-mail at all times while making it easily accessible when necessary. Organizations can use the solution in conjunction with the Java Communications Suite to focus on regulation-related data archiving and retrieval challenges. Based on the AXS-One Compliance Platform software, the solution delivers powerful capabilities for storing and managing electronic records.

Chapter 6

Sun Java System Communications Suite in Action

Two large organizations representing very different interests rely on the Java Communications Suite to achieve critical goals.

Health Care: Complying with Regulatory Requirements

The challenge: While consolidating its vast, distributed, heterogeneous communication infrastructure, a large health care delivery network faced the added challenge of ensuring regulatory compliance. Specifically, the organization needed to meet stringent HIPAA requirements for guarding the privacy of patients' personal data.

The solution: To consolidate electronic communication and applications across the organization, the health care network chose an integrated solution consisting of the Java Communications Suite, as well as components of the Java Identity Management Suite and Java Application Platform. The communication infrastructure serves nearly 17,000 e-mail users, including 10,000 remote users consisting largely of network physicians and their staff.

The technology: To prevent unauthorized access to patients' private information in electronic communication, the organization's Java Communications Suite implementation supports 128-bit Single Socket Layer (SSL) encryption as well as high-performance authentication. Integration with the Java Identity Management Suite enables secure, role-based access to communication and other applications.

The results: According to the organization's director of enterprise architecture and network security, in a recent HIPAA-related security assessment, the organization received high ratings for the security of its communication infrastructure. The report cited the organization's use of Sun's Web-based e-mail products as one of the reasons the level of security was so high.

The future: To meet regulatory requirements and organizational goals for e-mail archival, the health care network is now working with Sun to integrate centralized archiving and access capabilities into its communication infrastructure.

Nonprofit Sector: Safeguarding Users' Sensitive Data

The challenge: One of the world's largest religious organizations required a highly secure and reliable communication infrastructure to support secure electronic communication with millions of followers worldwide.

The solution: To support its high-demand, e-mail environment (100,000 messages a day), the organization chose the Java System Messaging Server, which provides multimedia messaging services, a mail transport agent, and mail multiplexing capabilities to enable robust, secure Web-based e-mail. Other software components of the integrated solution include Java System Directory Server to manage user access to applications and Java System Web Proxy Server to provide the Web interface to e-mail.

The technology: In the interest of data protection and privacy, the Sun messaging implementation features security strengths such as multiple authentication mechanisms that the organization employs to identify valid users and addresses; SSL and transport layer security (TLS) support for session encryption; and server-side rules for filtering messages to weed out spam and viruses.

The results: According to a representative of the organization's Internet Office, the ability to safeguard the messaging environment made it possible to serve one of the most high-demand communication environments of its kind, while minimizing risks to data security and privacy.

The future: The organization is expanding its Sun communication infrastructure to include other components of the Java Enterprise System, including Portal Server, Identity Server, Access Manager, and related applications.

Chapter 7

Conclusion

Compliance has become a top priority and primary driver of electronic communication security and privacy initiatives for many organizations today. But it is important to keep in mind that security and privacy are about much more than compliance. They are aspects of electronic communication that can also empower organizations to strengthen business relationships, make better decisions, operate more efficiently, and increase revenue growth. Investing in the right security and privacy solutions for electronic communication can do much more than enable compliance with regulatory requirements; it can also allow organizations to achieve key business objectives.

Your business runs safer with Sun. The Java Communications Suite and other Sun solutions are designed to address every aspect of secure electronic communication, from authentication and encryption to virus protection and privacy options.

To learn more about the Java Communications Suite and its role in achieving improved security and compliance, or to request additional information about the suite and its components, visit sun.com/comms.

© 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

Sun, Sun Microsystems, the Sun logo, Java, and the Network is the Computer are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.