



September 2009

We've updated The Compass to compliment our new website design!

See what else is new by **visiting us** on the web.

Meet Experts of The Compass at the Following Events:

2009 Calendar of Events

10|08 CCUL Mt. Diablo Chapter Casino Night Fundraiser, Pleasant Hill, CA

10|14 WIB Annual Bank Technology & Security Summit, San Diego, CA

Archive Download

Download a printable PDF to share with colleagues or access **The Compass** archives:

» The Compass, September 2009 - **Download** (PDF)

» The Compass - **Archives**

Sign up to receive The Compass monthly.

Not already on our mailing list? Our monthly newsletter will help you keep abreast of industry and regulatory developments for the financial industry. **Sign up now!**

Contact us!

We are constantly working to improve **The Compass** and appreciate your feedback! Send your comments to: **education@compushare.com**

Rate this article!

Click here. Your response will take less than 1 minute!

Ensuring Email Compliance – Key Considerations for Security and Regulatory Compliance

**by Karn Griffen
Chief Technologist
Compushare, Inc.**

As I mentioned in the **March Compass** edition on reducing email costs, "email" as we used to know it – a simple messaging solution – has grown into a complete communications platform, often incorporating mobile access, live conferencing, group calendaring, and task management among other features. In addition, the cost of properly maintaining regulatory compliance and securing email has increased. In most of our clients' organizations, reliance on the email platform has muscled its way into the "mission critical" category. This is especially true in institutions that employ call centers, customer service departments, or communicate in any way with their customers or staff by email.

Proper messaging compliance and security should now be considered among the most critical infrastructure elements, and as an absolute necessity for community financial institutions. As such, it is important to deploy a solution that provides the best combination of threat remediation, throughput and overall cost effectiveness.

In this issue of the Compass, I will outline the major areas of concern for ensuring email compliance and security. Financial institutions should consider the following as a guidance for strategic planning.

Security and Compliance Are as Difficult as Ever

As communication through electronic mediums has become more of a standard between the institution and customers, legal counsel, other institutions, regulatory bodies and audit firms, the criticality and legal liability for ensuring safe electronic communications has increased. At a minimum, financial institutions must consider the following in designing and implementing a messaging solution:

- Spam and Virus Protection
- Content Filtering
- Encryption
- Remote Access
- Mobile Access
- Archiving

Spam and Virus Protection

You must have this, period. With over 95% of electronic communications being classified as spam, and every 1 out of 150 emails containing a virus, there is absolutely no way that you should not have Spam and Virus filtering inbound AND outbound.

Content Filtering

Covering the misuse of electronic mail by your employees, content filtering typically prevents outgoing email by categories, or specific words, or both. The lexicon that is used to block unwanted outbound mail grows over time and depends on each individual institution's tolerance. While not specifically mandated by regulatory agencies, it is a good idea just for legal liability reasons.

Encryption

Also a must-have nowadays, encryption should allow you to seamlessly encrypt message by the employee's choice, and also allow you to automatically force encryption using a lexicon of words or number patterns. Encryption should require a quarantine that audits offenders, and lists the reasons for encryption.

Remote Access

Most institutions allow some sort of remote access to email. When dealing with off-site employees, remember that anything sent in an email can be then downloaded to that remote computer and can no longer be controlled by the institution. Here, email archiving can help if there was a need to verify that the communication actually reached remote parties.

Mobile Access

With the advent of Treo, Blackberry, Activesync, and iPhones, mobile messaging is here to stay. Mobile access carries with it the same risks as remote access, with the added risk that devices can easily be misplaced or stolen, triggering your incident response plans and requiring notification to customers that their information could be in the wild. Strict policies governing mobile devices must be created and enforced including password protection, device encryption, and remote wipe capabilities.

Archiving

Possibly the most confusing of the above issues is archiving email. Is archiving necessary? What is the appropriate length of time to store email? How should policies be set? Many clients are relying on pseudo-archive technology (such as storing emails in a .PST file), which relies on the end user to determine if a message should be archived. This user controlled approach can consequently result in litigation, financial penalties, HR problems, as well as damage to company reputation if proper archiving policies are not followed.

Of course, if your institution is overseen by the SEC or NASD, you already know that you are required to maintain compliant email retention up to seven years. For smaller institutions, you are still advised to have a method to retain electronic messages that would pass muster in a court of law.

The OCC issued an **Advisory Letter of Electronic Record Retention** on June 21, 2004. The Advisory Letter points to the **Electronic Signatures in Global and National Commerce Act** (E-Sign) as special reason for financial institutions to set up electronic record keeping systems. The E-Sign Act generally confirms the legal effectiveness of electronic commerce transactions, including e-mail contracts. The implication for financial institutions is that their electronic records, such as e-mail records, can be evidence of legally-binding contracts and other transactions. The OCC Advisory Letter states:

"Banks should design, implement, and operate their electronic records systems so that they are adequate to serve the following purposes and functions according to the nature of the retained records:

- Potential use in litigation support,
- Internal and external audits and controls,
- Bank supervision, and
- Compliance with regulatory requirements."

The Advisory Letter goes on specifically to emphasize the retention of electronic message and email records.

Consistent with the OCC Advisory Letter, the FDIC has also issued guidance on the retention of electronic records under the E-Sign Act.

The FDIC Handbook states: "Record Retention. The E-Sign Act requires a financial institution to maintain electronic records accurately reflecting the information contained in applicable contracts, notices or disclosures and that they remain accessible to all persons who are legally entitled to access for the period required by law in a form that is capable of being accurately reproduced for later reference."

The **FDIC's 1998 Electronic Banking Safety and Soundness Examination Procedures** specifically discuss record retention procedures for e-mail. Page 8 says examiners should expect financial institutions to have retention policies for e-mail. It reads: "Determine if retention guidelines exist and are updated for source documents supporting electronic activities, such as account applications, instructions for account transactions, and other records. Determine whether the guidelines also address electronic mail, data files, and similar records."

For these reasons, we believe that all financial institutions should have a formally written policy in place and have an archiving solution that meets the Federal Rules of Civil Procedure (FRCP). At a minimum, the archive must:

- Eliminate the employee's choice in saving email. All email must be archived for the period chosen.
- Provide easy, fast and simple discovery tools to find relevant emails.
- Ensure email cannot be tampered or altered after being stored on the archive
- Ensure that all access is auditable.
- Ensure that end users are aware of the policies and procedures and have signed off on those procedures.

In conclusion, maintaining an effective messaging solution for the institution is not as easy as simply turning on a group of Gmail accounts for the users. Each security and compliance consideration discussed above must be thoroughly addressed by the institution with the proper policies and procedures put in place. Furthermore, email now

being a mission critical application, you must ask yourselves, how long can the institution tolerate not having access to email in the event of an outage? How will you recover, resume business and communications, and conduct damage control to mitigate potential loss to reputation with your customers? Compushare can provide your institution with expert guidance and a truly comprehensive solution built specifically for your messaging requirements unique to your institution. For more information on Compushare's email security and compliance solutions, please reach out to your Client Solutions Executive or contact me at kgriffen@compushare.com.

###

Compushare delivers viable and proven solutions exclusively for community financial institutions including areas of information security, risk management, business continuity, business resumption, hosted email, archiving, encryption and message security. Learn more about our approach toward **Strategy, Safety, Soundness** and **Support**.

To learn more on how your institution can benefit from a hosted message collaboration and email solution, contact your Client Solutions Executive or education@compushare.com.

© 2009 Compushare, Inc. All rights reserved.