

EMC PERSPECTIVE



Reader ROI

- The National Association of Securities Dealers (NASD) and other regulatory agencies have established standards for electronic data including communications generated by e-mail, instant messaging (IM), chat rooms, and blogs.
- To comply with regulations, financial services firms must monitor and protect these communications.
- An effective risk management/communications management program requires attention to policy, process, governance and stewardship, and consistent enforcement via automated solutions.

Managing Risk of Corporate e-Communications

In today's stringent regulatory environment, corporations are required to comply with the supervisory and correspondence review requirements of the National Association of Securities Dealers (NASD) and those of the various exchanges. Evidence of compliance must be available for auditors when demanded.

The regulations, which have grown out of concern about insider trading and the misuse of information, guard against the destruction of information which might be used as evidence in a court of law. Thus, firms must have in place stringent data protection systems.

Business communications in the 21st century

While some of today's electronic chatter is informal, much of it is related to business objectives and responsibilities. Today, people discuss the latest tips via chat rooms, instant messaging, and e-mail. Cell phones, blackberries, and other mobile communication devices are extensions of the corporate communications system.

This reliance on electronic communications has prompted an increase in regulations requiring that these communications be monitored and stored as part of the firm's records. This mandate places the first line of data compliance with the individual corporation.

When is chat on the record?

The NASD Conduct Rule 2210(b) clearly states that sales literature, both written and electronic, must be maintained as part of the books and records. And registered representatives are required to follow the same rules when participating in chat rooms as they would if standing in front of an audience. So if a representative uses his home PC for work, his firm is responsible for the integrity of the content of his communications.

This regulation makes it easy for employees with no malice or wrongful intent to put their employers at risk. This, in turn, places their job and career security at risk, as well. Depending on the nature of the violation, an employer may have no alternative but to terminate even the most productive employee.

Further, electronic messages—including e-mail, chat, IM, text messaging, e-fax, Blackberry, message boards, and blogs—once “monitored and stored” as part of the books and records, leave behind an indelible record or “electronic DNA” that exists for a considerable period in its original form for all to peruse. This record, if subpoenaed, stands as irrefutable.

Managing risk

Clearly, vigilant corporations must establish risk management programs that include electronic surveillance of electronic communications. A good risk management program incorporates several components:

- **Communications policy:** The Office of General Counsel (OFGC) typically establishes policy management for a comprehensive list of electronic communication types.
- **Training of employees:** Employee training in appropriate use and storage should be reinforced regularly and augmented by additional safeguards.
- **Electronic signature:** The electronic signature can be used as proof of the firm's communication of its policies as well as to validate employee understanding of the firm's policies.
- **Automation:** Manual processes are often applied inconsistently. Automation provides more consistent enforcement of policy governing access rights, archival capability, and retention.
 - Many vendors offer surveillance programs that send alerts, signaling suspicious communication or behavior. Policies may flag communications based on language or content that demonstrate inappropriate employee behavior, theft of intellectual property, or content that signals money laundering or other fraudulent activity.
 - Automated archiving capability affords the firm the tools to respond quickly to regulatory assessments and legal inquiries.

- **Governance:** Governance integrates key issues and components of the policy management program. Key to the governance structure is the role of the steward who must:
 - Understand regulations driving electronic communications surveillance.
 - Establish data quality metrics and monitor and report on data quality.
 - Enforce/reinforce best practices.
 - Provide a framework for project governance, collaborating with various teams which may use different methodologies.
 - Oversee the integration of stovepipe technology systems.
 - Assume the responsibility for issue/risk identification, tracking, reporting, and mitigation.

Data management imperative

While communication at the speed of light has enabled economic advances, it has ushered in an era of new business risks. Poor data practices can affect a firm's credibility, its bottom line, and its market value. It is imperative that companies proactively protect themselves from the misuse of communications channels by establishing risk management policies to monitor and archive communications. These records furnish proof of regulatory compliance and may be used as evidence in legal matters.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com