OnBoard Quarterly

Volume I, Issue II
JUNE 2006

INFORMATION ON BOARD RELATED ISSUES BROUGHT TO YOU BY THOMSON FINANCIAL

"The most valuable or sensitive data, such as corporate trade secrets or financial data, should be secured by a password and a second authentication method, such as fingerprints or a token that generates a constantly changing second password."

Michael Totty
The Dangers Within
Wall Street Journal Special Report
on Information Security
February 2006

Ensuring Secure Board Communication

In today's high pressure board environment, directors are continually challenged by the difficulties of learning about their company with limited available time. The demands for more information and faster delivery have forced directors to find new communication channels to get the information they need in the most efficient way possible.

Although traditional mail is still the primary delivery method for distributing board-related materials, directors have increasingly turned to the Internet and e-mail as a solution. But despite gains in productivity and accessibility, boards might also be taking on more risk than they bargained for.

According to the 2005 Benchmarking Survey conducted by the Society of Corporate Secretaries and Governance Professionals, just under 90% of respondents use electronic communication methods for the board. Roughly two-thirds restrict such communications to e-mail messages, with 53% using non-encrypted e-mails and just 13% using encrypted e-mails. (See Figure 1, next page)

Recent events have put a spotlight on the security of e-mail communications, including highly publicized breaches of personal financial information, compromised information on stolen laptops, and the passage of regulations governing privacy and data security. Proofpoint's May 2005 survey of 332 e-mail decision makers at US companies with more than 1,000 employees found that 35% of companies had investigated a suspected e-mail leak of confidential or proprietary information in the past 12 months.

Security threats from e-mail messages are not new to corporations—spam, viruses, worms, phishing scams, and denial of service attacks are just a few of the villains that target e-mail users and the information they send. The rapid adoption of e-mail as a delivery medium, however, has resulted in significant exposure of personal and corporate information.

E-mail's "Most Wanted"

The consensus is that e-mail sent over the Internet is not a secure method of information transfer due to several inherent risks:

- E-mails can be inadvertently forwarded or mis-delivered, arrive late or not arrive at all. Timeliness of information is critical for directors—they need sufficient time to review materials and prepare for meetings.
- The information contained in an e-mail can be intercepted, corrupted, or destroyed. E-mail messages often contain viruses designed to harvest confidential information. An analysis of e-mails conducted by Symantec showed that 54% of all "malware" is designed to extract confidential user data. In addition, numerous software programs exist that are designed to hack into e-mails from both internal and external sources.

- Corporate e-mail boxes are often monitored, allowing unauthorized access to potentially sensitive content. The Proofpoint survey found that more than a third of companies employ staff to read and review outbound e-mail. With corporations now monitoring most e-mail communications, the "enemies within" are even more of a risk than external sources. According to Gartner, more than 80% of high-cost security incidents occur when data from inside the organization gets out.
- Even encrypted e-mails are subject to certain threats, primarily from an organization's own employees or former employees. Research shows that insiders are the most likely culprits of security breaches—8 out of 10 times hackers of corporate information come from inside the company. In fact, law enforcement officials estimate that 60% of computer system break-ins are the result of employees gaining unauthorized access.

Despite these risks, e-mail continues to be used to transmit confidential information. Proofpoint's findings indicate that almost 25% of outgoing e-mails contained content that could pose a legal, financial, or regulatory risk.

With Friends Like These...

The use of e-mail entails risk that proprietary or confidential information will be exposed, which could be extremely damaging given the sensitive information corporate secretaries disseminate.

Specific laws now govern many e-mail communications. The Gramm-Leach-Bliley Act, SEC Rule 17a, NASD Rules 3010 and 3110, and the HIPA Act all contain provisions for maintaining security, privacy, and non-disclosure of e-mail communications. Although Sarbanes-Oxley does not specifically point to e-mail, it does require the safeguarding of information against unauthorized access and therefore has implications for the use of e-mail messages. In addition, any inadvertent disclosure of material information could run afoul of Regulation Fair Disclosure (Reg FD).

Aside from the regulatory issues, enforcement of e-mail communication policies makes good business sense. A 2003 CSI/FBI Computer Crime and Security survey demonstrated that organizations lose millions of dollars a year due to lost or stolen information. In addition to financial and regulatory risk, disclosure of confidential information has high reputation risk and could lead to competitive disadvantage, violate corporate privacy guidelines, and possibly result in fines or legal action.

Figure 1: Electronic Communication

Almost 90% of respondents use some form of electronic communication for the Board:

E-mail	53%
Encrypted e-mail	13%
Web site for board communications	12%
Deliver board meeting materials electronically	27%
Considering using some form of electronic delivery	36%
Provide hard copies of the materials at board meetings	41%

Source: Society of Corporate Secretaries and Governance Professionals, 2005 Benchmarking survey

The bottom line: time sensitive and confidential communications should not be sent via general e-mail. If a board wants to keep its communications safe, it should invest in encryption software that allows entitled users to open the mail but prevents them from forwarding, altering, or duplicating it. Alternatively, it can invest in a board portal that allows for secure point-to-point messaging and document archiving.

The Rise of the Board Portal

A portal is a Web site that serves as a starting point for other destinations on the Web. Online services like AOL were part of the first Web portals which simply provided access to the Internet. Now

more sophisticated Web portals such as Yahoo! offer e-mail, search engines, discussion forums, and online shopping so their site becomes a primary "gateway" to the Web.

Portals can also refer to sites that offer specific services to a particular set of Web users, such as a bank portal where customers can access their checking, savings, and investment accounts. A board portal is a secure Web site that allows corporate secretaries to post information and allows directors online access to board materials. Typically, these solutions contain some or all the following features:

- High level of security to protect sensitive material
- Central repository for board-related materials
- Ability to easily access and distribute materials electronically
- Calendar of board and committee meetings
- Online board book creation and review
- Committee workspaces for online collaboration
- Online approval of minutes and/or resolutions
- Access to corporate and peer financial information
- Secure messaging capability

Board portals help streamline the cumbersome board communication process, thereby saving time and effort and increasing the effectiveness of board and committee work, with the ultimate goal of allowing directors to make better, more informed decisions.

Board Portal Security: Are Passwords Enough?

Protecting access to potentially sensitive data and other information is critical—any solution needs to be secured and encrypted with the latest technology. Yet security also needs to be balanced against accessibility, for example, requiring directors to remember answers to a list of security questions may place an undue burden on them.

Although passwords do offer a certain amount of protection, they are a weak foundation for authorization and access control. In fact, according to Secure Computing, 12% of audited network accounts had the word "password" as the password and 35% of passwords can be found in a user's work area—like on a sticky note.

Passwords are also vulnerable to attack and theft—social engineering to gather personal information and keystroke grabber software that captures passwords from public internet computers are just two of the risks associated with passwords.

Stronger and more effective options exist that can significantly improve a portal's data security. More secure authentication methods include tokens, smart cards, digital certificates and biometric readers. These methods use multiple factors for identification, combining something you know—like a password or PIN—with something you have—like a fingerprint, iris, voice scan, or hardware token—into a system referred to as two-factor authentication.

35% of companies have investigated a suspected e-mail leak of confidential or proprietary information in the past 12 months

Source: Proofpoint's May 2005 Survey

Two-factor security tokens with rotating passcodes have emerged as a good balance between security and accessibility. They act like your ATM card on the Web. In fact, all U.S. banks will need to offer some form of 2-factor authentication for access to their online banking systems by the end of 2006.

Other Key Drivers of Adoption

Beyond security, there are two other drivers that have accelerated the movement towards board portals as a solution to the communication and information needs of directors:

Usage – There is a behavior change that has to occur to get boards online so the simpler, the better. Some directors are not familiar with technology while others are easily able to access the Web, check e-mail, or use online software products. Too many bells and whistles can reduce usage, while user-friendly screens and consistent Web-based navigation can assist in migrating directors online. The use of e-mail alerts can also drive users back to the portal and encourage this desired behavior change. Board portals can also provide directors with additional reasons to routinely log in, such as including links to third-party information.

Accessibility – Efficient communication between the board and the company is needed, however, board books are not the most effective means of communication. A board portal can save significant time and effort for Corporate Secretaries and make their jobs easier. At the same time, electronic communication and delivery can help directors do more with less time by increasing the effectiveness of their board and committee work.

Since it is accessible via the Internet, Directors can log in to a board portal anytime, anywhere. The Web can provide instant access to information but it can also provide easy access to an historical archive. Directors value a central repository of board information as it is often difficult for them to digest the current board book let alone be expected to recall what was discussed and decided on at prior board meetings.

For these reasons, Web-based board portals have emerged as a cost-effective solution to securing board information online while also providing additional tools to assist in board processes and workflows.

Conclusion:

Today's information needs require that boards become more efficient in how they receive and send information. And while the overall trend toward utilizing technology to facilitate board communication is building, there are tradeoffs between improved efficiency and information security. Clearly, a need exists for a service that meets the communication, information, and security needs of both corporate secretaries and directors. Such a service would streamline the board communication process, save time and effort for directors and corporate secretaries, and help directors to be more informed and make better decisions while providing greater assurance that market-moving information remains secure.

Going forward, expect interest to grow in Web-based portals that provide boards with a cost-effective and secure means of streamlining and improving their board communications.

Byline written by Greg Radner, SVP of Thomson Financial Corporate Executive Services.
He can be reached at 617-856-1696 or greg.radner@thomson.com.