New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 247—NO. 63
TUESDAY, APRIL 3, 2012

FEDERAL E-DISCOVERY

More Than a Security Risk: Director E-mails in Discovery

By **H. Christopher Boehning**
And **Daniel J. Toal**

In today's economy, where so much business is transacted remotely or on the go, corporations would be well advised to focus on communications with their outside directors. And outside directors would be well served to consider the personal disclosure burdens and risks they may face as a result of their board service. Corporate directors today are frequent travelers who often serve on multiple boards. To accommodate their lifestyles, corporations often send board books and other sensitive communications to directors by any means available, including via the director's private or "day-job" e-mail accounts. In addition to the security risk this practice creates, many directors do not realize these accounts will be vulnerable to discovery in the event of litigation. Companies (and directors) confronted with this reality need to be mindful to balance the desire for security against the risks and burdens associated with the possibility of intrusive discovery into the personal e-mail accounts of their outside directors.

The Practice

The results of a recent Thomson Reuters comprehensive global survey of corporate counsel and company secretaries about board communications and director behavior are unsurprising. The survey revealed that

ISTOCK

corporate directors travel frequently, live across the world from their companies, and must often receive board updates from afar and on the go.[1]

More surprising to the tech savvy observer, however, is the extent to which corporations send board members their board books to non-company e-mail accounts. According to the survey, nearly two-thirds of companies do not issue company e-mail accounts to board members, yet 49 percent of companies report sending board materials over e-mail. Another 37 percent of those surveyed reported either that company document preservation protocols do not call for routine retention of board e-mails, or that they were not sure whether e-mails were retained.

Board member habits are likely the root cause of this practice.[2] Peripatetic directors conduct board business over tablet computers and smart phones.[3] A major concern of corporate secretaries and in-house counsel is that, as a result, confidential information will be leaked as directors continue to receive board books over e-mail. They resoundingly agree that director travel habits are a major obstacle to ideal corporate governance and information security.[4]

The Visible Problem

It is no wonder that the gatekeepers of corporate information stay up at night worrying about the security consequences of sending information to traveling directors. Sensitive financial information contained in board materials is enticing bait for thieves. Last year, 300 companies' sensitive information was compromised when hackers penetrated the security system at NASDAQ OMX's board portal "Directors Desk."[5] Remote desktop access sends security personnel into a frenzy over all of the potential risks to corporate data. Some have begun to demand complex login procedures to avoid security breaches.[6] The corporate attitude towards electronic communication sometimes resembles a "fortress mentality."[7]

Companies struggle with how to balance providing convenient board book access for their directors with ensuring security of information. But adding security may just provide directors with more incentive to request workarounds. What is a company to do when it receives a plea from a director struggling with security measures or Internet access to "e-mail it to my BlackBerry?" The risk of security compromises, though, is not the only reason to search for alternatives to the practice of sending board books to personal e-mail addresses.

H. CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison LLP.* LAURA BOWER, *an associate at the firm, assisted in the preparation of this article.*

The Unforeseen Problem

An often unanticipated and always unfortunate consequence of e-mailing board books is that board members may be subjecting themselves to invasive searches of their private files and e-mails if litigation erupts.[8] Many outside counsel have had awkward conversations with directors about the need to search their home files and private e-mail accounts.

While this is not uniquely a Delaware phenomenon, Delaware law on this subject is noteworthy both because of the frequency with which companies incorporate in Delaware and because Delaware courts have made their position on director e-discovery clear. The Delaware Court of Chancery issued guidelines on best e-discovery practices last year. These guidelines are designed to "remind all counsel…of their common law duty to their clients and the Court with respect to the preservation of electronically stored information ('ESI') in litigation."[9]

> Experience has shown that some of the potential problem areas regarding preservation of ESI include business laptop computers, home computers (desktops and laptops), external or portable storage devices such as USB flash drives (also known as thumb or key drives) and personal e-mail accounts.

Delaware courts do not take this duty lightly. In 2009, Chancellor William B. Chandler III ruled on a motion to compel in *Grace Brothers* v. *Siena Holdings*.[10] Grace Brothers filed the motion to force Siena to produce e-mails sent to and from the board of directors, most of whom received board e-mails via their private accounts. Grace Brothers responded that the e-mails would be wholly duplicative of e-mails already in the production.

Chandler was distrustful of defense counsel's assertion that there would be no unique e-mails because "Siena failed to even ask that the directors look for any relevant e-mails in their accounts." The court held that it would not be overly burdensome to require Siena's directors to produce e-mails from their personal accounts, despite the risk that very little new information would be gained by a search of private e-mails, and granted Grace Brothers' motion.

This risk of finding unique e-mails seems particularly acute in light of the above statistic noting that many companies do not routinely retain e-mails to directors. At those companies, a director's personal e-mail account may very well be the only place those communications will be available.

Vice Chancellor J. Travis Laster went a step further in *Roffe* v. *Eagle Rock Energy*.[11] In response to plaintiff's discovery requests, counsel to Eagle Rock asked board members where they stored communications from the company. The directors assured counsel that they had diligently saved each e-mail in a folder designated for board communications and forwarded the contents of the folder for production. Finding this insufficient, the court scolded the attorneys for failing to supervise these e-mail searches personally:

An often unanticipated consequence of e-mailing board books is that board members may be subjecting themselves to invasive searches of their private files and e-mails if litigation erupts.

> And if he chose to use his personal computer, well, that was his bad choice. All right? And if he has it mixed in other stuff that he gets, 150 e-mails a day, or whatever, that was his bad choice. That makes it all the more essential that a lawyer get on a plane, and go and sit down with Mr. Smith, and go through his e-mail and make sure that what is produced is—what is responsive is appropriately produced.

These attorneys were then faced with the awkward task of explaining to the directors why they would need to be visiting them at home. Delaware Courts have ordered and likely will continue to order discovery of directors' personal e-mail accounts when they are used for company business.

As they often do, other jurisdictions are likely to follow Delaware. The U.S. District Court for the Southern District of New York has held that work-related documents and e-mails in the possession of an employee are under the control of the employer and therefore discoverable. In fact, federal courts have ruled that corporations must ask former employees for documents in their private possession that may be discoverable.[12]

Solutions

Corporations must find a way to protect the security of their sensitive financial information while still facilitating communications with directors who must execute fiduciary duties in a timely fashion while on the road. In order to protect directors from discovery of their personal accounts and computers, the proper tool will need to have the following features:

- A way to alert a director when important information is available without revealing sensitive content about the information;
- The ability to access and edit documents without saving them locally to a laptop or tablet;
- Emergency access to board materials on a device (such as a smart phone) when no computer access is available to the director that will not make the other contents of the device discoverable; and
- Easy but secure remote access for a director who does not use the program every day.

A few solutions have been proposed. Commentators have suggested that board-packs be sent exclusively over highly secure company issued e-mail accounts to minimize risk of hacking.[13] If executed perfectly, this would also protect director e-mail accounts. Unfortunately perfect execution eludes directors. The average director of a public company holds three directorships (and a job) but prefers to operate from one account that is programmed to "ding" the smart phone.[14] In addition, security measures may lock directors out of seldom used company accounts. Evidence has shown that, when work e-mail is creating delays, executives often resort to personal e-mail accounts for business purposes. [15] Directors do the same. Finally, documents downloaded onto a director's own computer from these e-mail accounts may make the contents of the director's computer discoverable.

Another method companies increasingly use to combat the security risks created by mobile directors is the "board portal." A board portal is an online workspace designed to give remote, secure access to confidential information to board members.[16] The corporate secretaries upload the information to a secure portal that directors then access remotely. Increasingly, board portals are adapting their technology to accommodate the needs of directors without

compromising security.[17] Unfortunately, board portals have yet to strike the perfect balance.[18] Complex security measures and multiple passwords (as well as multiple logins for directors who serve several boards) frustrate the purpose of the portals because impatient directors bypass the security measures.[19] For any platform to work, directors must embrace it. At present, as noted above, board portals are too attractive to hackers to loosen security measures to facilitate ease of access.

Some companies have created home grown portal-like methods for disseminating encrypted information. Instead of e-mailing the director, the corporation sends the information directly to the director's tablet using a secure application. The downside is that to edit documents, the director must save them locally. Litigants will request the annotated versions so the contents of the tablet will still need to be harvested, read, and produced.

An ideal solution may involve a hub where a director can direct the flow of all information she receives from the different boards she serves. The "directornet" could issue the director a smart phone and/or a tablet to use exclusively for board purposes or carve out isolated space on the director's existing devices for each board. The director would only need one set of log-in data that she would use almost daily.

Conclusion

Regardless of the method chosen, corporations would be well advised to closely consider the risks of continuing the practice of sending e-mail board books to their directors. A director, like many of those in the Thomson Reuters survey, whose company will not pay for a portal or a company e-mail account, still has options. Companies should be more assertive in taking steps to ensure that board book materials are transported and stored in a safer environment. Companies should establish and require compliance with best practices for storage of materials, e.g., saving into a dedicated, password protected folder on a hard drive. And companies should educate directors of the risks they face in the event they seek to avoid these policies. Absent a better alternative, a director should set up an e-mail account to use exclusively for board business. Since such a director will be helpless to protect the security of sensitive information, at minimum the director can protect her personal data and her home company's data by maintaining strict separation between board and personal or work e-mails.

•••••••••••••●●•••••••••••••

1. Kimberly Allan, Better Board Governance: Communications, Security, and Technology in a Global Landscape of Change: Results of the 2011 Thomson Reuters Board Governance Survey, 4 (Thomson Reuters 2011).

2. John Steven & Hilary Kincaid, "Are electronically-delivered board packs a good idea?," *Minter Ellison Corporate HQ Advisory*, Sept. 12, 2011.

3. London Stock Exchange, "BoardVantage Announces iPad Briefcase," London Stock Exchange Aggregated Regulatory News Service, Jan. 28, 2011.

4. Allan, supra note 1, at 10.

5. Dominic Jones, "NASDAQ hack targets Fortune 500 board secrets," *IR Web Report*, Feb. 6, 2011, http://irwebreport.com/20110206/directors-desk-hacked/.

6. See, e.g., Mathias Thurman, "Security Manager's Journal: First task is to tighten up SaaS security," *Computerworld*, Dec. 6, 2010, http://www.computerworld.com/s/article/352873/Tightening_Up_SaaS_Security.

7. James Brashear et al., "Mastering New Technologies for Boards and Corporate Secretaries," Society of Corporate Secretaries & Governance Professionals, Oct. 17, 2011.

8. While the focus of this article is director discovery, it is worth mentioning that directors are not the only employees who bear discovery risk when using home accounts and devices for work purposes. For example, in *Koosharem v. Spec Personnel*, Magistrate Judge William Catoe ordered eight employees who had used their personal accounts and computers for work purposes to "turn over their home and work computers to a third party for forensic analysis." 2008 WL 4458864 (D.S.C., 2008). The government has also sought discovery into private e-mail accounts used to send work information, including "diaries" employees keep by sending e-mails to themselves. See, e.g., The Financial Crisis Inquiry Commission, "Early 2007: Spreading Subprime Worries," *The Financial Crisis Inquiry Report* 238-39 (2011) (quoting e-mails sent by Bear Stearns employees from personal e-mail accounts concerning the financial crisis).

9. Delaware Court of Chancery, Court of Chancery Guidelines for Preservation of Electronically Stored Information, Jan 18, 2011, http://courts.delaware.gov/forms/download.aspx?id=50988.

10. C.A. No. 184-CC (Del. Ch. June 2, 2009) (Memorandum Opinion).

11. C.A. No. 5258-VCL (Del. Ch. April 8, 2010) (Telephone Conference Transcript).

12. *Chevron v. Salazar*, 11 Civ. 3718 (S.D.N.Y. Aug. 3, 2011) (Memorandum and Order) (citing *Caston v. Hoaglin*, No. 2:08-CV-200, 2009 WL 1687927, at *3 (S.D. Ohio June 12, 2009)); *Export-Import Bank of U.S. v. Asia Pulp & Paper*, 233 F.R.D. 338, 341 (S.D.N.Y. 2005).

13. John Steven & Hilary Kincaid, "Are electronically-delivered board packs a good idea?," *Minter Ellison Corporate HQ Advisory*, Sept. 12, 2011.

14. Christa Bouwman, Overlapping Boards of Directors: Causes and Consequences for Corporate Governance, Financial Contagion: The Viral Threat to the Wealth of Nations, John Wiley & Sons, Feb. 2011.

15. Ian Grant, "Bosses are the biggest threat to corporate data…," *Computer Weekly*, Aug. 10, 2010.

16. Bader & Associates, Great Boards Buyer's Guide to Board Portals, 2009.

17. For example, industry leaders are increasingly providing smart phone and tablet applications that attempt to isolate board communications from other e-mails and the rest of the director's computer. See, e.g., BoardVantage, Security, http://www.boardvantage.com/security (last visited March 26, 2012); The Four Key Requirements of a Board Portal, Boardbooks, available at http://www.boardbooks.com/diligentbooks/board-portal-requirements.shtml.

18. Id.

19. Matt Perkins, "Board Portals: No Assembly Required," *Directorship*, April 22, 2008.