Board Cybersecurity:

Moving from Risky Preferences to Sound Policy

With cybersecurity attacks on the rise and becoming ever more sophisticated, corporate directors must prioritize the security of their communications. Boards should incorporate cybersecurity strategies and regulations into their guidelines, for a complete understanding of what is and is not acceptable to communicate and download, with whom, and most importantly, how. Directors should lead by example and maintain adherence through trainings and audits.

Cybersecurity risk is not a new concept for boards in 2017—neither are the threat of a work smartphone falling into the wrong hands nor the misconceptions that email and in-house data storage are secure, and that password protection equals security.[1]

Headlines continue to reinforce the legal, reputational, and competitive risks of a data breach or leak. In October 2016, a leaked Salesforce board email and presentation shared with the world a list of the company's potential acquisition targets.[2] In March 2017, authorities arrested a Lithuanian man who swindled over $100 million from two U.S. tech companies. His mode of attack: sending electronic communications that looked like messages from a well-known Chinese manufacturer.[3]

Diligent

1 "Cyberthreat and Securing the Board: Three Misconceptions That Undermine Boardroom Security"

2 http://www.businessinsider.com/leaked-salesforce-email-adobe-acquisition-list-2016-10

3 https://www.theguardian.com/technology/2017/mar/22/phishing-scam-us-tech-companies-tricked-100-million-lithuanian-man

Lawmakers and regulators are responding to these intensifying threats. The State of New York, for example, now requires that all financial services firms doing business in the state (and all companies doing business with them) have cybersecurity plans covering everything from audit trails to access to customer data—with board sign-off.[4] And recent lawsuits involving Target and Wyndham Worldwide present failure to put adequate data protection controls in place as a potential breach of directors' fiduciary responsibility.[5]

As a result, directors have been putting enterprise-wide security on their radar. Yet directors' own communications aren't reflecting this growing awareness. According to a 2017 survey conducted by NYSE Governance Services, 92 percent of the more than 380 directors surveyed expressed a preference for personal email. Nearly 60 percent admitted that they regularly send board communications via personal email accounts, including Google, Yahoo, and Hotmail. Heightening security vulnerabilities even more, 22 percent responded that they routinely store board materials on personal or external drives.

Despite recent increases in awareness and education, boards still struggle to keep on top of cybersecurity and risk issues, across the enterprise and in their own activities. In a 2017 survey by Harvard Business School and WomenCorporateDirectors Foundation, only 24 percent of directors responded that they would rate the cybersecurity for their own activities as "above average or excellent."[6]

Where can boards start to narrow the gap? One place is in their bylaws and governance policies.

MAKING SECURE COMMUNICATIONS PART OF BOARD GOVERNANCE

Board policies and bylaws cover a lot—financial behaviors, acceptance of gifts, confidentiality, and disclosures. These policies often include rules for communications, from specifying what can be communicated among directors (e.g., no business solicitations or opinion surveys) to how communications should occur with members of the media and the public.

In today's world of intensifying risk and consequences, cybersecurity needs to be part of these guidelines. The State of New York's regulations recommend that policies cover data access and privacy, identity management, systems and network monitoring, business continuity, and more.[7]

What should you consider for you own policy in your next audit committee, governance, or directors' meeting? Based on our experience with thousands of corporate boards worldwide, Diligent recommends:

RECEIVING AND SENDING MESSAGES

Fellow directors, general counsel, c-suite executives—who should be sending and receiving board communications, and who shouldn't be? Stipulate this in all of the necessary detail in your guidelines, and establish policies for sending and receiving attachments, retaining and archiving messages, and remotely wiping communications from a lost or stolen device. Then support adherence with technology like Diligent Messenger that "closes the loop" against inadvertent mis-sends—e.g., autofilling the wrong email address in an email's recipient field.

Given the rise of phishing emails in cyberattacks, guidelines also need to explicitly prohibit responses from unauthorized parties. Even the most secure board messaging applications may not be 100 percent airtight against increasingly sophisticated hacking techniques.

The Lithuanian hacker who tricked tech companies into sending him $100 million is just one example. Another recent attack strategy gets victims to open an email by hijacking the "send address" of a trusted contact. The recipient is then redirected to a fake (but convincing) gmail log-in screen. Here attackers capture name and password information for access into the recipient's email inbox. [8]

Finally, define what exactly constitutes "official board communications." Some things, like minutes, are more obviously confidential information, but what about meeting invitations and agendas, or one-on-one emails between directors? Make it all clear in your secure communications policy.

HANDLING ATTACHMENTS

When a Boeing employee forwarded a spreadsheet to his spouse for help with formatting issues, he concurrently exposed the names, birth dates and social security numbers of 36,000 employees to security risk.[9]

In addition to establishing dos and don'ts for sending and receiving messages, your communications policy needs to cover the transmission of electronic files. Files related to board activities should never be sent via unsecured/unencrypted methods, and they should be sent only to authorized users. Outline in all necessary detail exactly who these authorized users are.

4 http://fortune.com/2017/03/01/cyber-regulations-new-york

5 https://iapp.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors/

6 https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

7 https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf

8 http://fortune.com/2017/01/18/google-gmail-scam-phishing/

9 http://www.bizjournals.com/seattle/news/2017/02/28/boeing-discloses-36-000-employee-data-breach.html

Your policy should also specify the types of files directors can and cannot download. In today's climate of phishing, malware, and suspect freeware and shareware, "what may appear to be an innocuous download for work purposes can easily introduce a virus to your network and expose sensitive business data," cybersecurity experts at Sentek Global write in *Entrepreneur* magazine.[10] Your internal or vendor cybersecurity team should be able to provide guidance here.

ARCHIVING AND RETAINING COMMUNICATIONS

Saving minutes or an M&A document onto a laptop hard drive or keeping a robust email archive across several years can be time-saving "convenience hacks" for a busy director on the go. Yet this practice opens your board up to significant vulnerability if devices are ever lost or stolen or if an email inbox is ever compromised by malicious parties.

Stipulate in your board policy the types of materials directors are allowed to download, plus the specific smartphones, tablets, computer, and software they can use. With personal devices and inboxes now subject to e-discovery—and a director in danger of personal subpoena if the company goes through litigation—regulations on board communications need to cover all relevant angles. How must these devices be secured? Will directors be required to delete files or historical emails after a certain time period?

This part of your policy should also provide guidance should things go wrong. In the Boeing situation, the company conducted a forensic investigation of both devices to make sure all known copies of the spreadsheet were destroyed, followed up by a notification letter to all affected parties (with an offer of two years of free credit monitoring) and additional employee training on the handling of personal information.

Who should incidents be reported to? By what means should data and devices be "wiped"—and how will you be able to show that these measures were effective?

Your internal or vendor cybersecurity team should be able to guide you on specific technical details, such as secure storage, data encryption, identity authentication, and administrator access control.

ENCOURAGING ADHERENCE

Getting the right rules into place is the first step, and can be accomplished at your next committee or board meeting. Making them work will be an ongoing process afterwards.

To increase your odds of success, have a technology solution ready to go that accommodates your guidelines. Diligent recommends a secure, controlled, closed-loop messaging system that integrates with an existing secure board portal system. Look for data encryption and multifactor authentication (reinforcing passwords with a secondary method for confirming identity) across all devices.

"What directors might sacrifice in convenience by not using personal email they gain in cybersecurity, mitigation of cyber risk, and reduced personal liability," says Dottie Schindlinger, governance technology evangelist at Diligent.

To help directors avoid the temptation of workarounds, make any technology solution you provide simple and stress-free. It should:

- Be intuitive to set up—like downloading an app rather than requiring several unfamiliar steps
- Be easy to use
- Sync across the smartphones, tablets, and laptops directors use to get their information on the go

Whatever solution you choose, regular and correct use will be key to its success. Take the time to educate directors on the new technology through hands-on training. (In NYSE's survey of directors of publicly traded companies, only 9 percent of respondents reported that they were required to take the same cybersecurity training as employees.) Reinforce adoption through periodic refreshers, plus auditing and verification that involves chief executive officers of information security, compliance, and IT.

With spearphishing expected to become more targeted and advanced, data sabotage rising as a threat, and nation-state and internet of things attacks complicating matters overall,[11] cybersecurity continues to ascend as an organizational priority. Meanwhile, the reputational and competitive consequences of not keeping up are getting more serious. According to Matteo Tonello of The Conference Board, deficient risk and control management processes as well as IT security are "increasingly seen as mere symptoms of a 'bad' or 'deficient' risk culture."[12]

Cybersecurity diligence is imperative—and it starts at home. Given the escalating threats and risks in today's business environment and the growing role of boards in cybersecurity oversight, directors can't afford to wait to ensure that their own communications follow cybersecurity best practices. Adding secure messaging to their guidelines and communications policies is one place to start.

10 https://www.entrepreneur.com/article/272847

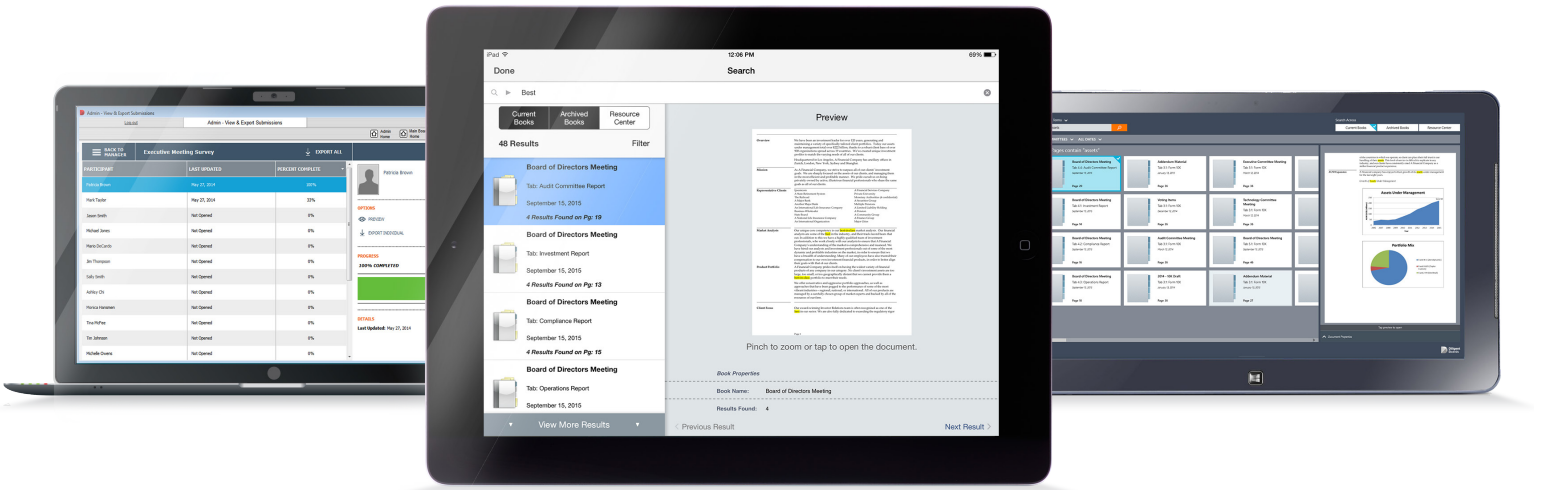
11 http://www.insurancejournal.com/news/international/2017/01/11/438549.htm

12 https://corpgov.law.harvard.edu/2017/02/15/risk-management-and-the-board-of-directors-4/

Diligent

Unleashing the value of information. Securely.

Diligent helps the world's leading organizations unleash the power of information and collaboration—securely—by equipping their boards and management teams to make better decisions. Over 4,700 clients in more than 70 countries rely on Diligent for immediate access to their most time-sensitive and confidential information, along with the tools to review, discuss and collaborate on it with key decision makers. Diligent Boards expedites and simplifies how board materials are produced and delivered via iPad, Windows devices and browsers. At the same time, Diligent Boards delivers practical advantages like cutting production costs, supporting sustainability goals, and saving administrative and IT time for leaders around the world. Join the Leaders. Get Diligent.



Download on the App Store | Get it from Microsoft | GET IT ON Google Play | AICPA SOC | ISO 27001 CERTIFIED BY BRIGHTLINE

For more information or to request a demo, please contact us by:

Tel: +1 877 434 5443
E-mail: info@diligent.com
Visit: diligent.com

WP0029_US