Six Best Practices for Secure Board Communications and Why Email Is Insecure

Diligent

Part of the Diligent Module Series of White Papers

How to better position your board for successful communications and a close look at the benefits of adopting Diligent Messenger

Communication and collaboration are vital in order for boards to succeed. However, there is often a lot of pressure on the company secretary, the general counsel or the main board administrator to manage, secure and govern board communication. Meanwhile, the volume and velocity of digital communication are increasing, and this is burying the board—including directors, general counsels and board administrators—in a deluge of emails.

While digital technology can help facilitate communication between board stakeholders, it also produces challenges. For example, board directors may often sit on multiple boards, which is not inherently a bad thing; the issue is that each board has a different means of communication. Therefore, board directors may have to use a variety of email accounts and, most frequently, unsecure personal email.

How can boards maintain a level of control, visibility and trust over all of these digital communications? How do security, governance, timeliness and accuracy impact board communications? What are some best practices for board communications?

Effective board communication requires vision, strategy and an actionable plan. In this white paper, we will provide insights on best practices for board communications, address the challenges faced and make the case for adopting Diligent Messenger.

Here are the top six best practices for board communications:

1. Secure Your Communications

Board directors and all board stakeholders must stop using email, which can be prone to phishing and malicious attacks, and should instead use a secure communications technology that affords them the ability to communicate with each other when dealing with any matters pertaining to the board. Boards deal with highly sensitive and confidential information, but directors continue to use insecure email to send information back and forth. Not surprisingly, directors are relying on personal and business email accounts to share and collaborate on confidential board materials. It's imperative that boards adopt secure communications technology to keep this information away from hackers.

When considering a communication technology solution provider for your board, it is important to select a technology vendor with the following attributes:

- World-class security technology certificates
- All information contained within a secure environment
- Regular third-party vulnerability testing
- Proven track record

Data breaches and cybersecurity are no longer just the concern of IT and security teams. The board and all members of an organisation must work together to secure the business's most important asset: data. Cybercriminals know the vulnerabilities of insecure email and have been increasing their attacks on boards. The average cost of a data breach was US$3.9 million in 2019, according to the IBM Ponemon Institute Study.

Board members are often well-known individuals and, therefore, are more likely to be targets of hacking than the average person. High-profile victims of email hacks include Australian politicians, police and judges as well as former U.S. Secretary of State Colin Powell. Powell, who sits on the board of Salesforce.com, was hacked, and sensitive emails discussing regulatory concerns of increased trading activity in advance of Salesforce's acquisition of Demandware were made public. Overall, if a board is using a board portal and not pairing that with a secure communication solution, they are putting their whole organisation at risk.

2. Minimise Opportunities for Communications Errors

Security is not just about protection from hacking and external threats, but also protection from insider threats. However, not all insider threats are malicious; in fact, some threats are caused by human error, including:

- Sending an email to the wrong address
- Mistakenly replying to all individuals on emails instead of just replying to the sender
- Accidentally replying to group distribution lists
- Forwarding (intentionally or accidentally) of information to unauthorised recipients

3. Value Timing

Effective decision-making by the board is based on "real-time" information. Board directors need to be informed of the most up-to-date information—whether they need to review the board pack, review other recently submitted materials before a board meeting or respond to a questionnaire. Emphasis should be placed on the most beneficial time to send board information to value the time of the other board directors.

Moving from paper-based board packs to digital board portals is a step in the right direction. However, not all board portal solutions are the same. When selecting a solution, be sure to ask the board portal vendor:

- How are real-time updates communicated to users?
- Does the solution have the ability to send real-time notifications?
- Can notifications be escalated to other means if directors are nonresponsive?
- Can users (board directors) comment on new resolutions in real time?

4. Standardise and Centralise all Communications to the Board

The company secretary should be the gatekeeper of all information shared with the board. Various digital communications, such as email and text messaging, and the increasing velocity and volume of these communications, create growing challenges for the corporate secretary, who needs to control what's being shared.

Challenges faced include:

- Is this the same information shared with all directors?
- What are the relevancy, accuracy and timeliness of this information?
- If a legal discovery process occurs, how can communications be identified and reviewed?

Board stakeholders should submit all board information via the office of the company secretary. As the main custodian of all board information, the company secretary relies on higher levels of control and visibility. If all of the board information goes directly through the company secretary, that person can take steps to secure it.

5. Consider the Most Appropriate Means of Communication

How do your board directors want to be contacted? Is their preferred method safe and secure, or does it create risk? How often do they want to be communicated with? Do they prefer one method of contact versus another?

Digital communications seem more advantageous than paper-based communications. However, not all digital communication technology is secure. Mobile devices, for example, may provide accessibility and convenience, but there are inherent risks of emailing/texting board information.

Steer your board directors away from using personal email and texting on their mobile devices when communicating with the board. Even within a single board, information must be compartmentalised within various committees because not all directors should be privy to all information. Communications solutions should be capable of compartmentalising as needed to maintain privacy within specific committees, and be flexible enough to allow all-board communications as well. Consider adopting secure communications technology to mitigate any risks.

6. Ensure Proper Records Management and Documentation

Develop a sound records management and documentation policy and determine who is the main person or team

responsible for retaining information. Most likely, it will be the office of the company secretary. Information retention is essential for archiving information for legal and governance purposes.

Create a document-retention policy, and make sure that all stakeholders are educated on the best practices for saving messaging and submitting the information to the individual/team in charge of information retention. To assist in proper records management and documentation, consider a board governance management technology provider that can empower your board with the ideal tools and solutions.

Retention is only half of the story. The policy and records management systems of boards must also be designed to comply with all laws and regulations, but also to protect the company and directors within said laws and regulations. Part of that protection is an automated means for communication retention and deletion of those communications on a standard, predictable cadence. If, however, directors are using third-party corporate email, communications sent to those accounts may not be privileged because these emails are on a third-party email server where individuals (e.g., IT departments, other executives) may have access to it.

Cybercriminals know the vulnerabilities of insecure email and have been increasing their attacks on boards. The average cost of a data breach was US$3.9 million in 2019, according to the IBM Ponemon Institute Study.

Reasons to Adopt Diligent Messenger

Diligent Messenger, which integrates seamlessly with Diligent Boards™, delivers the ideal solution to meet all of these best practices for board communications. If you made the switch from paper-based board packs to a digital board portal, you've taken a step in the right direction. However, trying to use different board technology point solutions may create more obstacles. Organisations already deploying Diligent Boards™ are well positioned with an innovative and intuitive board governance management platform that functions perfectly in conjunction with Diligent Messenger.

Here's how and why:

Diligent Messenger Delivers Rock-solid Security

To secure your board communications, choose Diligent Messenger, which is built on the same security standards as Diligent Boards™. Diligent Messenger is a closed environment that includes only authorised and approved users; all information is contained within Diligent's security perimeter.

As discussed, you want to move your board directors away from email (whether personal, third-party or corporate) and text, which create myriad vulnerability risks. Diligent Messenger's user interface is familiar, powerful and easy to adopt, and rivals the functionality of email—but without all of the inherent vulnerabilities and risks.

Key Diligent Messenger security attributes include:

- SSAE 16/ISAE 3402 (SOC 1 Type 2) service organisation annual audit of controls
- Type 2 SOC 2 Security and Availability audit
- HIPAA AT 101 audit
- ISO 27001 certified
- Third-party vulnerability scanning and penetration testing
- Diligent employee training in data security requirements

What happens when a board stakeholder's device goes missing? The Diligent Messenger user's account can be instantly disabled, which can help mitigate the risk of data breaches.

Note: We do not remotely wipe data.

Advanced Functionality

Because Diligent Messenger seamlessly integrates with Diligent Boards™, users can make an easy transition. Diligent Messenger is a multiplatform solution that works on computers and mobile devices, and that can help eliminate the clutter, vulnerabilities and other challenges associated with email.

Functionality features include:

- Split-screen view capability of Diligent Boards™ and Diligent Messenger
- Identical log-in process, using the same credentials as Diligent Boards
- Instant connection to other stakeholders while reviewing board materials
- Capability for group messaging and attachment sends
- Document sharing (e.g., PDFs, videos, photos)
- Capability to comment on new resolutions in real time

Your board directors need to have "real-time" information in order to make timely and critical decisions. Diligent Messenger's notification feature allows you to escalate time-sensitive information to board directors. Through Diligent Messenger, you can send discreet notifications to the board director to alert them to log into Diligent Messenger to retrieve the information. The notification, however, is just an alert, and will not contain any sensitive data due to the vulnerability of email.

Greater Control and Visibility

Board portals today need to be more than just a digital repository for board information. Diligent is helping to redefine the technology as Enterprise Governance Management software platforms for organisations. Diligent Messenger helps augment governance and accountability while enhancing communication and collaboration among the board.

As discussed in the "Best Practices" section, boards need to ensure proper records management and documentation. Diligent Messenger helps your board to stay compliant with an organisation's document retention policy. Depending on your organisation's retention rules, Diligent enables settings to automatically retain or delete messages. When directors use text and email (corporate or personal), it becomes a liability issue for a board's general counsel and board administrator. Diligent Messenger provides control where it is needed.

Conclusion

With Diligent Messenger, Diligent delivers an advanced, but intuitive, solution to meet all of these best practices for board communications. We also offer robust training options, from in-person to self-service, with award-winning, white-glove customer service that is available 24/7/365. As new technology emerges, there are often unforeseen challenges as well as unforeseen advantages. Because Diligent listens to our customers, we're committed to leveraging innovative technology. Diligent's commitment to innovation puts you in control of an environment that improves efficiency, collaboration, communication, security and board governance.

Diligent

Diligent helps the world's leading organisations unleash the power of information and collaboration—securely—by equipping their boards and management teams to make better decisions. Our flagship product, Diligent Boards™, is the most widely used board portal in the world, relied on by more than 650,000 board directors in 16,000 organisations in more than 90 countries. Diligent Boards expedites and simplifies how board materials are produced and delivered via iPad, Windows devices and internet browsers.

Join the Leaders, Get Diligent.

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

Australia: 1800 646 207
New Zealand: 0800 434 5443
Singapore: +65 6932 2638
E-mail: info@diligent.com
Website: diligent.com/au