Diligent

Are We Safe?

5 Questions to Ask About Your Board & Executive Communications

Protecting board and executive communication requires a different level of security. Board members and management team members are among the most attractive targets for hackers and other bad actors, given the sensitive information they possess. According to a recent Forrester/Diligent survey, over 50% of directors and C-suite executives regularly use personal email to communicate about their organization's most sensitive topics, putting their companies' information at significant risk.

A secure communication solution allows you to maintain control over confidential communications, distribute documents and files for faster and easier collaboration, and ensure a rapid response during crises. But not all solutions are created equal. Look for the following when evaluating options in the marketplace:

1. Is Communication Encrypted?

Encryption translates "plain text" data into a cryptographic key, a string of characters to protect information in transit. Encryption is the most effective way to achieve data security and an essential part of any communication solution. Why? Because sensitive data in transit is increasingly more vulnerable to phishing attacks, password hacks, and other potential breaches.

Your communication solution should protect messages and attachments with state-of-the-art security infrastructure and encryption. ISO 27001 certification is the gold standard for information security.

Other features to look for: the ability to retract messages and "view-only" attachments. The latter prevents attachments from being downloaded, saved, exported, captured via screenshot, copied, or forwarded to other users.

Diligent

2. Are Platforms Integrated?

When sensitive information "lives" in different places—including emails, director devices, and disparate systems—security problems increase. Boards and executive teams can gain significant benefits from a communications solution that offers messaging, chat, collaboration, data storage, and more from a single network of connected platforms.

Organizations should consider solutions that connect their secure messaging platform to file-sharing systems, board management software, and so on. It's important that a solution provides a central workstream for company leaders and pulls all sensitive updates, conversations, and documents out of unsecure channels like email.

3. Is the Solution Easy to Use/Adopt?

Nearly half (49%) of Diligent's survey respondents reported that securing documents or board materials is "challenging" or "very challenging."

To ensure director adoption—and data security—make sure your communication solution:

- ☐ Mirrors the functionality and design of everyday tools and systems (e.g., email, text)
- ☐ Enables real-time updates and notifications
- ☐ Supports all types of communication across groups (e.g., peer to peer, committees, full board or executive team)

4. Does It Minimize Weak Links?

Nearly one third (29%) of the board members Diligent surveyed said they lost or misplaced a device over the past year. Moreover, 21% said that someone on their board had their identity stolen and used to access sensitive materials.

It only takes one incident to cause irreparable harm and financial damage. Make sure your communication solution:

- ☐ Gives administrators the ability to remotely "wipe" lost or potentially compromised devices
- ☐ Is supported by training on product use and cyber hygiene

Diligent

5. Does It Meet the Standards of Your Security Team?

Actively engaging your IT team in the selection process benefits everyone in terms of protecting sensitive data—and safeguards your organization against unnecessary liability.

Specific to a secure communication solution, CIOs and CISOs will ask about:

- **Access and authorization:** What kind of control will administrators have over access rights and locations—for instance, can they restrict or disable user access or prevent access from unknown, untrusted devices?
- **Discoverability:** How will messages be retained and deleted? Is there an ability to report on messages sent within a specific date range?
- **Redundancy:** Is data backed up across remote, geographically dispersed locations? Does the provider offer real-time, 24/7 intelligence on data performance?
- **Customization:** Can the solution be tailored to the board's needs—for example, in areas such as password strength and lockout policies?

CIOs and CISOs also need to know if the solution's provider:

- Invests in cybersecurity research and development
- Is transparent about security processes, such as system monitoring, breaches and resolution, protection of servers and routers, and screening for new hires
- Regularly conducts penetration testing to keep up with evolving threats
- Provides training and customer support—for example, helping a director who's locked out of the system because of repeatedly mistyping a password

Diligent Secure Collaboration Tools, Defined:

- **Diligent Boards:** Provides a secure and central location for board books and sensitive meeting materials, along with the tools to review, discuss and collaborate. Voting and questionnaires can also be completed through this app.
- **Diligent Messenger:** A secure, encrypted messaging platform (accessible on phone, iPad or desktop) that resembles both SMS texting and email. Allows boards and senior leadership teams to securely communicate in groups or one-on-one. Integrates with Diligent Boards.
- **Secure File Sharing:** A virtual data room that integrates with Diligent Boards. Ideal for M&A, crisis communication, or sharing sensitive documents with permissioned third parties (e.g., auditors, consultants).
- **Secure Meeting Workflow:** A workflow tool that allows permissioned users to collaborate on documents and presentations collectively within a secure, encrypted environment.

Diligent

About Diligent

Diligent is the pioneer in modern governance. Our trusted, cloud-based applications streamline the day-to-day work of board management and committees, support secure collaboration, manage subsidiary and entity data, and deliver insights that empower company leaders to make better decisions in today's complex landscape. With the largest global network of corporate directors and executives, Diligent is relied on by more than 16,000 organisations and 650,000 leaders in over 90 countries. With award-winning customer service across the globe, Diligent serves more than 50% of the Fortune 1000, 70% of the FTSE 100, and 65% of the ASX.

Learn more about Diligent's Secure Collaboration Tools:

Diligent's Secure Collaboration Solution provides boards and executives with secure alternatives to email and the ability to collaborate on highly sensitive documents and workflows.

Ready to see these tools in action?

REQUEST A DEMO