# Secure Board & Executive Communications Software Buyer's Guide

Diligent

## Secure Director and Executive Communications for Modern Governance

Electronic communications between corporate directors and senior executives is an integral part of how business is conducted. The expectation is that when an executive or director has something sensitive to discuss, they will pick up the phone. The reality, though, is that they will usually opt for the easier and more convenient email or electronic message. For a lot of these organizations, however, these communications are not secure or well managed. Providing a communications solution that is "automatically" more secure is essential. A key reason for this demand is that human error is often the starting point for data breaches and unintended disclosure of sensitive information.

Organizations are responsible for providing a secure communications environment for directors and officers that substantially reduces vulnerabilities from human error. It is time to change the status quo of using unsecured or personal communication tools. If this challenge is ignored, it leaves an attractive "hole in the fence" for those looking to steal sensitive information. This creates roadblocks for your organization to meet the challenges of modern governance. Modern governance is the practice of empowering leaders with technology, insights and processes to fuel the good governance that organizations require to thrive and endure.

The communications component of modern governance is often overlooked. Rather than deploying an email and messaging solution specifically designed to support modern governance through enhanced security and collaboration capabilities, organizations rely on a mix of public apps or standard email services that cannot meet the recommended standards for today's directors and senior executives.

Modern governance, in addition to many legal, compliance and regulatory regimes, demands comprehensive security for messaging and email services used by directors and senior executives. Attackers know that directors and executive communications have the information that can provide the greatest financial gain.

According to the 2019 Verizon Data Breach Report, high-level executives are six times more likely to be the focus of an attack. The same source tells us that 94% of attacks are email based. Email credential theft is common, and rogue employees, including IT administrators, are always a risk. The Verizon report indicates that insider attacks account for as much as a third of all data breaches.

Corporate email systems, such as Outlook, are not secure enough to provide protection for the sensitive communications of directors and senior executives. For example, during deal-making, directors and executives need an easy way to collaborate. If a counteroffer needs to be made urgently, companies are unlikely to trust communicating this over corporate email systems. Besides the risk of zero-day vulnerabilities — an opening that is discovered by attackers prior to a security patch being available —any user that does not keep up to date on patches or updates can be at risk.

Another problem may be inconsistent and spotty retention policies for board communications. The use of corporate email can also create problems when there is litigation against another company on whose board the director serves, and that director's email becomes discoverable. When this occurs, it may open up your sensitive board communications to the discovery process. And in some cloud-based deployments, an accidental deletion is forever. The inability to restrict email or file forwarding and attachments can also result in embarrassing disclosures.

Public email services such as Gmail are an even less secure alternative. Many of the same issues that impact a corporate email service exist in public systems, but there is almost no ability for the organization to control public email accounts. Files or data sent to them must be considered gone forever. And security is completely up to the individual. One common vulnerability is saved passwords in a browser, allowing anyone with access to that device to view, forward or steal any emails in that account. Data encryption is also rarely used, leaving messages vulnerable.

The public messaging systems aren't much better. Numerous known vulnerabilities have affected messaging or chat services. A good example is the recent issues with WhatsApp. This makes it even more important to find solutions that have been proved secure and compliant. When it comes to the communications systems used by directors and senior executives, reducing the attack surface by eliminating communications tools with known vulnerabilities is a big step forward.

## A Buyer's Guide for Evaluating Director and Executive Communications Services

Once an organization understands that a secure and comprehensive messaging system that supports modern governance is essential, finding the right solution that meets the challenge becomes a critical process. What follows is a detailed list of the features and capabilities organizations must demand in a secure communications solution. The questions to ask focus on three primary aspects of an optimal solution: governance, security and ease of use.

**Governance: How Secure Communication Improves**

A best-in-class solution for sensitive communications for the board and executives must be able to meet key compliance and legal requirements. This presents several questions:

- **Are all types of board or sensitive communications (texts, messages and emails) contained in one system?**
- **Does all information, including files and attachments, stay within the system, to prevent leakage?**
- **Does the vendor have internal staff with governance and compliance expertise?**
- **Does the service meet discovery and legal hold demands?**
- **Does the vendor's customer support team understand compliance and governance issues?**
- **Does the solution allow for the quick wiping or disabling of lost or stolen devices?**
- **Does the system ensure transparent board/executive communications?**
- **Does the vendor have a strong reputation for compliant solutions?**
- **Does the system support proper records management?**

## A Buyer's Guide for Evaluating Director and Executive Communications Services

- **Support for multiple communication modes:** Governance and compliance is often about control, and if directors and executives are using many different tools for email and messaging, control is lost. The best solution provides one tool for both email and messaging.
- **Preventing data leaks:** A great deal of sensitive information can be found in files and attachments, not just the email or message. Diligent Messenger protects the message and ensures that attachments and files cannot leave the secure system.
- **Vendor staff with governance expertise:** Many mail and communications systems are for general use, and the vendor staff have no governance expertise. This stands in sharp contrast to Diligent Messenger, a tool supported by staff who have deep and meaningful governance expertise.
- **Compliance with legal hold/discovery requirements:** Corporate and public email systems typically fail this test. Corporate systems tend to have generic retention periods and little support for discovery. Public services have almost no controls. And when an email is accidentally deleted, it's often gone forever.
- **Customer support teams that understand compliance/governance issues:** Support requests are a common and normal occurrence. With a system for board and sensitive communications, many support queries are really seeking assurance that the communications system meets strict governance regimes. The support teams for your communications service must speak this language, and at Diligent, they do.
- **Documented management of lost/stolen devices:** Compliance regimes have strict rules on how to handle a key person losing a device—or having it stolen. Many require that the device be wiped or otherwise disabled. Without this, running afoul of regulations is almost a certainty.
- **Ensured communications transparency:** A key demand of many legal, compliance and governance regimes is transparency. Too often, transparency is lost not by design, but by the complexities of using many different communications products. Using one communications solution simplifies ensuring transparency.
- **A reputation for delivering compliance:** Providing solutions that support modern governance is not a design goal of every vendor. Diligent Messenger has a reputation for meeting the latest governance demands.
- **Support for proper records management:** Using a purpose-designed communications solution makes proper records management much simpler for the organization. It is no longer necessary to try to link multiple systems or set up records management in software that doesn't have the right functionality.

## Security: Understanding the Security Behind Secure Communications

Cybersecurity has become one of the most important priorities in any organization. Successful cyberattacks damage an organization's reputation, cause financial harm and can result in huge penalties. Sensitive communications involving directors and senior executives are a particularly attractive target. The key security-focused questions to ask include:

- **Are all messages/communications encrypted?**
- **Does the vendor staff undergo rigorous security training?**
- **Is there support for both secure messaging and email?**
- **Does the vendor document that its operations employ the latest security technologies?**
- **Can customer support answer security questions?**
- **Does the vendor undergo and pass audits?**
- **Does the vendor have a strong track record of delivering secure messaging solutions?**
- **Does the solution protect file attachments and limit cut/paste functionality?**
- **Is it a closed communications platform that is not publicly accessible?**
- **Does the vendor use vulnerability and penetration testing on its own product?**

## The Answers to Key Security Questions That an Ideal Board/Executive Communications System Should Provide:

- **Encrypted communications:** Encrypting email, messages and other sensitive communications is the first and most basic step to securing them. Many messaging systems can turn on encryption, but default encryption provides a foundation for secure communications. The default for Diligent Messenger is to encrypt all communications.
- **A vendor staff trained in security:** Delivering secure products is the job of every Diligent Messenger employee. Your vendor must invest the time and resources to ensure that its development and customer-facing employees have security expertise.
- **Support for secure messaging and email:** One platform for all communications makes it far easier to deploy strong and consistent security. Attackers will seek out the one weak app when many different communications products are used, making breaches much more likely.

- **Vendor commitment to secure operations and use of the latest security technologies:** A vendor that is committed to security will utilize the latest security technologies in its own operations. The vendor should be able to easily document its use of the most effective security tools and technologies.
- **Customer support security expertise:** Deploying and using a secure communications platform will inevitably result in support instances focused on security. If the support team members are not well trained and knowledgeable about cybersecurity issues, they cannot provide adequate support. Diligent's support team is continually trained on cybersecurity issues.
- **Security audits with positive results:** A vendor should be able to provide specific details on what security audits or tests it has passed. Diligent is proud to detail the number of security and compliance audits that it has passed, including SOC2, HIPAA AT101, SSAE 16/ISAE 3402 and ISO 27001.
- **A vendor track record of delivering secure solutions:** Another important question for the vendor is about its track record of delivering secure communications for directors and executives. Unfortunately, a simple Google search will show that many communications products have had numerous past problems.
- **Attachment and cut/paste control:** The most common ways that data is lost are poor security for file attachments in emails and a lack of control over information that can be cut and pasted. This must also include management of "screen shots" that may result in untracked copies of sensitive information. Diligent Messenger provides a comprehensive solution for restricting file attachments and limiting cut-and-paste capability.
- **No public access to the communications platform:** Many email and messaging apps are open to anyone. Attackers can simply sign up for an account and gain access. This makes attacks easier. Diligent Messenger is a closed and self-contained messaging service that does not allow for public access.
- **Vulnerability and penetration testing on the vendor service:** Confirming that a secure communications service is truly secure requires the vendor to complete both vulnerability analysis and penetration testing to be certain that there are no places that attackers could exploit to gain access to sensitive information.

## Ease of Use: How Easy Is the Tool to Adapt?

Choosing a secure communications platform that meets all governance and security demands isn't enough. The solution must also be engaging for users. If the communications solution is hard to use and so complex that it requires a lot of training, the directors and executives will just ignore it. Asking these critical questions about usability is necessary:

- **Is there one easy-to-use environment for both email and messaging?**
- **Is there outstanding tech support for directors and business executives?**
- **Does it have split-screen views for enhanced usability?**
- **Does the vendor have a reputation for usability?**
- **Can the solution provide instant connection to other team members?**
- **Is there version control to ensure that everyone has the same files or documents?**
- **Does the system use automation to simplify legal hold/ discovery management?**
- **Can a user recall messages or emails sent by mistake?**

## The Answers to Key Security Questions That an Ideal Board/Executive Communications System Should Provide:

- **One environment for mail and messaging:** For maximum usability, you want a single environment for all communications. For ease of use, access from any device is critical. Having a single solution in place will drive consistent usage, fostering rapid learning and effective use. This benefit is common for users of Diligent Messenger.
- **Outstanding user support:** It is essential that the vendor have a strong reputation for user support services. For example, Diligent has many customer references and case studies showcasing its outstanding support services. The support team provides the right answer the first time and interacts with executives in an appropriate manner.
- **Split-screen views:** The ability to have both files and information visible while communicating enables better collaboration. In addition, the ability to review key information while chatting or communicating in real time enhances productivity.
- **A vendor reputation for usability:** The vendor must be able to show both internal and external testaments to the usability of the communications platform. The directors and senior executives have unique usability needs that the solution must address.
- **Instant connection to team members:** The speed of business has increased dramatically, and in many scenarios, directors and senior executives will demand real-time communication. Many email and messaging systems can't provide this. However, Diligent Messenger is lauded for instant communications.
- **Version control for consistent information:** Information and data can change constantly. Providing directors and executives with a communications platform that ensures that everyone has the same and most up-to-date information is a critical feature. The platform should not force users to search archives.
- **Automation of legal hold and discovery:** Removing the onus of maintaining the legal hold or discovery status of every message or email is critical to ease of use. In addition, automation ensures consistent application of policies. This is a highly valued feature of Diligent Messenger.
- **Message and email recall:** The ability to recall a message or email is an essential feature for directors and senior executives, since incorrect or outdated messages can become a problem. They also waste valuable executive and director time.

## Diligent Messenger Delivers Secure, Easy-to-Use Communications That Support Modern Governance

Enhanced communications for the top tier of management are critical to organizational success. Diligent Messenger provides the comprehensive, secure and easy-to-use solution that enables boards and executives to collaborate much more effectively. This product enables the team to share intellectual property, access confidential files and share perspectives without limits or concerns about message interception. Encryption and security allow directors to work beyond the firewall without worry. With both messaging and email in the same platform, directors and executives can communicate in whatever mode they prefer.

Diligent Messenger is closely aligned with modern governance initiatives. It empowers directors and executives with the right technology platform for critical communications that enables more effective interaction while meeting governance and security demands. Diligent Messenger provides functionality beyond what public/private email systems and messaging apps can deliver. Messenger is also integrated with Diligent Boards, the leading modern-governance technology solution for supporting boards of directors. This combination of features and capabilities makes Diligent Messenger the optimal communications platform for modern governance. As an integrated component of Diligent's Governance Cloud, Messenger is a synergistic component of a comprehensive platform.

Diligent Messenger's solution simplifies meeting compliance and governance requirements. Among the most important, and most common, compliance demands are for a single, secure environment for board and executive communications that ensures that confidential information remains confidential. Support for complete transparency is also provided. The ability to recall emails and wipe devices that are either lost or stolen supports key governance and compliance provisions.

Diligent Messenger is also a highly secure solution that protects sensitive communications. It is ISO 27001-certified, the gold standard for information security. It has iOS and Android device authorization, with multiple levels of security. This non-public solution keeps your communications under your control. Full encryption ensures that attackers cannot view any intercepted information. There is also full file attachment and cut/paste control, along with the ability to retract messages, to prevent information leakage.

Ensuring that there is a very high level of usability is a key design goal for Diligent Messenger. It provides a comprehensive, yet uncluttered, communications platform specifically for board activities. Push notification ensures that directors and executives are instantly aware of any new messages. And with split-screen view, directors can interact while reviewing the latest information. Directors can also focus on key tasks, since Diligent Messenger automates many housekeeping chores such as setting legal hold/retention. To ensure that directors and executives get the most from Messenger, each customer has dedicated "Customer Success Managers" who offer training, tutorials and 24/7 support.

### Common Use Cases for Diligent Messenger

The ability to communicate with full security among select groups is not limited to the directors and executive management. Diligent Messenger's functionality also supports other use cases. These are some of the other common business scenarios where Diligent Messenger delivers an ideal solution:

- **Executive management teams or working groups:** Developing a new or modified corporate strategy and preparing a product launch are among the business functions that require a more secure and comprehensive communications solution that doesn't have the vulnerabilities or lack of control common in corporate email or smartphone text messaging systems.
- **M&A project teams:** Secure communications for an M&A team is critical. Leaked information is more than an inconvenience, since accidental disclosure of M&A plans can result in fines or SEC actions. Using Diligent Messenger as the communications platform for an M&A project solves many of the communication problems that can throw a project like this off the rails.
- **Strategic product development teams:** In many organizations, product roadmaps and development plans are highly valued intellectual property. It is essential to ensure that any communications about these plans, including the attachment of files associated with them, are done in the most secure manner possible.
- **Internal legal issues:** In today's highly litigious environment, lawsuits and legal actions are common. The ability to control and secure any communications about these and prevent disclosures is mandatory. Using a truly secure communications platform, rather than common email or text messaging tools, helps prevent accidental revelation of sensitive information.

## Key Takeaways

Digital businesses rely on digital communications. And while many of the email and messaging systems that are in common use are enough for common business processes, they just don't provide the security, compliance and usability necessary for scenarios that have more stringent demands, such as board-level communications. The vulnerabilities, lack of control and potential legal governance issues that can arise with the use of public or corporate email and uncontrolled messaging systems are just too risky.

For these reasons, many organizations are deploying Diligent Messenger, a solution designed to meet the demands of board-level communications or other scenarios that involve sensitive information. Before committing to any solution, an organization must require answers to the key questions listed in this Buyer's Guide. Diligent Messenger is designed from the outset to meet the need for a secure, compliant and usable communications solution for the board and sensitive projects, as part of an overall focus on modern governance.

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, please go to:**

**Email: info@diligent.com**
**Call: +1 877 434 5443**
**Visit: diligent.com**