Diligent

THE FUNDAMENTALS OF SECURE GOVERNANCE COMMUNICATION

Boards need to be ready for anything at a moment's notice. But being agile and quickly shifting focus as new challenges emerge frequently creates the opening bad actors need to gain access to sensitive materials. A large-scale data breach threatens every aspect of an organization's success: its valuation, its profitability, its brand and its reputation. Despite heightened awareness of data security, data breaches are increasingly the result of internal human error.

According to a recent study from Proofpoint and the Ponemon Institute, insider threat incidents rose 44% between 2020 and 2022. Meanwhile, costs per incident are up by more than a third to $4.35 million with the time required to contain an incident increasing from 77 to 85 days.

To effectively navigate this threat landscape, corporate boards and c-suites need to get ahead of insider risk proactively. That means building up controls to prevent unforced errors and ensure the protection of sensitive data and communications at all times.

A Virtual World's Very Real Risks for Executives

Executives now share in an environment where everyone plays a role in data protection. Even as executive teams manage cyber risk across the organization, their own communication channels and operational infrastructures too often remain exposed.

On a daily basis, management teams deal with data, conversations and documents that require various levels of confidentiality ranging from sensitive to highly classified. Yet, the tools they leverage – email, company servers, text messages – are no more secure than the tools in use by every other company employee.

This discrepancy between classified information and insecure tools is even more dangerous in a virtual world. What an executive team doesn't know about its seemingly secure systems and workflows can mean the difference between transformational growth and becoming the latest cautionary tale.

Increasing Regulatory Oversight

Regulators are increasing scrutiny of businesses that don't protect customer and partner data has resulted in fines that compound reputational damage.

- Between January 2021 and January 2022, E.U. data protection authorities handed out $1.2B in GDPR fines, which represents a sevenfold increase from the prior year.
- In May of 2022, the Securities and Exchange Commission proposed a rule "to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies… The proposed amendments would require… current reporting about material cybersecurity incidents and periodic reporting to provide updates about previously reported cybersecurity incidents. The proposal also would require periodic reporting about a registrant's policies and procedures to identify and manage cybersecurity risks; the registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures. The proposal further would require annual reporting or certain proxy disclosure about the board of directors' cybersecurity expertise, if any.

[1] Imaginetime, "The Biggest US Data Breach Penalties of 2019," September 10, 2019. https://www.imaginetime.com/blog/the-biggest-us-data-breach-fines-penalties-and-settlements-of-2019/

[2] Thomson Reuters, "Who is liable when a data breach occurs?"https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability

Understanding the Insider Threat

Despite elevated levels of external risk, a company's greatest or most immediate cyber threat is often internal. Whether through malevolent acts or privilege misuse, company employees are involved in nearly every major data breach.

The insider's role in a breach is not always malicious; in fact, 84% of data breaches involve human actions that are either unintentional or inadvertent[3]. Yet, that doesn't make the internal threat any less dangerous.

To combat internal cyber risks, executive teams can prioritize a few key actions: The first is training employees regularly on how to identify threats and practice safe communication. Second, executive teams must take a closer look at the tools and channels that support their most sensitive information flows — particularly those used by the C-suite, their direct reports and other departments (legal, finance, etc.) that handle classified information.

C-Suite Cautionary Tales

Impersonating senior executives is a favorite approach for cybercriminals. Executives can authorize large transactions, and subordinates may be reluctant to question their requests. These costly breaches demonstrate the damage of unsecure workflows:

- In 2014, American commodities trader Scoular was defrauded of $17.2 million when an executive wired the money to a bank in China after emails purporting to be from the CEO and the firm's external auditor instructed him to do so.[4]
- In 2016, one of Mattel's finance executives seemingly received a request from the CEO to pay a new vendor in China. She made the requested transfer of $3 million to a Chinese bank.[5] They recovered their money only through fortuitous timing.[6]
- In 2019, the CEO of a UK-based energy firm transferred £201,000 in response to instructions given by telephone in the voice of his superior – but that voice was generated via artificial intelligence.[7]

By the Numbers: Data Breaches & the C-Suite

- Executives are less likely to follow the security policies that organizations have in place.[8]
- More than 99% of threats required some human interaction – to follow a link, open a file or document, or enable a macro – demonstrating the importance of social engineering behind such breaches.[9]
- C-level executives are 12 times more likely than other employees to be targeted by social engineering attacks.[10]
- A 2013 study showed 90% of senior managers had uploaded business files to personal email or cloud accounts. Nearly 60% had sent sensitive information to the wrong person.[11]
- The average cost to the enterprise for a data breach is $15.38 million.[12]
- The annual cost of cybercrime and economic espionage around the world may be as much as $445 billion, almost 1% of global income.[13]

[3] https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/
[4] https://omaha.com/money/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html
[5] http://https/www.cbsnews.com/news/mattel-vs-chinese-cyberthieves-its-no-game/
[6] https://www.csoonline.com/article/3049392/chinese-scammers-take-mattel-to-the-bank-phishing-them-for-3-million.html
[7] https://gdpr.report/news/2019/09/02/privacy-fraudsters-scam-energy-firm-using-ai-voice-manipulation/
[8] https://www.cio.com/article/3247428/safeguarding-your-biggest-cybersecurity-target-executives.html
[9] https://www.helpnetsecurity.com/2019/09/10/cyberattacks-human-interaction/
[10] https://www.verizon.com/about/news/verizon-2019-data-breach-investigations
[11] https://www.csoonline.com/article/2134263/senior-managers-fumble-security-much-more-often-than-rank-and-file.html
[12] https://www.ibm.com/security/data-breach
[13] https://www.csoonline.com/article/3040982/data-breaches-often-result-in-ceo-firing.html

The Risks Lurking in Legacy Platforms

Corporate email: Email is still the lifeblood of organizational communication, but it's no place for confidential C-suite discussion or sensitive documents. Easily hacked by outsiders, and accessible by IT teams and administrators, "private" email communication among company leadership is never private. Broader IT teams retain administrative access. Misfired emails or unintended recipients are a regular occurrence. Plus, phishing remains the most effective tactic for accessing sensitive information, affecting employees at every level of the organization. Executives and the teams that directly report to them must have a more secure alternative when confidential information is involved.

Videoconferencing platforms: The recent shift to virtual working has accelerated the adoption of videoconferencing for remotely conducted meetings. Like email, however, these systems, such as Zoom and WebEx, are often easily hacked despite seemingly robust security features. In fact, Zoom users endured a bug that opened webcams to spying, and the company struggled to marry its claim of end-to-end encryption to its actual capabilities.[14] Company leaders can take simple steps to make their sensitive meetings more secure. These include removing meeting links from email calendars and sending videoconferencing links through encrypted channels instead.

General-purpose collaboration tools: The tools that executives and their teams use daily for rapid communication, easy file sharing and productive collaboration – tools like Box, Google Drive and Slack, to name a few – are often as unsecure as email and videoconferencing platforms. In a recent example, Slack inadvertently exposed users to a vulnerability that enabled automated collection of "massive amounts" of session data.[15-16]More secure alternatives, however, are only as secure as they are convenient — meaning if they fail to mirror the way leadership teams work, they fail to solve the problem. The good news is that a suite of better tools does exist, and those solutions are covered in this white paper (p. 11).

C-Suite Communications, Workflows and Processes Requiring Greater Security Than Legacy Tools Provide

- Compensation and performance data
- Strategic growth and M&A plans
- Unaudited financials
- Human capital planning
- Budgeting
- Strategic planning sessions
- Communications that need to remain undiscoverable

[14] https://www.zdnet.com/article/make-sure-your-zoom-meetings-are-safe-by-doing-these-10-things/
[15] https://www.zdnet.com/article/slack-vulnerability-allowed-session-hijacking-account-takeovers/
[16] https://securityaffairs.co/wordpress/99626/hacking/slack-bugs-account-takeover.html

Privilege Misuse: An Unnecessary Evil

One overlooked vulnerability of many collaboration tools and platforms is the way they are implemented and managed throughout the organization. In most companies, the IT department or its equivalent has privileged, unlimited (or largely unlimited) administrative access to those platforms. So, too, do other privileged employees for reasons related to their job functions: payroll, tax, accounting, recruitment and so on.

When other users and departments outside of the C-suite have the ability to intercept, monitor or otherwise access and view sensitive data and communications, the risk of an insider-caused breach increases exponentially. Inadvertent mistakes in data handling, as well as malicious acts by disgruntled current and former employees, expose organizations to unnecessary risks.

63% of employees report taking company data with them after leaving a job, opening up their organizations to breach opportunities.[17]

> “Overwhelmingly, corporate technology teams have the best interests of their organizations at heart. But by the nature of their roles as data custodians, those employees are considered privileged users if they have the ability to see what the C-suite is working on, talking about, deciding and planning. Consequently, they are opening up their organization to additional risks. Malicious actors often target those types of users via social engineering methods or other means of attack in order to gain full access to the system.”
>
> **Henry Jiang**
> Chief Information Security Officer,
> Diligent Corporation

Jiang continued: “Still, malicious insider threats are also a real concern. The most recent CapitalOne cyber breach in 2019 was a direct result of a rogue Amazon IT administrator who exploited a misconfiguration in the AWS environment.” [18]

[17] https://www.cnbc.com/2019/12/17/hacker-behind-your-companys-data-breach-may-be-in-the-next-cubicle.html
[18] https://cipher.com/blog/analysis-cyber-attack-capital-one

5 Key Elements of a Secure Collaboration System

Given these risks, what does a modern, secure solution for the C-suite look like? To be truly secure yet still effective, a collaboration solution must ensure:

- Confidential materials are held securely against unauthorized view, even within the organization.
- Sensitive communications are conducted in a closed-loop environment that can't be viewed by others, even within the organization.
- Executives have secure environments and workflows to communicate and collaborate with their boards, away from other viewers within the organization.
- The system is intuitive and convenient, so executives remain within its workflows and processes without straying to other systems and creating security gaps.

Five components are required to protect sensitive information while still enabling efficient collaboration:

1. ENCRYPTION

Encryption capabilities are essential for transmitting secure data and documents. Encryption translates data into a cryptographic key or a string of characters to protect information in transit.

- When using cloud-based video platforms like Zoom or Microsoft Teams, meeting links should be shared only on encrypted platforms to mitigate risk of them falling into the wrong hands.
- Board members, executives, legal and security teams should have access to encrypted tools for secure one-to-one or group messaging, for sharing documents, and for secure board communication and meeting management.

2. USER PERMISSIONS

The ability to set user permissions is critical to protecting sensitive information. Additional nuances must be considered at the board and senior leadership levels:

- Executives and board members need the ability to shield information from system administrators to ensure classified information remains truly classified. They should also be able to extend special permissions to the general counsel or other privileged parties when necessary.
- User permissions must work just as securely with external third parties (e.g., lawyers, auditors, consultants).

3. COMPLIANCE

Are your new virtual workflows compliant with the General Data Protection Act (GDPR)? Do they follow HIPAA guidelines for protecting the kind of employee health data that's shared during a pandemic?

- Organizations must ensure that the rapid transition to remote work hasn't compromised compliance in critical areas.
- Platform security must meet regulatory requirements for data processing and transmitting, and compliance often requires both encryption and system integrations.

4. RISK AND LEGAL CONTROLS

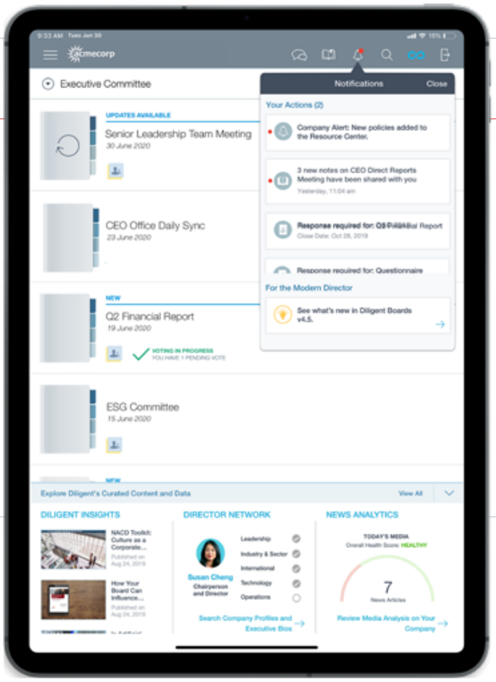
Mitigating legal risk and discoverability are inherent in any secure collaboration solution.

- Legal counsels should have the ability to either retain or destroy sensitive conversations, documents and notetaking when necessary.
- Organizations need the ability to wipe clean lost devices of all sensitive data.
- Confidential meeting records, messages and notes must have the ability to expire after a designated period of time set by the general counsel, corporate secretary or CISO.

5. SEAMLESS USER EXPERIENCE

Organizations must not underestimate the importance of integration and user experience when it comes to building secure collaboration workflows. Secure tools must be able to mirror the existing workflows of today's boards and leadership teams. Otherwise, there will be little progress toward a better solution.

- Secure messaging platforms should feel as seamless as email or text messaging.
- Minute-taking, voting and compliance reporting should all integrate with the board's management software.
- Permissioned users should be able to collaborate in real time.



Company Alert: New policies added to the Resource Center.

3 new notes on CEO Direct Reports Meeting have been shared with you
Yesterday, 11:04 am

Response required for: Q3 Financial Report
Close Date: Oct 28, 2019

Response required for: Questionnaire

See what's new in Diligent Boards v4.5.

Enabling a Secure Collaboration Solution

Understanding the benefits of secure collaboration tools – and the risks inherent otherwise – is vital for true implementation and adoption. To fully enable a secure solution within your organization, follow these steps:

1. EVALUATE YOUR CURRENT SYSTEMS

Determine whether your organization is already using a fully secure system for its sensitive data:

- ☐ Board members and executive teams have access to a fully encrypted platform that enables collaboration among members.
- ☐ Company leadership has access to a secure messaging platform to keep sensitive conversations outside of email.
- ☐ Company leadership has remote and mobile access to secure communication tools in the event of a crisis.
- ☐ Our current tools facilitate good governance and operations with improved visibility, robust security tracking features and optimized workflows.
- ☐ Our current tools provide high-touch technical and customer support in accordance with executives' expectations.

> "Systems that the C-suite thinks are secure — and may appear secure because they're password-protected or seem limited in scope — are often the systems that are ripest for exploitation. Accounting for all the users around the organization who have access to sensitive data is one of the first steps in securing those potential breaches. If you don't know who has access or how they access the information, you don't know where you're not secure."
>
> **Henry Jiang**
> Chief Information Security Officer,
> Diligent Corporation

2. IDENTIFY POTENTIAL PRIVILEGE MISUSE AND SECURITY WEAK SPOTS, AND EDUCATE LEADERSHIP ABOUT THE RISKS

An audit of current processes and privileged users is the best way to understand your organization's complete picture in terms of data access. Does the organization transmit these types of information over corporate email, personal email, text message or general-purpose collaboration tools (e.g., Slack, Google G Suite)?

- □ Financial information including unpublished P&L statements.
- □ Legal information and documents.
- □ Mergers & acquisitions information.
- □ Compensation, human capital and performance data.
- □ Strategic documents and growth plans.

Addressing Executive Objections

Understandably, members of the C-suite may raise concerns about adopting a secure collaboration platform. However, the benefits of a transition speak for themselves.

- **CFO:** The cost of selecting and onboarding a new system is considerable, both in dollars and human capital. Yet the cost of an inadvertent or malicious breach is significantly higher in every respect.
- **CIO:** Preventing privilege misuse in a secure collaboration platform may mean restricting or excluding some users who have admin access to other tools. But to ensure a truly secure system, only users with a defined need for the sensitive data should have access to it.
- **General Counsel:** Transferring data to a new system, often from multiple legacy tools, could result in lost data, missed compliance deadlines or other legal headaches if not handled properly. When selecting a secure collaboration partner, opt for one who thoroughly plans out those transitions and addresses concerns.

3. IDENTIFY AND ONBOARD A SECURE TECHNOLOGY SOLUTION

Invest the time and resources in identifying and evaluating a secure collaboration platform that will provide the protection and ease of use your C-suite will adopt and use. Look for the following features in a secure collaboration platform:

- □ **A fully integrated solution:** Designed specifically for C-suite executives and board members.
- □ **Secure messaging:** Instant message- and email-like functionality that allows executive teams to communicate securely.
- □ **Secure file-sharing:** Virtual data rooms and seamless document sharing, both internally and externally with trusted third parties (e.g., outside counsel, compensation consultant, auditors, etc.).
- □ **Secure workflows:** Encrypted tools designed to support various sensitive workflows (e.g., M&A transactions, sensitive meeting preparation, board materials preparation, etc.) among the C-suite, board finance and legal team members.
- □ **Controlled access:** Robust, customizable user permissions that shield data from anyone without an immediate need for it.
- □ **Centralized systems:** Secure platforms accessible by permissioned users across the organization.
- □ **Easy integration and adoption:** High-touch customer support available around the clock.

Gaining Buy-In Across the Organization

- □ Recruit other members of the C-suite to help you make the case within your organization. Adopting a new platform is a complex endeavor; other executives' use cases will help justify the undertaking.
- □ Take the time to evaluate available solutions in terms of the five critical criteria: encryption, user permissions, compliance, risk and legal controls, and user experience.
- □ Once the right system for your organization is identified, begin the onboarding process. Plan the time for a comprehensive rollout, so a full transition to the secure system can be properly made.

Mitigate the Insider Threat: Collaborate on Critical, Sensitive Topics With Confidence

To perform their roles effectively while still protecting the organization from malicious or inadvertent breaches, C-suite executives have increasingly turned to collaboration tools that offer unmatched levels of security – not only from outside actors, but from unauthorized access within the organization.

Many businesses already turn to Diligent Corporation for secure collaboration among their boards. Now, Diligent has assembled a comprehensive suite of tools — the Board & Leadership Collaboration — that supports secure collaboration and communication for executive teams.

The Leadership Collaboration Suite from Diligent:

- Is a fully integrated and encrypted solution.
- Features secure, real-time messaging, document sharing and editing.
- Facilitates easy integration and adoption.
- Promotes modern governance best practices.

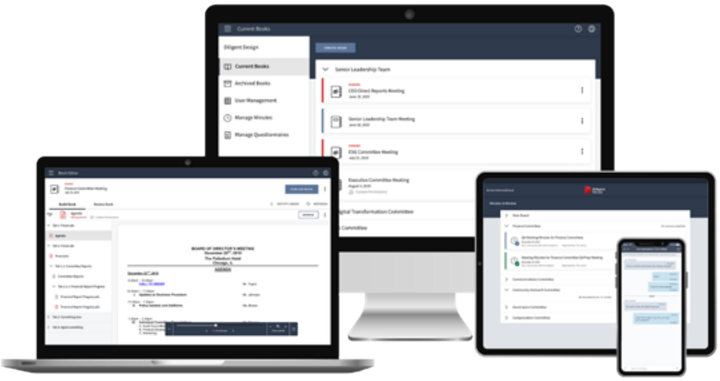
To take fullest advantage of the value Diligent's Leadership Collaboration Suite offers, an organization must be ready for the positive changes that the solution supports. Executives may already be aware of their growing vulnerability to data breaches (experts say it's a matter of *when*, not *if*),[19] and they should be aware of the risk breaches represent to the business and to its officers personally.

- **CEOs** often recognize the need for more secure collaboration tools, not only because they face some of the greatest personal risk, but also because of their roles in shaping culture and fostering innovation.
- **CFOs & Chief Counsels**, with their close ties to transactions, agreements, audits and compliance obligations, are often among the first to see the value of a closed loop for executive collaboration and communication.
- **CIOs** recognize the bulletproof, forward-thinking technology underlying the Leadership Collaboration Suite, and recognize that its security features will ease the risks they observe when collaborating with their peers.

Diligent's Leadership Collaboration Suite helps executives and their teams work securely, increase productivity and protect their organizations from risk. It enables leadership teams to communicate swiftly and effectively, to make agile decisions and to mitigate security risks — free of the insider threat.

[19] https://www.bloomberg.com/news/videos/2020-07-23/verizon-business-ceo-erwin-not-if-but-when-for-cyber-attacks-video

Securely Collaborate With Diligent



Encryption: With multiple levels of encryption, Diligent tools encrypt and decrypt data several times while information is in transit, providing an even higher standard of security than similar tools.

User Permissions: Strict user permissioning protects the data shared via Diligent Messenger, Diligent Secure File Sharing and Diligent Boards.

Compliance: A secure, single source of truth for executive teams mitigates risk by enabling transparency into compliance obligations and expirations.

Risk and Legal Controls: Tools like Diligent Boards and Messenger allow messages and notes to be set to expire after a designated period of time set by the general counsel, corporate secretary or CISO.

Seamless User Experience: Workflows mirror the communication and collaboration tools with which boards and management teams are already familiar.

About Diligent

Diligent is the global leader in modern governance, providing SaaS solutions across governance, risk, compliance, audit and ESG. Serving more than 1 million users from over 25,000 customers around the world, we empower transformational leaders with software, insights and confidence to drive greater impact and lead with purpose. Learn more at diligent.com.

Contact Us | Info@diligent.com | +1 877 434 5443 | diligent.com

SCHEDULE A DEMO ▸