Diligent

The fundamentals of secure governance communication

Diligent

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 data breach threatens every aspect of an organisation'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[1]. Meanwhile, annualised costs per incident hit a staggering USD $4.1 million, with the time required to contain an incident increasing from 77 to 85 days[2].

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 organisation, 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.

- Significant enhancements to Australia's Privacy Act came into effect in December 2022. The measures introduced a massive increase with maximum penalties now the greater of A$50million, three times the benefit of a contravention, or (where the benefit can't be determined) 30% of domestic turnover
- New Zealand gained a new Privacy Commissioner in 2022 who aims to raise organisational accountability for cyber security
- Indonesia, Japan, and Malaysia introduced tougher measures to their respective data protection and breach reporting schemes. The Thai Personal Data Protection act came into effect in June 2022, with enforcement action anticipated to hitting soon

---

[1] https://www.proofpoint.com/au/blog/insider-threat-management/insider-threats-are-still-rise-2022-ponemon-report
[2] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-au-tr-the-cost-of-insider-threats-ponemon-report.pdf

Diligent

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 prioritise 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 authorise large transactions and subordinates may be reluctant to question their requests. These costly breaches demonstrate the damage of unsecure workflows:

- In 2020, an Australian hedge fund collapsed after a cyber attack triggered by a fake Zoom invitation saw its trustee and administrator mistakenly approve A$8 million in fraudulent invoices. The funds largest institutional investor withdrew money as a result, collapsing the firm[4]

- In 2022, a group of hackers impersonated Binance CCO, Patrick Hillmann in a series of video calls with several representatives of cryptocurrency projects. The attackers used a deepfake (AI hologram) to fool representatives into making payments in exchange for listing their cryptocurrencies[5]

- In 2016, Chinese aircraft parts manufacturer FACC lost approximately USD $60 million when scammers impersonated top-level executives to deceive employees into transferring funds. FACC incurred additional expenses in their attempt to file a lawsuit against their CEO and finance chief, accusing them of neglecting to establish effective internal security measures[6]

By the numbers: Data breaches & the C-Suite

- Executives are less likely to follow the security policies that organisations have in place.[7]

- 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[8]

- C-level executives are 12 times more likely than other employees to be targeted by social engineering attacks[9]

- 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[10]

- The average cost of a data breach for organisations in Australian is USD$2.92 million and USD $2.87 million for ASEAN[11]

- The annual cost of cybercrime and economic espionage around the world may be as much as $445 billion, almost 1% of global income[12]

[3] https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/
[4] https://www.afr.com/companies/financial-services/fake-zoom-invite-cripples-aussie-hedge-fund-with-8m-hit-20201122-p56f9c
[5] https://www.theverge.com/2022/8/23/23318053/binance-comms-crypto-chief-deepfake-scam-claim-patrick-hillmann
[6] https://www.csoonline.com/article/3049392/chinese-scammers-take-mattel-to-the-bank-phishing-them-for-3-million.html
[7] https://www.cio.com/article/3247428/safeguarding-your-biggest-cybersecurity-target-executives.html
[8] https://www.helpnetsecurity.com/2019/09/10/cyberattacks-human-interaction/
[9] https://www.verizon.com/about/news/verizon-2019-data-breach-investigations
[10] https://www.csoonline.com/article/2134263/senior-managers-fumble-security-much-more-often-than-rank-and-file.html
[11] IBM, Cost of a Data Breach Report 2022, https://www.ibm.com/downloads/cas/3R8N1DZJ
[12] https://www.csoonline.com/article/3040982/data-breaches-often-result-in-ceo-firing.html

Diligent

The risks lurking in legacy platforms

Corporate email: Email is still the lifeblood of organisational 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 occurence. Plus, phishing remains the most effective tactic for accessing sensitive information, affecting employees at every level of the organization. Executives and the teams 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.[13] 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.

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.[14-15] 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

---

[13] https://www.zdnet.com/article/make-sure-your-zoom-meetings-are-safe-by-doing-these-10-things/

[14] https://www.zdnet.com/article/slack-vulnerability-allowed-session-hijacking-account-takeovers/

[15] https://securityaffairs.co/wordpress/99626/hacking/slack-bugs-account-takeover.html

Diligent

Privilege misuse: An unnecessary evil

One overlooked vulnerability of many collaboration tools and platforms is the way they are implemented and managed throughout the organisation. 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 organisations to unnecessary risks.

63% of employees report taking company data with them after leaving a job, opening up their organizations to breach opportunities.[16]

"Overwhelmingly, corporate technology teams have the best interests of their organisations 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 organisation 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

---

[16] https://www.cnbc.com/2019/12/17/hacker-behind-your-companys-data-breach-may-be-in-the-next-cubicle.html

Diligent

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 unauthorised view, even within the organisation

- Sensitive communications are conducted in a closed-loop environment that can't be viewed by others, even within the organisation

- Executives have secure environments and workflows to communicate and collaborate with their boards, away from other viewers within the organisation

- 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 my local data privacy requirements? What guidelines or frameworks do they follow to protect my requirements?

- Organisations 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

**Diligent**

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

- Organisations 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, company secretary or CISO

5. Seamless user experince

Organisations 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

Diligent
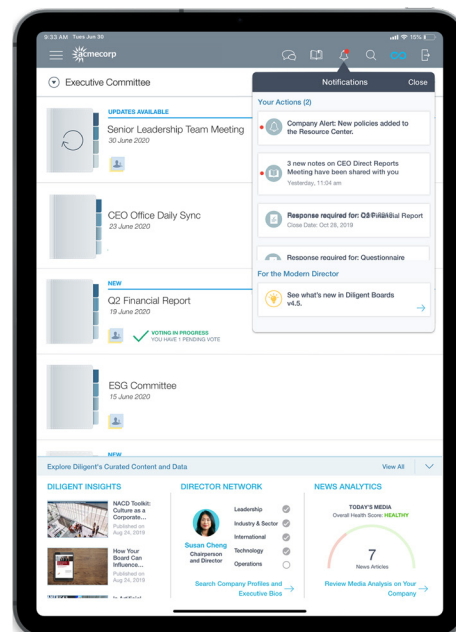
Enabling a secure collaboration solution

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 organisation, follow these steps:

1. Evaluate your current systems

Determine whether your organisation 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 emai.

- ☐ 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 optimised 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 organisation 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

Diligent

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 organisation's complete picture in terms of data access.

Does the organisation 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 and 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

Diligent

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, customisable user permissions that shield data from anyone without an immediate need for it

☐ **Centralised systems:** Secure platforms accessible by permissioned users across the organisation

☐ **Easy integration and adoption:** High-touch customer support available around the clock

Gaining Buy-In Across the Organisation

- Recruit other members of the C-suite to help you make the case within your organisation. 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 organisation 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

Diligent

Mitigate the insider threat: Collaborate on critical, sensitive topics with confidence

To perform their roles effectively while still protecting the organisation 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 unauthorised access within the organisation.

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 organisation 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*),[17] and they should be aware of the risk breaches represent to the business and to its officers personally.

- **CEOs** often recognise 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 and 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** recognise the bulletproof, forward-thinking technology underlying the Leadership Collaboration Suite, and recognise 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 organisations from risk. It enables leadership teams to communicate to swiftly and effectively, to make agile decisions and mitigate security risks — free of the insider threat.

---

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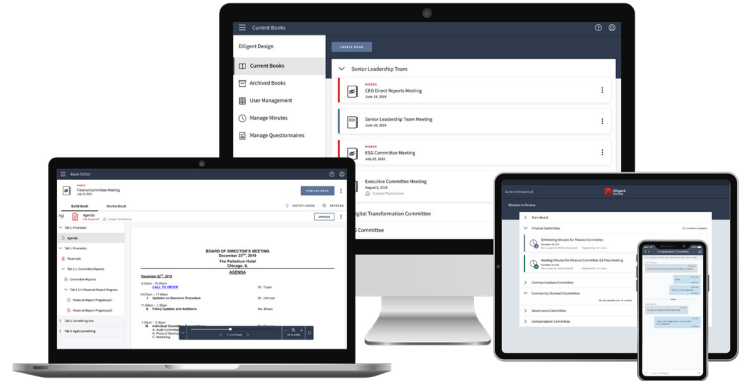
Diligent

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, company 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 | diligent.com/en-au

SCHEDULE A DEMO ›