Diligent

Board and Executive Collaboration: **Components of a Secure Platform for the Evolving Workplace**

Today's workplace is no longer limited to traditional definitions or boundaries. Companies are constantly adapting to new working models and exploring innovative ways to tailor them to the needs of their organization. The adoption of collaboration tools has skyrocketed as companies try to ensure that productivity and efficiency remain high, whether in a remote, in-office or hybrid work environment.

Many of these newly adopted collaboration tools are general-purpose solutions that meet the requirements of employee communication and collaboration well enough. But they may not be appropriate for the top layer of your organization — the board and executives.

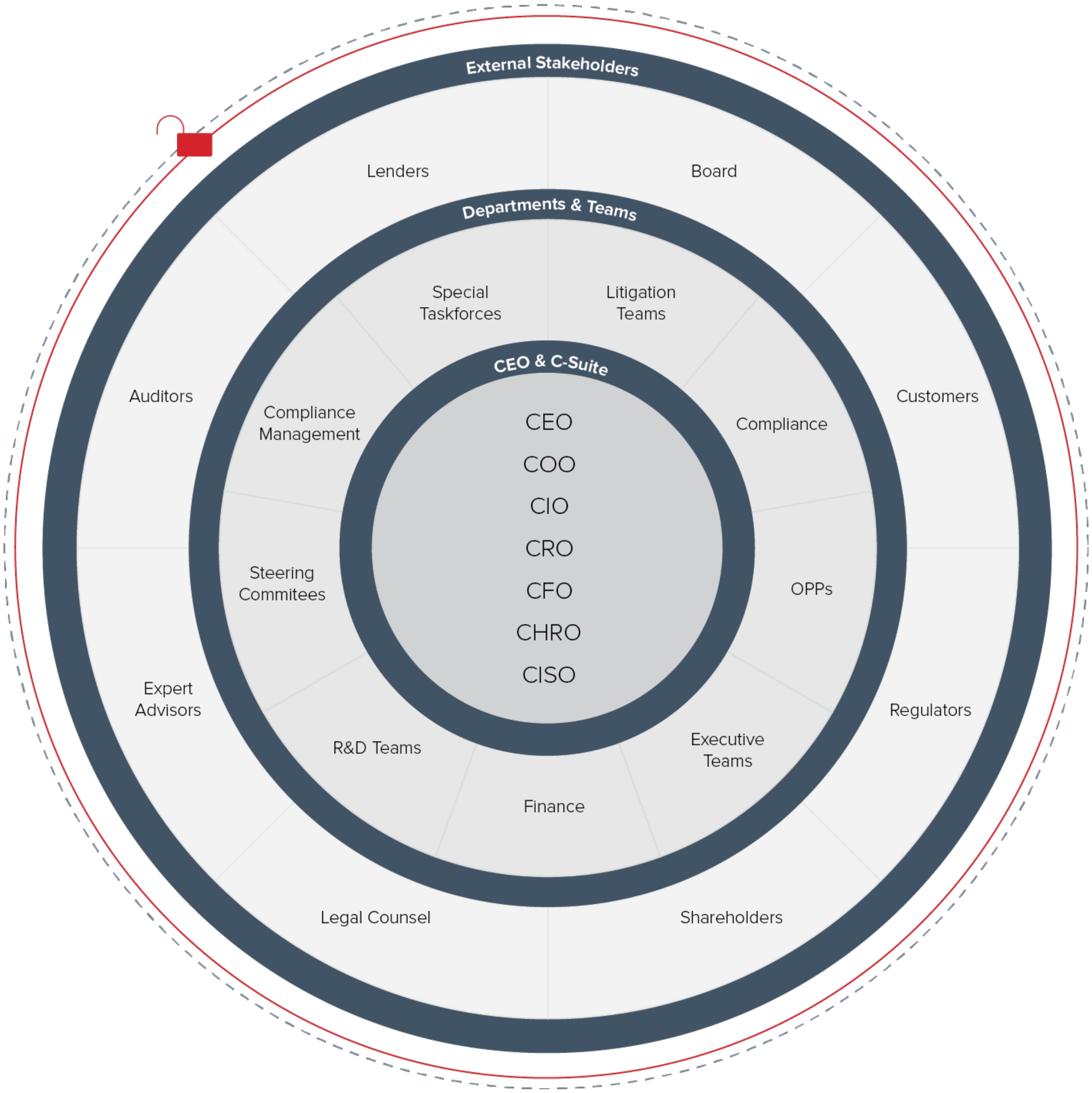
Your board and executives deal with information that is often highly sensitive and that consequently has higher costs of exposure. Think of the reputational, legal and financial repercussions if a classified document leaked because it was shared by executives on a general-purpose communication tool. The impact could be catastrophic. Additionally, recent cyberattacks have highlighted — not just for shareholders, but for all stakeholders — the importance of protecting an organization's most sensitive data. General-purpose collaboration tools are unable to offer the level of protection that stakeholders expect.

It's critical to transition board and executive collaboration to the appropriate tools. This guide will help you:

- Investigate the effectiveness and identify the shortcomings of your existing tools for senior teams
- Explore robust technologies that can help secure your organization's most sensitive targets — your board and executives
- Help you establish an agile and scalable platform that meets the evolving needs of your organization's return-to-office (RTO) strategies

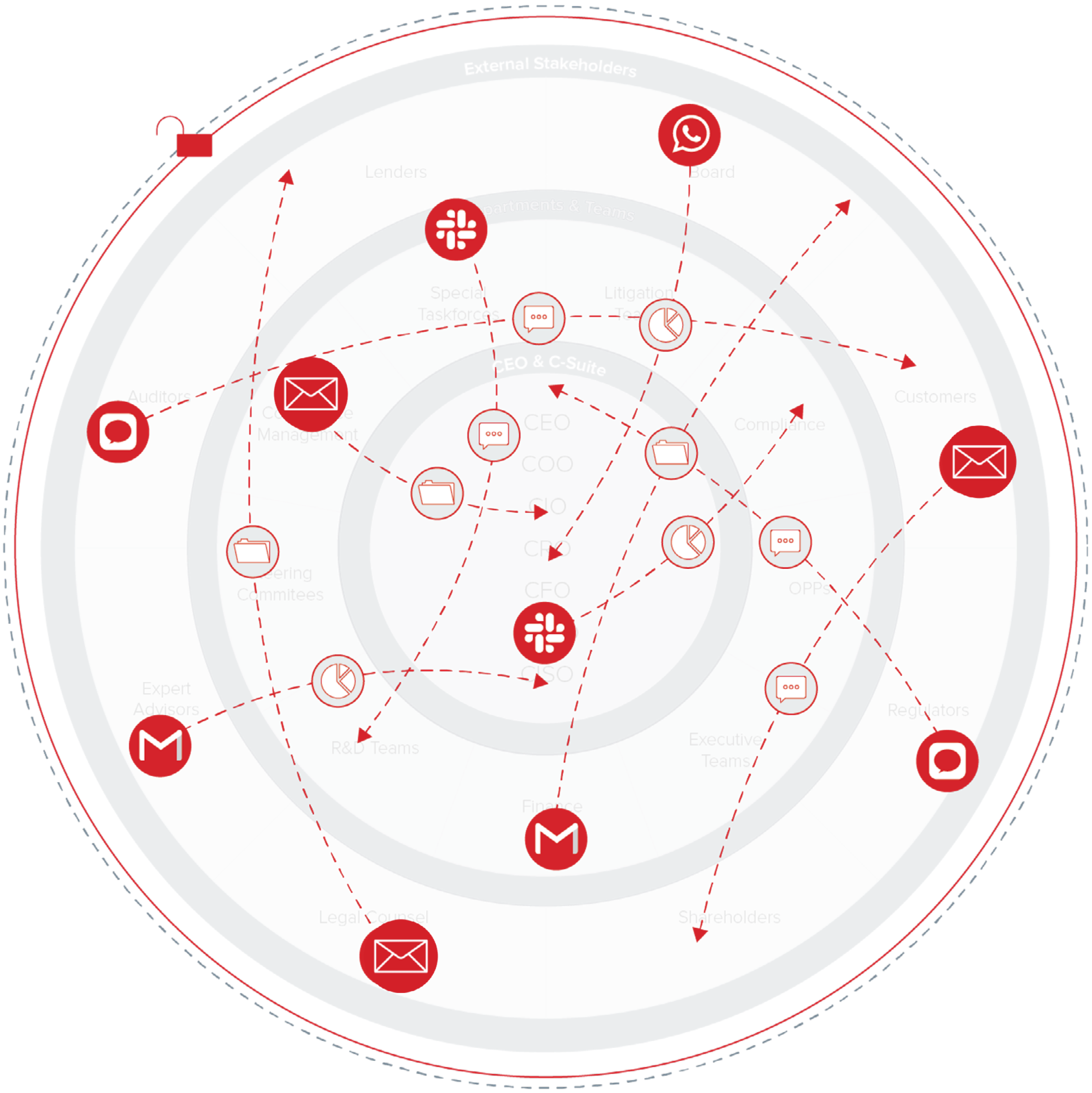
Risks Lurking in Your Board and Executive Team's Daily Communications

Navigating your evolving RTO plans requires careful coordination and collaboration between boards and leadership teams. This spans every business unit and includes collaboration with external stakeholders.



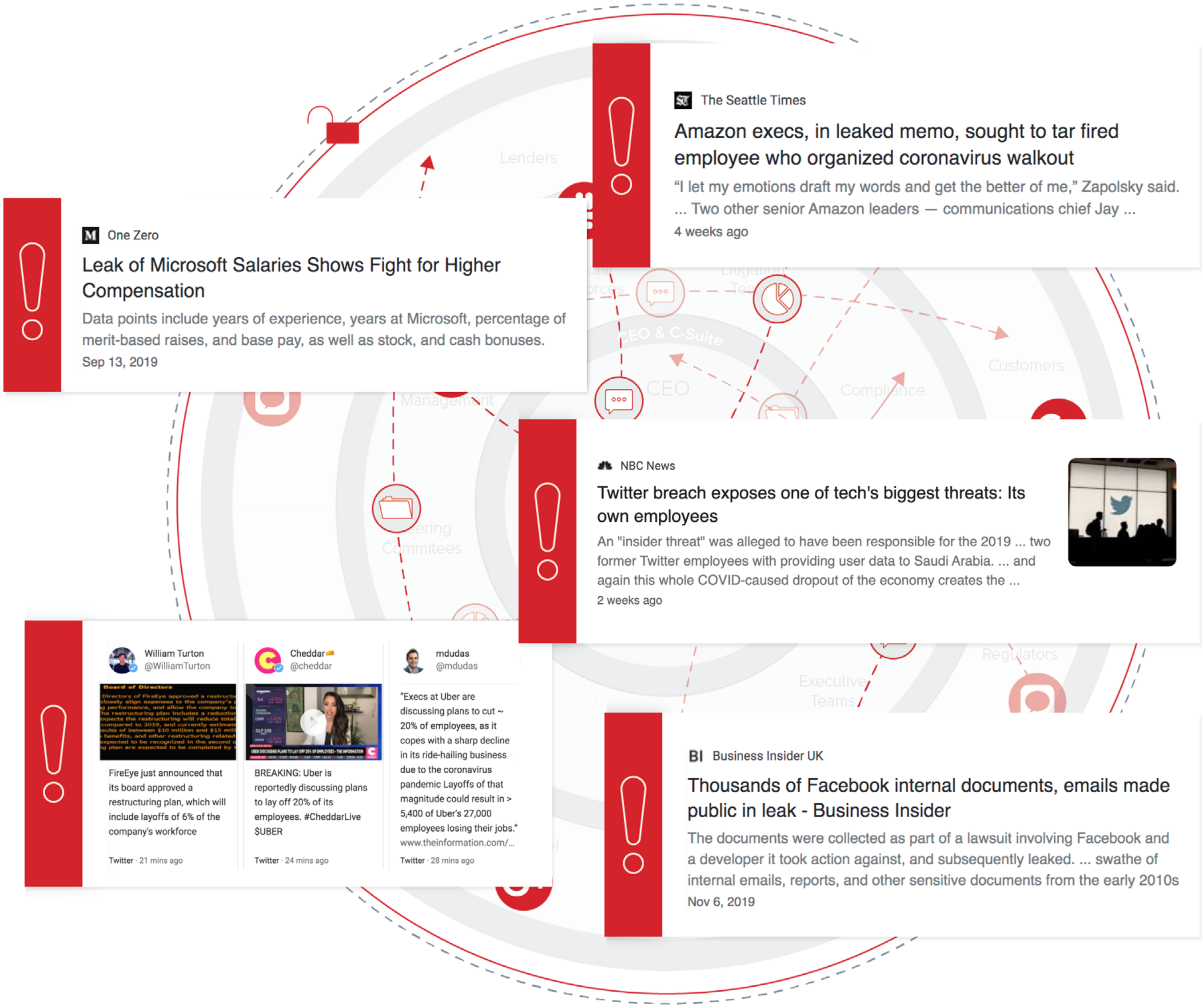
An organization-wide lens of stakeholders involved in governance who frequently engage in workflows containing sensitive data

The evolving nature of these strategies means that leaders are often making tough business decisions on information that can change overnight. This leads to daily, weekly and quarterly exchanges of confidential information inside and outside the firewall. Creating millions of touchpoints across email, Slack, file-sharing systems, text message and other channels exposes organizations to cyber and discoverability risk.



Millions of touchpoints across enterprise-wide tools increase discoverability and cyber risk

Costly leaks occur when the risks of using vulnerable communication channels aren't well understood. Without a clear policy, stringent controls and the right technology solutions, teams working with sensitive information often rely on email or general-purpose collaboration tools because they don't fully understand the risks associated with them.



The Seattle Times

Amazon execs, in leaked memo, sought to tar fired employee who organized coronavirus walkout

"I let my emotions draft my words and get the better of me," Zapolsky said. ... Two other senior Amazon leaders — communications chief Jay ...

4 weeks ago

One Zero

Leak of Microsoft Salaries Shows Fight for Higher Compensation

Data points include years of experience, years at Microsoft, percentage of merit-based raises, and base pay, as well as stock, and cash bonuses.

Sep 13, 2019

NBC News

Twitter breach exposes one of tech's biggest threats: Its own employees

An "insider threat" was alleged to have been responsible for the 2019 ... two former Twitter employees with providing user data to Saudi Arabia. ... and again this whole COVID-caused dropout of the economy creates the ...

2 weeks ago

William Turton
@WilliamTurton

FireEye just announced that its board approved a restructuring plan, which will include layoffs of 6% of the company's workforce

Twitter · 21 mins ago

Cheddar
@cheddar

BREAKING: Uber is reportedly discussing plans to lay off 20% of its employees. #CheddarLive $UBER

Twitter · 24 mins ago

mdudas
@mdudas

"Execs at Uber are discussing plans to cut ~ 20% of employees, as it copes with a sharp decline in its ride-hailing business due to the coronavirus pandemic Layoffs of that magnitude could result in > 5,400 of Uber's 27,000 employees losing their jobs."
www.theinformation.com/...

Twitter · 28 mins ago

Business Insider UK

Thousands of Facebook internal documents, emails made public in leak - Business Insider

The documents were collected as part of a lawsuit involving Facebook and a developer it took action against, and subsequently leaked. ... swathe of internal emails, reports, and other sensitive documents from the early 2010s

Nov 6, 2019

Vulnerable communication tools often cause irrecoverable damages – financial and reputational

The Inherent Risks of General-Purpose Collaboration Tools

While boards and executive teams rely on broadly connected tools such as Microsoft Teams, Box, SharePoint, Slack and G Suite for some of their daily tasks, these tools should only be used for the right reasons. Conversations around the potential shift to workforce policies, possible mergers and acquisitions, financial restructuring, human capital management and other sensitive matters require more secure solutions involving data encryption and privacy shielding.

Common Consumer / Commercial Products	Inherent Data Leakage Risks	Aggregated Risk Factors
WhatsApp	**Medium**	• Authentication: does not provide federated identity integration with enterprise customers
SMS text messages	**Very High**	• SIM card hijacking attacks • Communication not encrypted
Box and other file-storage systems	**Medium**	• Control of data contents resides within customer's reasonability • Misconfigured sites can result in data leakage • Larger attack targets (past attacks and known vulnerabilities)
Email	**High**	• Subject to account takeover attacks due to poor authentication methods • Contents downloaded from webmail platforms are often saved on disks unencrypted • Cannot enforce strong user authentication methods such as MFA • Email messages can be saved on personal devices without applying encryption at-rest control (e.g. full disk encryption solutions such as Microsoft BitLocker, Mac's FileVault are not enabled by default).
Infrastructure as a Service (AWS, G Suite, Azure)	**Medium**	• Documents are protected individually by data owner • Depending on the security policy of the provider, there could be gaps in optimizing configuration to the latest standards • Misclassified data or out of date policy can result in unintentional data leakage
Enterprise file sharing systems (e.g., Citrix file sharing, Slack)	**Medium**	• File share locations are left open beyond original information exchange period • Files can be downloaded to undecrypted workspace such as local hard disks

Beyond the reputational risks and financial costs of leakage, when using email and enterprise collaboration solutions, the data, metadata, documents and communications shared on those platforms are all discoverable.

Total litigation costs of the Fortune 500 = $210 billion which is estimated at 1/3 of profits

(eLaw Forum)

20% to 50%

of all costs in federal civil litigation are incurred to perform discovery *(Duke Law)*

The exploding volume of email and other communication channels expanded regulations related to data retention. The remote/hybrid work environment has exponentially increased the costs associated with risks surrounding data.

All of that data has to be stored and preserved, which is a cost and time investment from Legal and IT

$40M

spent on an email archiving system for preservation purposes at Eli Lilly

Regulations related to cyber/data privacy increasing

50%

of GCs feel more exposed to cybersecurity and data privacy protection issues *(Norton Rose Fulbright 2019)*

38%

of GCs feel regulators are becoming more interventionist *(Norton Rose Fulbright 2019)*

5 Critical Components Needed for Boards and Executives to Collaborate Securely

1 Risk and legal controls

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

- The communication platform should equip users with the ability to either retain or destroy sensitive conversations, documents and note-taking when necessary.
- Lost devices, especially those of senior executives in the organization, must be wiped clean of all sensitive data.
- Confidential meeting records, messages and notes must have the ability to expire after a designated period, as defined by the policies set by your organization's security leaders.

2 Scalable compliance framework

Your RTO plans may need to be compliant with several regulatory obligations; your remote workflows may need to be compliant with the General Data Protection Act (GDPR); your organization may need to follow HIPAA guidelines for protecting the kind of employee health data that's shared as they return to a physical office location; and so on.

- Platform security must meet regulatory requirements for data processing and transmitting, and compliance often requires encryption and system integration.
- Compliance workflows must be automated to gain real-time overviews of internal and external obligations
- Your compliance framework must be scalable to align with evolving regulatory, legislative, business and contractual obligations..

3 User controls to protect sensitive information

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 to shield information from system administrators to ensure that classified information remains truly classified. They should also 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).

4 Robust data 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 the 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 the risk of sensitive information falling into the wrong hands.
- Board members and executives 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.

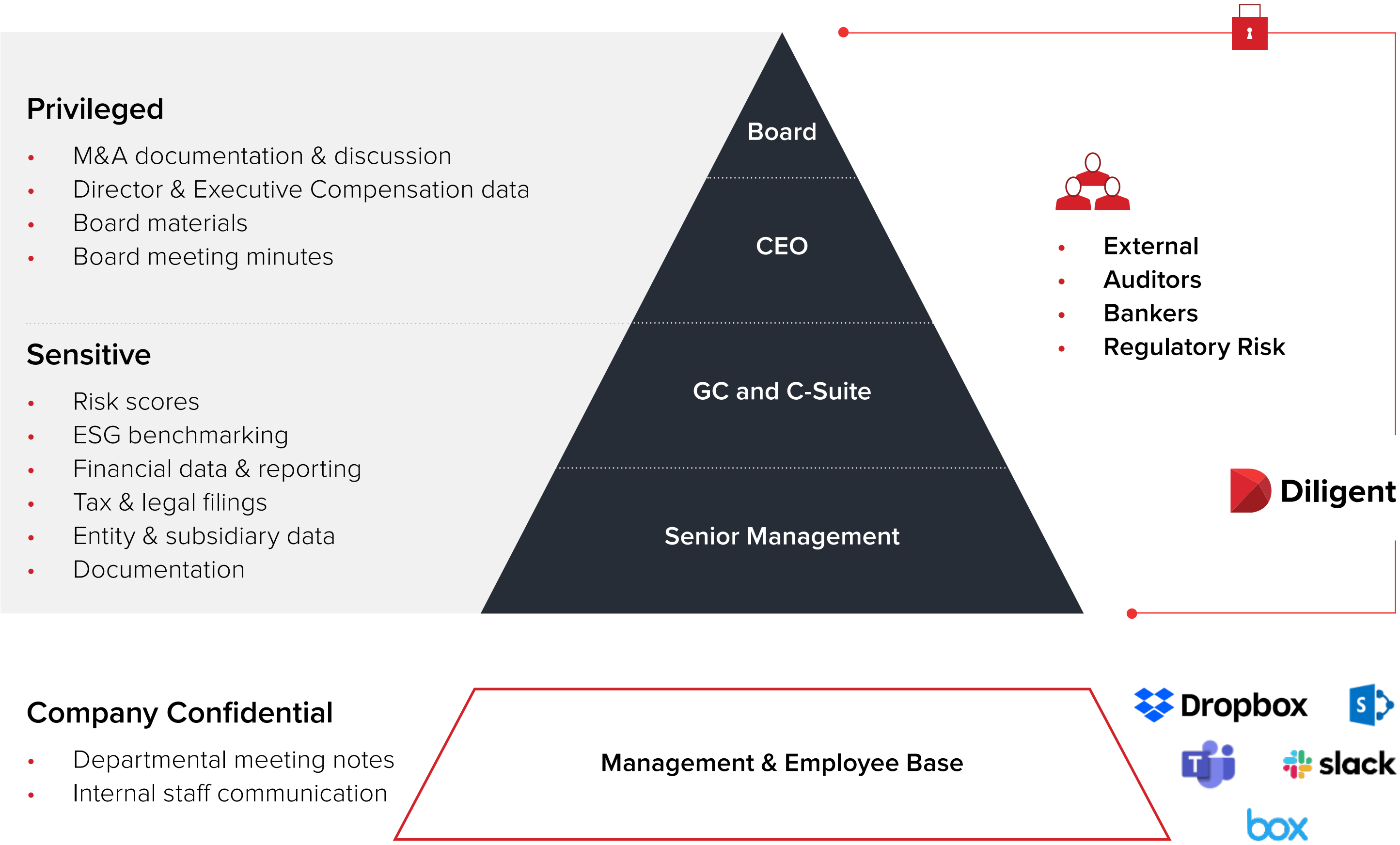
5 Seamless user experience

Organizations must not underestimate the importance of integration and user experience when 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.

Protect Confidential Information at the Most Senior Levels of Your Organization With Diligent

In this evolving landscape, you're only as secure as your lowest common denominator. Boards and executives operate at an information tier that requires a heightened level of privacy and security — one that general-purpose collaboration tools cannot provide.



Privileged

- M&A documentation & discussion
- Director & Executive Compensation data
- Board materials
- Board meeting minutes

Sensitive

- Risk scores
- ESG benchmarking
- Financial data & reporting
- Tax & legal filings
- Entity & subsidiary data
- Documentation

Company Confidential

- Departmental meeting notes
- Internal staff communication

- External
- Auditors
- Bankers
- Regulatory Risk

The information being shared today is more sensitive than ever — crisis response strategies, employee health data, P&Ls in flux. What happens when this information ends up in the wrong hands? Diligent's solutions are purpose-built to protect the most sensitive data and workflows while enabling efficiency.

Board & Leadership Collaboration From Diligent:

- Is a fully integrated and encrypted solution
- Features secure, real-time messaging, document-sharing and editing
- Facilitates easy integration and adoption

Tasks	Diligent	Slack	Teams	Email
Share agendas and sensitive content for executive team meetings	🔒			
Collaborate on business continuity and contingency plans	🔒			
Discuss major corporate initiatives, like restructuring or layoff plans	🔒			
Communicate with your board, executive team, or outside counsel	🔒			
Plan organizational strategy or market activity, like M&A projects	🔒			
Review press release statements before going public	🔒			
Access resources from anywhere using your mobile device	🔒	🔒	🔒	🔒
Collaborate on daily activities and projects		🔒	🔒	🔒
Connect with IT support for help with technology challenges		🔒	🔒	🔒
Celebrate team wins, team members’ birthdays and other milestones		🔒	🔒	🔒
Web conferencing with full team or department participation		🔒	🔒	🔒

Drive Board and Leadership Effectiveness and Mitigate Risk While Collaborating Remotely

Communications within the Diligent ecosystem are secure and private where activity is not tracked to prevent liability. Data, documents and workflows managed in Diligent are shielded from the rest of the organization, minimizing discoverability. This reduces internal IT costs, as technology teams don't have to spend on infrastructure for security or on personnel for additional support.

Communicate securely

Enable safe and secure communications between board members and executives with total control of data retention.

Manage access to information

Completely lock down the security of your data at rest and in transit with strong encryption and granular access controls.

Protect sensitive data and workflows

Secure and automate the creation, editing, storage and sharing of highly sensitive materials while collaborating with stakeholders.

Mitigate risk of security breaches

Diligent's products are backed by the world's leading security standards with secure data centers located around the world.

Diligent's industry-leading suite of solutions changes how work gets done at the executive and board levels. Leaders rely on Diligent to drive accountability and transparency, while also addressing stakeholder and shareholder priorities. Our comprehensive, integrated suite of secure applications means all workflows fall under the same security umbrella, driving operational efficiency and mitigating cyber risk.

> "[Diligent] helps ensure important messages don't get lost, and it provides us with another layer of protection knowing communications are being made on the securest platform available."
>
> **Ben Backberg**
> **Senior Counsel and Assistant Corporate Secretary, General Mills**

Collaborate Securely 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 Diligent Messenger allow messages and notes to be set to expire after a designated period 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.

Board and Executive Use Cases

1

Support board meetings and global leadership meetings and operations

The switch to remote and hybrid work has exacerbated the need for a centralized platform that hosts executive teams' meeting materials, news updates, task managers, documents, data rooms and messages, all in one secure place. Organizations of all sizes use Diligent to streamline and secure their board and executives' daily meetings and operations.

2

Collaborate with external stakeholders

Protecting the highly confidential exchange of ideas is a top priority for board and executives. Diligent provides an unmatched security infrastructure to ensure executives and leadership teams can collaborate with their trusted partners effectively.

3

Protect sensitive materials in high-value departments

Executives and leadership teams look to Diligent to protect information shared during regular business meetings, such as senior leadership team meetings, M&A, sales forecasts, product R&D and internal strategy.

4

Shield confidential IP outside the firewall

Forward-looking institutions rely on Diligent to protect their highest-level IP when it's shared outside the organization, giving individual salespeople, customer success reps and senior leadership their own personal folders to use when sharing documents externally.

5

Access crisis management and business continuity information

Diligent is a central repository for boards and executives to access scenario plans, external communications or supply chain updates in real time. It also provides a secure environment for critical information exchanges, reports and collaborative decisions.

6

Curate insights and market intelligence

Diligent's curated personalized intelligence keeps leadership informed about industry news and can also be used more widely across the organization to keep employees and stakeholders abreast of market trends and competitors.

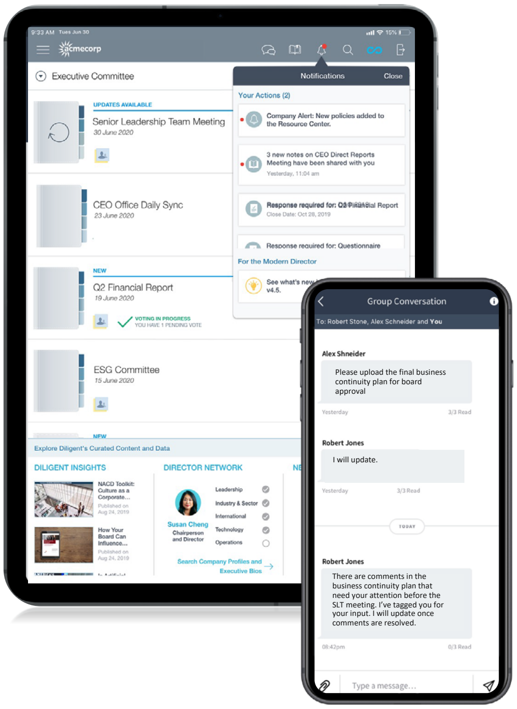
7

Safeguard merger and acquisition data

Effective M&A and corporate development require the ability to collect, segregate and leverage competitive intelligence. Diligent enables teams to manage this highly sensitive information, provides teams with control over access to this data on a need-to-know basis, and facilitates easy coordination during post-merger integration for selective groups within and potentially outside the company.

> “We had to communicate highly sensitive government directives to the board prior to [their] becoming public knowledge, and collaborating via Diligent was reassuring. We didn’t have sensitive data moving around our email network, and this meant we kept valuable patient data and system information secure and confidential.”

Dauniika Puklowski
Director, Board Administration Services Ltd,
Board & Committee Effectiveness, Professional Services, New Zealand



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: Q2 Financial Report
Close Date: Oct 28, 2019

Response required for: Questionnaire

See what's new v4.5.

To: Robert Stone, Alex Schneider and **You**

Alex Shneider
Please upload the final business continuity plan for board approval

Robert Jones
I will update.

Robert Jones
There are comments in the business continuity plan that need your attention before the SLT meeting. I’ve tagged you for your input. I will update once comments are resolved.

For more information or to request a demo:

Email: **info@diligent.com** • Visit: **diligent.com**