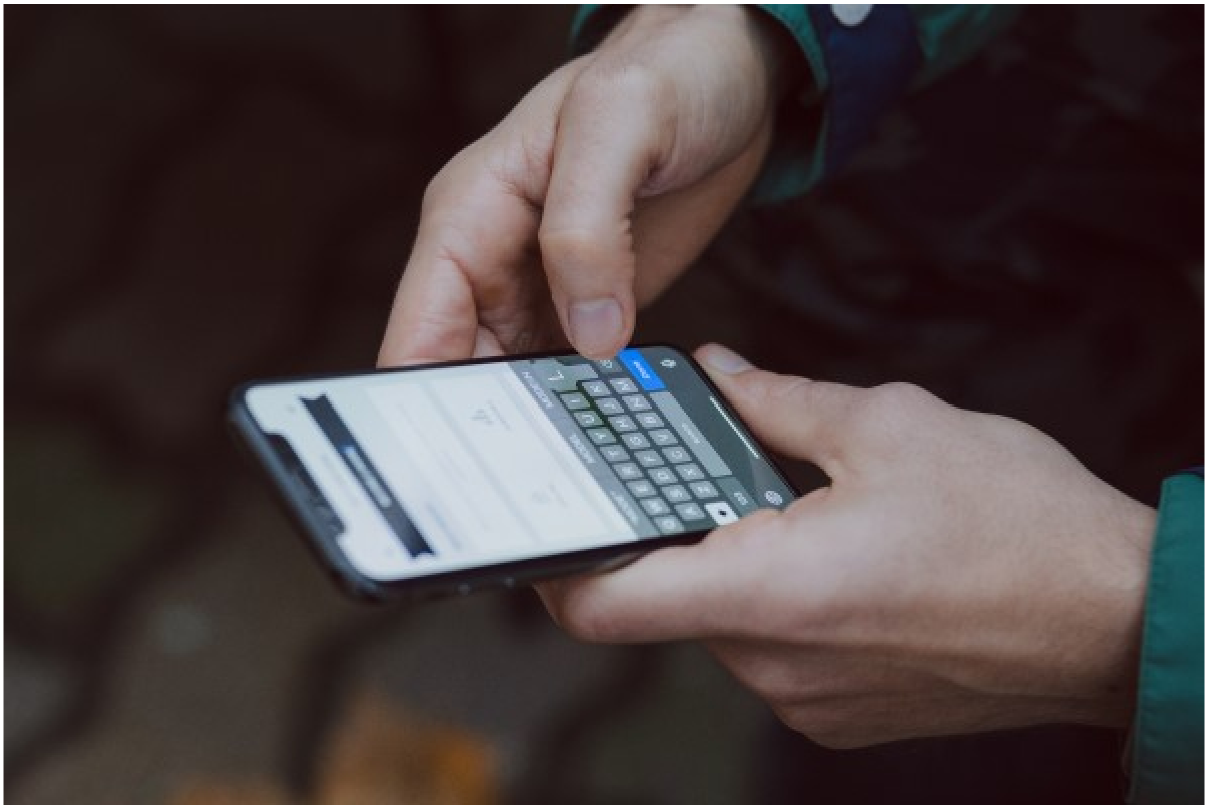
Governance Institute of Australia

The dangers of unsecure communication

by **MARY FETHEROLF, DILIGENT**

15/12/2020



(sponsored article) When the coronavirus pandemic began earlier this year, organisations were forced to move their processes online. Now, sufficient time has passed to assess the systems they adopted when COVID-19 was a new emergency. The patchwork of tools assembled under the urgent conditions of 2020's first and second quarters should be reevaluated for their fitness for purpose, their efficiency and interoperability, and — most importantly — their security capabilities.

Many organisations have already adopted a ‘next wave’ of systems designed to provide highly secure collaboration for board members and senior executives. Diligent’s recent Modern Governance Summit 2020 included a session entitled ‘Best practices for remote sensitive communication, collaboration and meeting workflow.’ Presenters described a current state of operations characterised by multiple business units and stakeholders, inside and outside the organisation, getting the work done together. Without proper technology in place, they warned, board members and senior executives use the same standard-issue collaboration and communication technology to conduct the tasks of corporate governance. The tools leaders are using for collaborations about sensitive board and C-suite topics are often no more secure than the tools used by any other employee.

The presentation described how organisations can ensure that sensitive information concerning board and leadership meetings remains confidential and secured against the dangers of a breach.

What are the risks of unsecure communication?

Stock price, profitability, business and personal reputations: There is a surfeit of stories about the costs and dangers of data breaches. Board members and senior executives already work in an environment where all players must be conscientious about data protection. Yet business leaders’ channels of communication are especially vulnerable, especially now. Businesses persist in using the broadly available collaboration and communication tools they’d adopted when COVID-19 first propelled leaders into home offices. Meanwhile, bad actors have taken note. They’re exploiting the new vulnerabilities arising from sensitive information that remote work has made more mobile: sensitive links texted, confidential files emailed and teleconference login information made public. Among the risks found in general-purpose collaboration tools like SMS text messaging, file storage systems, email, and infrastructure as a service, experts find unencrypted communication, takeover attacks due to weak authentication, and data leakages stemming from misconfiguration and misclassified information.

Addressing unsecure communications in governance

Organisations can control sensitive board and C-suite communications by assessing their current processes. They can evaluate how information travels today: personal email, enterprise-wide email, SMS text messaging, generally available collaboration tools (such as Slack) or virtual meeting technology (such as Zoom). Then, they can check whether any of the following kinds of information is shared on these platforms:

- financial statements
- legal documents

- merger, acquisition and divestiture information
- human resources materials related to compensation, recruiting or performance
- documents concerning corporate strategy.

General-purpose collaboration tools will get used to share sensitive information unless highly secure, highly adoptable alternatives are provided. Look for a suite of secure, interoperable collaboration tools. The technology should include secure file sharing and workflow designed expressly for governance tasks such as the collation, distribution and management of board meeting materials. It should also include a secure messaging platform that feels like email and texting to users, but that safeguards leadership communications in a closed loop, and that can deliver messages and notifications via laptop, tablet or mobile platforms.

'When we looked at Diligent Messenger it just had everything… and it shows up on your phone… it says, "You have a message," but it doesn't send the sensitive data. So, at no time does any of our material leave the secure portal. And that was our biggest concern.'

Tammy Wellcome, Corporate governance paralegal

What to look for in a secure platform

Secure collaboration tools should protect confidential materials from unauthorised views, even within the organisation. All sensitive board and executive communications should be conducted within a closed environment that can't be accessed by anyone else. If the governance collaboration environment isn't intuitive and easy, users may look for more convenient (and less secure) ways of getting their work done. So ease of use and strong adoption are paramount.

- **Collaboration tools must protect vulnerable data in transit**. Look for encryption that will protect information in transit from one party or place to another. Ideally, the technology will encrypt and decrypt data multiple times while it's in transit. Encrypted tools will allow board members and senior executives to message one another, share documents and manage virtual meetings securely.
- **Collaboration tools must facilitate sharing, but shield data**. Look for user permission features that will accommodate nuanced and dynamic needs. Robust user permission features will ensure sensitive information is protected, but also allow board members and senior executives to grant special permissions to other privileged parties when they need to.
- **Collaboration tools must be compliant**. Organisations are subject to a variety of data privacy regulations such as General Data Protection Act (GDPR) and other standards. The rapid conversion to remote work introduced a hazard of drifting away from meeting such compliance

obligations. Look for platforms that are secure enough to meet regulatory requirements for secure processing and transmission of private data.

- **Collaboration tools must mitigate legal risk**. Your legal team should be able to retain or destroy sensitive information as they deem necessary. A general counsel, corporate secretary or chief information security officer should also be able to establish retention and expiration times for confidential meeting records and other sensitive board and executive communication.
- **Collaboration tools must emulate the habitual offline flow of work that is already familiar and comfortable for users**. Board members and senior executives should be empowered to communicate in real time, seamlessly moving from messaging, to file sharing, to secure virtual meetings.

Organisations that want to enhance secure collaboration for their board members and senior executives can find technology to meet their needs. It's a matter of seeking out tools designed expressly to support the collaborative tasks of the board and C-suite, while guarding sensitive data from security violations.

The pandemic has intensified and revealed the shortcomings of general-purpose collaboration tools, including inefficiency, dis-integration and security vulnerabilities. A secure collaboration platform designed specifically for the work of boards and senior executives will safeguard sensitive leadership information against bad actors, while providing an efficient, easily adoptable suite of tools for the critical work of governance.

FIND OUT MORE

Mary Fetherolf writes about the impact of new technologies and regulations on business strategy and operations. This second career follows several years consulting with business and technology leaders on program management and governance in regulated industries. Topics of interest include corporate governance, cybersecurity, data privacy, regulation, compliance, and digital transformation.

Return to Newsletter