THE SILENT CYBER RISK THREAT IN THE BOARDROOM:

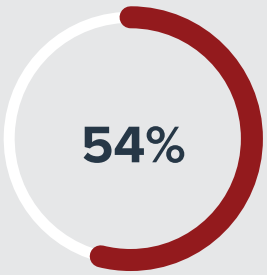
DIRECTOR COMMUNICATIONS AND DIGITAL BEHAVIOUR

Diligent

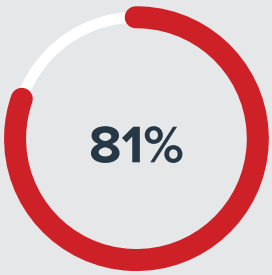
Contents

In this report

This report summarises the findings of a comparative study of 118 Australian organisations and companies, conducted in late 2017 by Diligent and Conscious Governance in partnership with the Governance Institute of Australia.

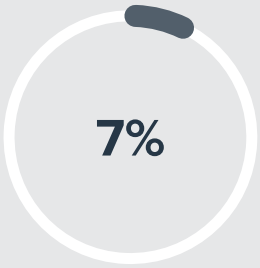


Believe more can be done to secure board communications



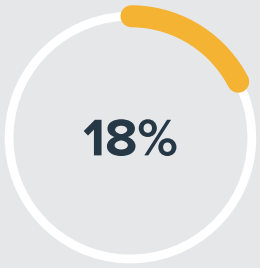
Communicate via **personal email** accounts

Require **cybersecurity training** for the board

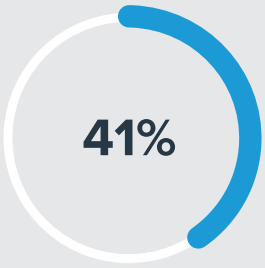


Board communications are sanctioned by the **IT/Data Security** team

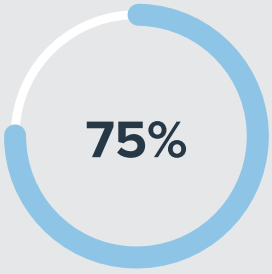
Say **digital tech** has increased the frequency of board communication



Monitor board compliance with communications guidelines



Use a **personal PC, laptop or tablet** for board business



Download board materials onto personal devices/drives

Introduction

Directors guide the success of organisations with their management, governance and strategic insights. Yet there's a deep disconnect between their perception of cyber risk and their day-to-day behaviour.

Diligent's survey of 118 directors, governance professionals and senior executives across Australia and New Zealand reveals the common communications practices that are inadvertently putting organisations' profits and reputations at risk.

Dozens of recent high-profile cybersecurity incidents underline the reality of the risk. Many organisations are playing catch-up as the rapid pace of technological change continues.

BUT TIME IS RUNNING OUT.

Diligent's survey reveals why and also pinpoints areas where improvements are needed, including training, monitoring and support, if boards are to manage their exposure effectively.

Research objectives

The survey explored practices at the highest levels of organisations to give a new perspective on boardroom cybersecurity culture, including:

- Whether directors' communication norms and digital behaviour provide adequate protection
- How much training and support directors receive on cyber issues
- The extent of boards' cyber risk awareness and oversight responsibilities
- What impact technology has on the information management provides to boards

We hope that organisations will use this report to inform their own boardroom cyber risk practices and to develop stronger defences.

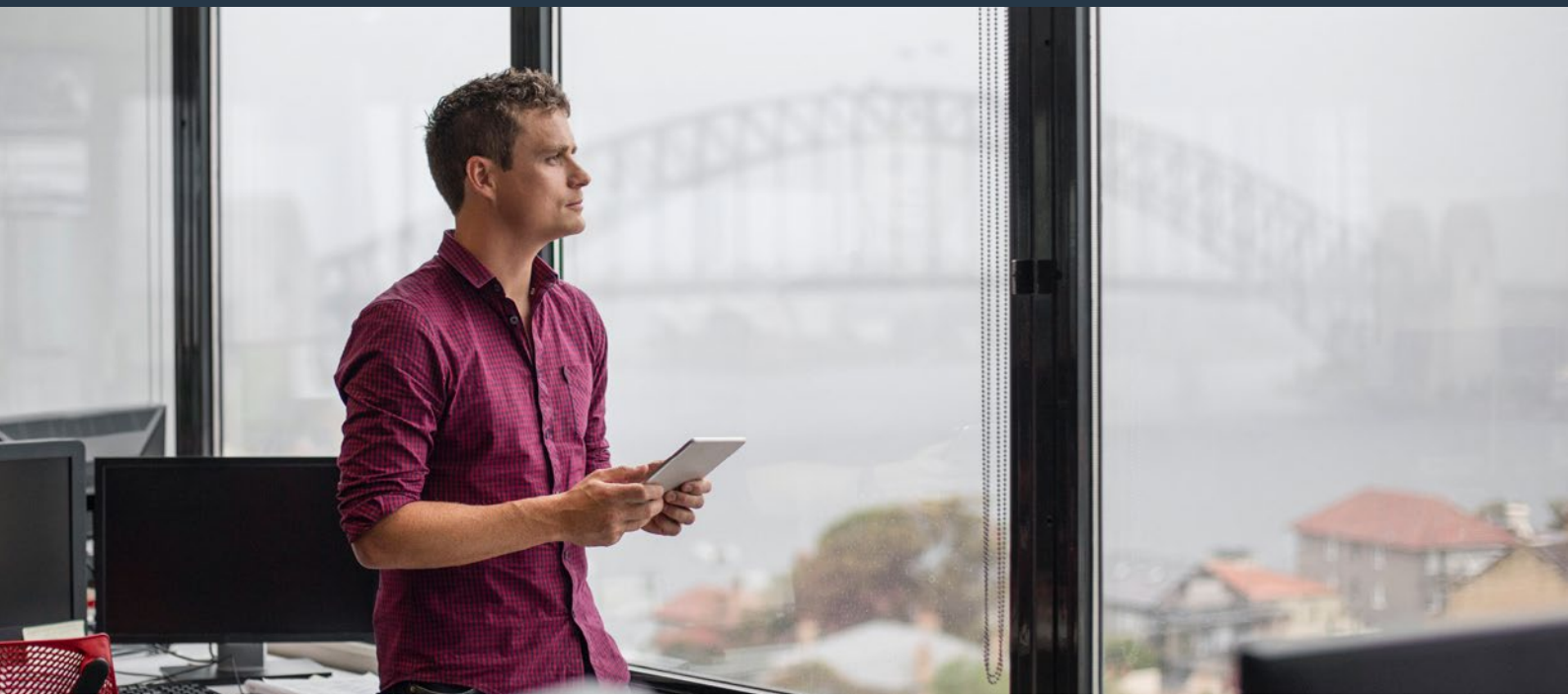
Key findings

Five key themes emerged from responses to the survey:

1. Directors' email use is a common weak link in cybersecurity – but it's not the only one
2. Board communications often fall outside of organisational policy and oversight
3. Many directors agree that board communications need to be more secure
4. More information and support are needed for boards to oversee cyber risk effectively
5. Technology is driving more communication between directors and management

This report presents the detailed survey findings, their implications and risks, accompanied by practical suggestions for how to strengthen boards' cyber risk culture.

Part of a bigger picture



Australia has already taken significant steps to address the growing cybersecurity threat. The national Cyber Security Strategy has been developed by the Federal Government's Department of Prime Minister and Cabinet. It encourages broad collaboration across business, government and other stakeholders to advance the country's cybersecurity defences.

As part of the national strategy, the Australian Securities Exchange earlier this year released the ASX 100 Cyber Health Check Report, which assessed cyber risk maturity across the country's largest listed companies.

This survey follows a 2017 report undertaken in the US, in partnership with NYSE Governance Services and Diligent, that looked at the practices of more than 350 listed companies.

INSIGHT:

"Cyber security is becoming a key strategic priority for boards of all shapes and sizes. Understanding where you, as a Director, might be breaking the chain of cybersecurity to enable potential successful cyber attacks is both a governance and legal obligation."

STEVEN BOWMAN, FOUNDER AND MANAGING DIRECTOR, CONSCIOUS GOVERNANCE

INSIGHT:

Directors' email use is a common weak link in cybersecurity – but it's not the only one.

What the data revealed

Directors play a fundamental role in shaping organisational culture. The values and behaviours they demonstrate in the boardroom and beyond reverberate through offices and work sites.

It is essential for directors to set the tone from the top for a strong risk management culture. But when it comes to digital security, their own practices often aren't keeping pace.

From how they communicate, to where they keep their board information, directors are inadvertently increasing their exposure to cyber risk.

The majority of respondents (81%) use their personal email accounts to communicate with fellow directors and management 'at least occasionally' – half of respondents (49%) 'regularly' use personal email accounts for board business. Personal email ranks in the top-three communications channels, behind face-to-face meetings (98%) and on par with corporate email (82%).

Three-quarters (75%) of respondents download board materials onto personal devices such as PCs, laptops, tablets or smartphones. Close to half (43%) say they download that information 'always' or 'most of the time'.

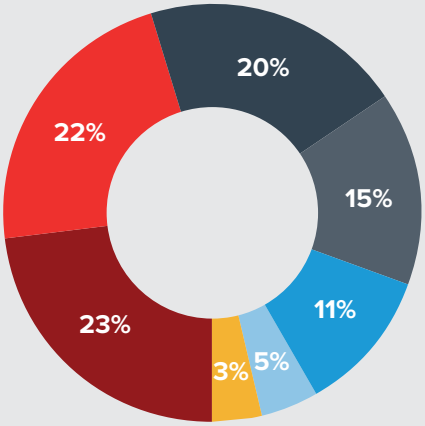
Company servers are the most popular location to save downloaded board materials (38%). But more than a quarter of respondents use file-hosting services such as Google Drive (28%) or personal or USB drives (also 28%). Some people routinely download documents to multiple locations for their ease of review and preparation.

Every single respondent uses a PC, laptop or tablet for at least some of their board preparation (some use more than one device). Print is far from finished, though, with almost half of respondents (47%) needing paper copies of board information more often than not, even when it has already been provided electronically. Fewer than one in five people (17%) never need printed information.

FIGURE 1

ROLE TYPES
(MOST SENIOR ROLE HELD)

There is a fairly even spread of role types, with CEO and Consultants making up the majority of the 'other' category.



INSIGHT:

"Board members have heaps of confidential company information stored on their personal PCs."

NON-EXECUTIVE DIRECTOR, SMALL NOT-FOR-PROFIT ORGANISATION

FIGURE 2

MARKET CAPITALISATION

Not-for-profit and small business made up the majority of board members.

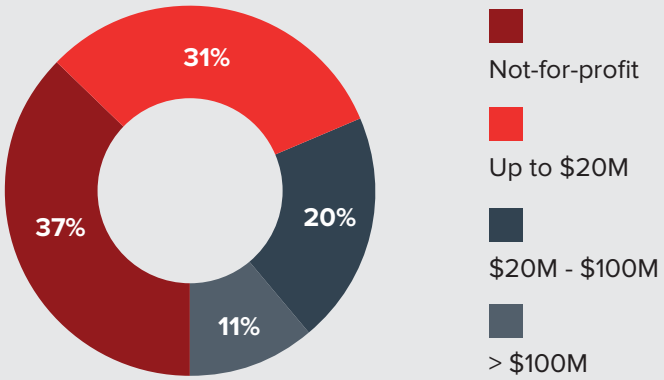


FIGURE 3

INDUSTRY

Not-for-profits made up a significant proportion of the board member base.

Not-for-profit	47%
Health Care & Social Assistance	14%
Education & Training	8%
Financial and Insurance Services	5%
Professional, Scientific & Technical Services	4%
Transport, Postal & Warehousing	4%
Other Services	3%
Government	3%
Mining	3%
Construction	2%
Retail Trade	2%
Accommodation & Tourism	1%
Administrative & Support Services	1%
Agriculture, Forestry & Fishing	1%
Electricity, Gas, Water & Waste Services	1%
Health/ Beauty Products & Fitness	1%
Information Media & Telecommunications	1%
Rental, Hiring & Real Estate Services	1%

FIGURE 4

DIRECTORS' MOST REGULARLY USED FORMS OF COMMUNICATION

Face-to-face and email were the most regularly used communications channels for Directors.

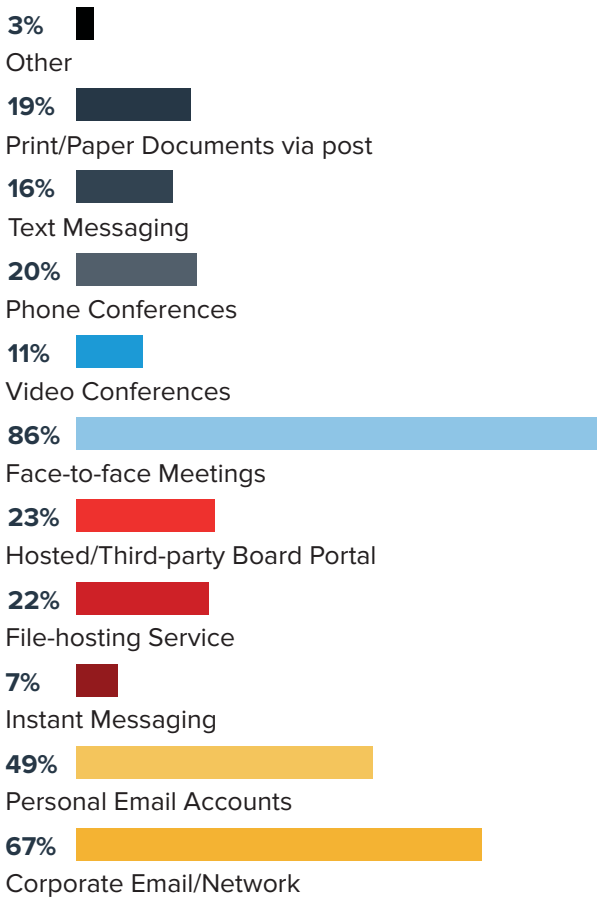
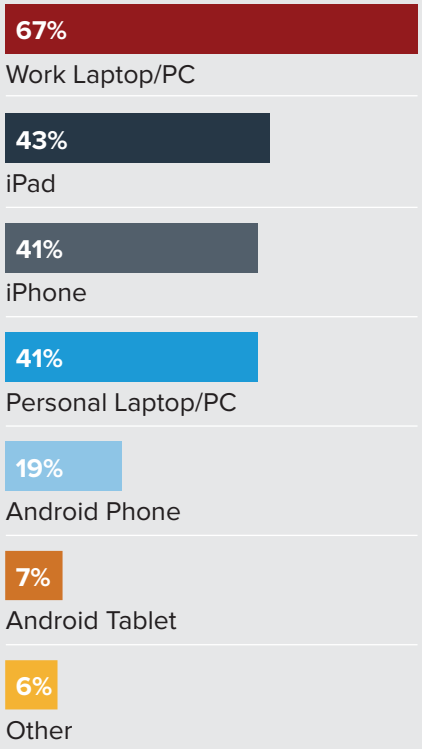


FIGURE 5

TECHNOLOGY USE

Laptops were used by the majority of board members when preparing for, conducting and following-up on board meetings.



Why organisations should be concerned

Security and confidentiality are key issues for directors, but they may not always appreciate how readily both can be undermined by their digital behaviour.

However, simply sticking with printed board packs isn't always practical – or popular. Nor does it alleviate the risk of data security. Papers can be misplaced or not stored securely. They often accumulate, rather than being shredded, or are disposed of improperly. Plus, paper board packs can be cumbersome to carry around.

Certainly, digital board documents carry their own set of risks – some of which might not be obvious. For example, directors typically have one paper reporting pack for each meeting, but a digital copy of an electronic document is created every time it is emailed, downloaded outside a secured software platform or backed up on personal drives. These copies can be cached and stored across multiple devices and systems, each of which is subject to cyber risk.

The trouble with email

The security risks associated with unsecured personal email accounts such as Gmail and Yahoo! Mail are well-established. However, just because directors use corporate email accounts for their board business doesn't mean they're immune to risk either. Increasing numbers of business email systems are being compromised through spear phishing and ransomware attacks.

Directors also risk inadvertently sending messages to the wrong recipient. One non-executive director said that for people with multiple board roles, emails sent to a work address at another organisation could compromise confidentiality.

INSIGHT:

"Some directors are on numerous boards, and having separate emails for each one is impractical. On the flip side, having private company information on another company's server is also undesirable."

COMPANY SECRETARY, LARGE LOGISTICS COMPANY

Who really controls your information?

Information transmitted by email, backed up to a third-party cloud, or saved in online file-sharing sites is no longer under a person's individual control.

It is subject to the policies of the companies that hold it, and the laws of the countries where they, and their servers, are located. Those companies are likely to put their own interests ahead of your own when faced with requests to release information to lawyers or regulators.

"The controls people put in place to safeguard against the accidental loss of their valuable information can come back to haunt them," said Dottie Schindlinger, Vice President and Governance Technology Evangelist at Diligent. "Seemingly prudent actions like backing up data to a public cloud such as Apple, Google or Microsoft effectively means your data is being managed according to the providers' policies – which might not match your company's standards. The safest bet is to make sure you understand how secure storage providers manage your board's data. Secure board software providers like Diligent ensure your company's storage and retention policies are strictly maintained, and that your company retains ownership of all your board's data."

How organisations can strengthen their practices

Take interim measures

Developing a robust boardroom response to cyber risk takes time and resources. However, there are steps that can easily be taken to help reduce the security gap in the meantime.

- Use an encrypted password vault. Three of the most common weaknesses are: using the same password across multiple locations, using passwords that are easy to guess and writing passwords down where they can be found or stolen. Encrypted password vaults provide secure storage and generate robust unique passwords.
- Ensure remote wiping is available for the board's mobile devices. Device manager settings and secure board management apps can enable smartphones and tablets to be locked and all board data erased if devices are lost or stolen.
- Stop sending board documents as email attachments. Email is notoriously hard to secure and most email platforms are unencrypted by design. There are many easy-to-implement secure messaging systems available, some designed specifically for governing bodies – find one, and implement it.

Make it easy for directors to be security-conscious

Most organisations make it easier for employees to follow security policies than to breach them. They have integrated systems, safe document storage and site blocking, overlaid with firewalls and regular security updates.

Non-executive directors often fall outside of these internal safeguards. Portability and convenience are important, particularly for directors with roles across multiple boards. Using separate systems for each organisation is generally impractical.

Governance software provides the secure external ecosystem that directors need, pairing strong protection from cyber threats with a single platform from which they can access and review board materials and communicate with each other and management.

Built-in instant messaging tailored for boards can be secured with users' biometric data to strengthen protection against unauthorised access. Deleting a message removes it fully from across the platform, with no copies retained on individual devices or in the cloud.

Board Communications Methods

INSIGHT:

Board communications often fall outside of organisational policy and oversight.

What the data revealed

It is the board's job to hold management accountable for their performance. But equally, directors must be held to account if their actions inadvertently increase the risk of cyber threats. Who is responsible for monitoring the board and providing the tools and advice they need?

According to our survey, a broad range of functions has responsibility for sanctioning and administering board communication methods. They include the company secretary, general counsel, investor relations department and administration. Frequently, multiple roles are involved.

Most of the time, it is the board itself that determines how its members should communicate. This is commonly one of the chair's responsibilities (75%), with the board's audit or risk committee involved less frequently (33%).

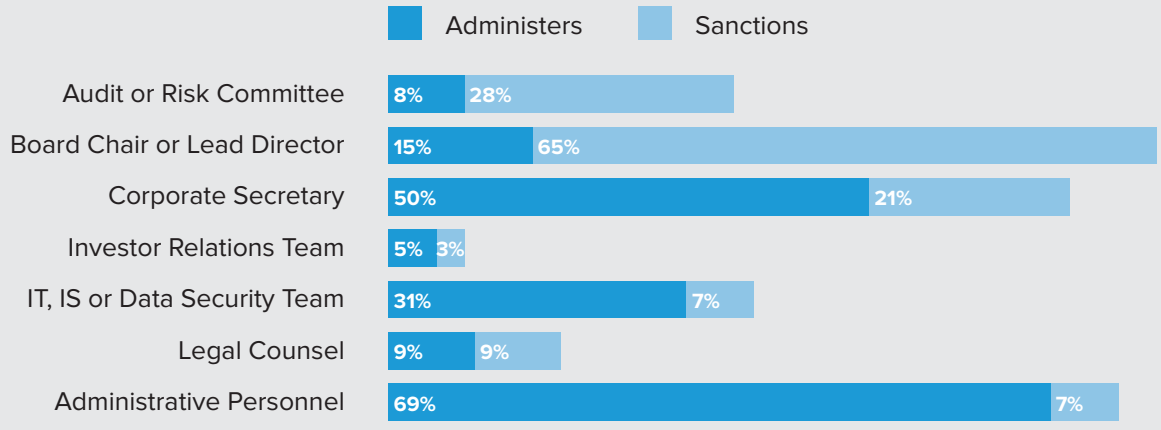
While cybersecurity is far from just an IT issue, it does need strong IT involvement. Surprisingly, only 7% of respondents say the IT or Data Security department sanctions board communication. In almost two-thirds of cases, IT or Data Security either is not involved (51%), or its role is unclear (14%).

FIGURE 6

SANCTIONING AND ADMINISTERING

Security and risk functions were only sanctioning or administering board communication in one-third of cases.

BELOW DATA SHOWS THE RESPONSES WHEN FOLLOWING GROUPS WERE ASKED: "WHO SANCTIONS AND ADMINISTERS YOUR BOARD'S COMMUNICATION METHODS?"

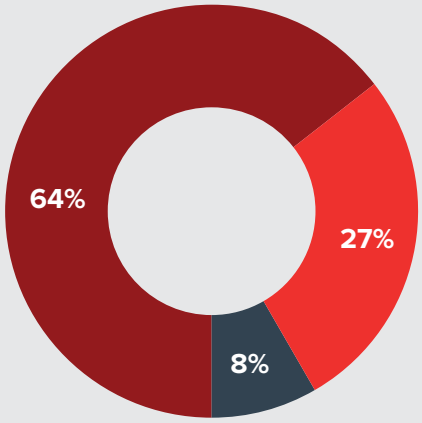


Board Communications Methods

FIGURE 7

BOARD MEETINGS

The majority of board members (64%) were satisfied with the detail they received from management in board meetings.



The right mix of summary highlights and accompanying details.

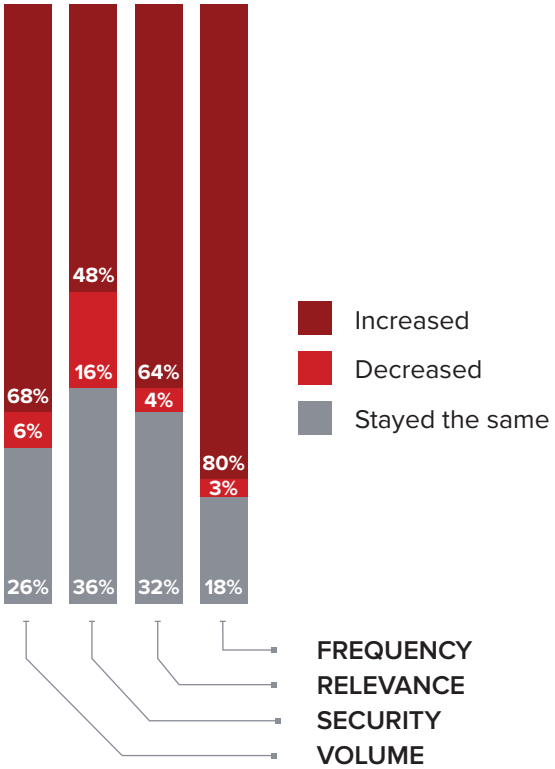
Too much detail, not enough summary highlights.

Not enough detail, too reliant on summary highlights.

FIGURE 8

DIGITAL TECHNOLOGY INFLUENCE

The rate at which the volume and frequency of management communication and information sharing has changed, outstripping the rate of growth in security.



INSIGHT:

"Cyber security is probably assumed rather than investigated."

LEGAL COUNSEL, LARGE RETAIL COMPANY

Why organisations should be concerned

Even the perception of a disconnect between directors' expectations and their own behaviour undermines trust and credibility. But its impact can be even more damaging. An organisation's cyber defences are only as strong as their weakest link.

"Organisations would be rightly concerned if they discovered there were external consultants who are given access to the most strategically significant and commercially sensitive information the company owns, and aren't required to operate within standard security procedures, nor do they receive any oversight from the IT or Data Security team. But when it comes to board members, in many cases, this is exactly what's happening," said Schindlinger.

While the chair's role is critical in fostering effective communication among directors, a question hangs over the appropriateness of their responsibility for sanctioning how that communication should occur outside the boardroom.

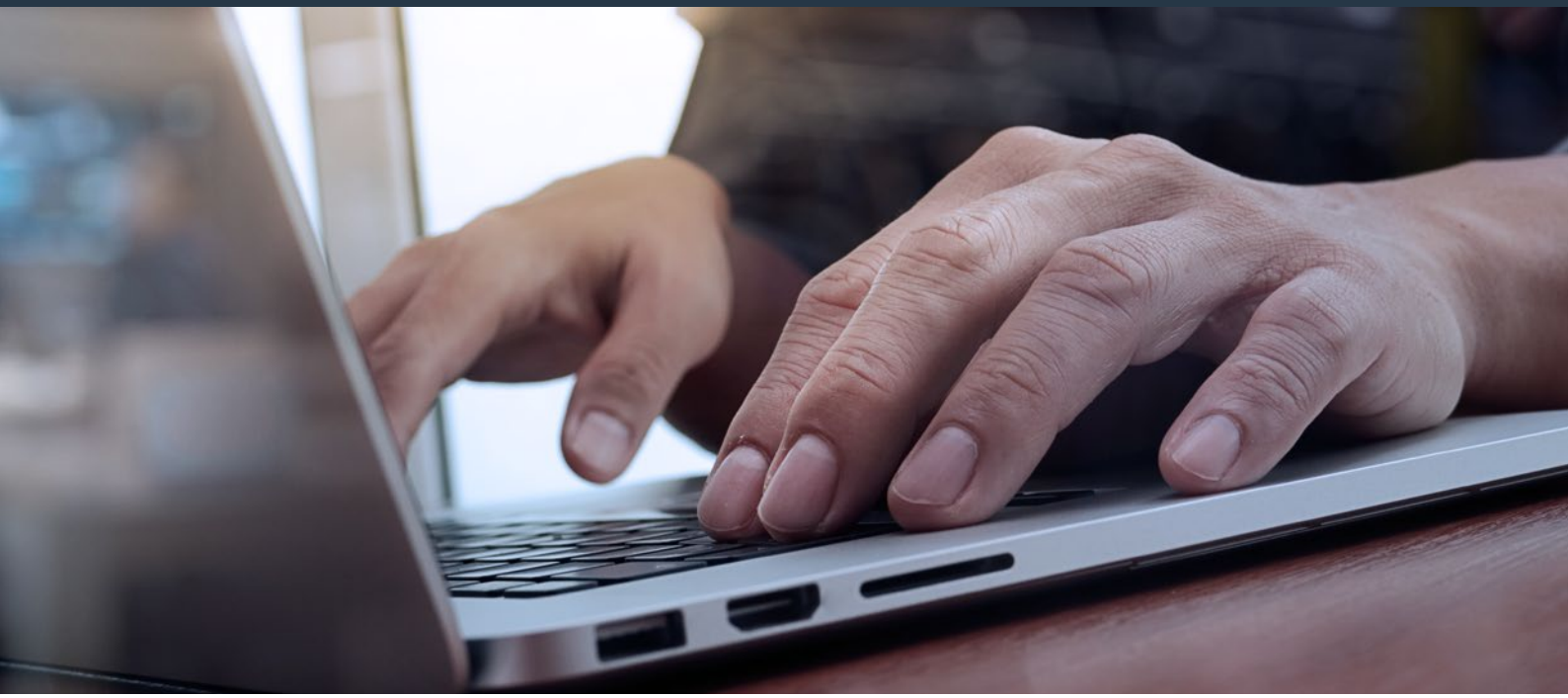
"Board chairs work closely with the company secretary and the chief executive to develop the agenda for meetings and the accompanying reports, but it's not the chair's role to prepare those things alone. The same approach should apply to board communication processes, with the chair briefing management on key principles so that they can develop robust processes underpinned by technical expertise," said Steven Bowman, Founder and Managing Director of Conscious Governance.

INSIGHT:

Similarly, fewer than one in five organisations (18%) report that IT monitors the board's adherence to corporate communications guidelines. And only a quarter of respondents (24%) say there are regular security audits of the board's communications practices. "Too many people have access to determining and administering communications."

NON-EXECUTIVE DIRECTOR, LARGE LOGISTICS COMPANY

Board Communications Methods



How organisations can strengthen their practices

Implement clear policies that include non-executive directors

Establishing strong cybersecurity policies and protocols at an organisational level raises awareness and sets consistent expectations for individual responsibilities. The challenge is that non-executive directors often fall outside of those policies and protocols.

At a practical level, organisations may grapple with how to apply controls to the highest echelons of their leadership. Including them in board-approved corporate policies is one way to meet this challenge.

“Organisations should review their security policies and ensure that non-executive directors are clearly included in the scope of policies where appropriate,” said Bowman. “Those policies should be provided to new directors as part of their induction program. In line with good governance practice, those policies should be approved by the board, and reviewed annually to keep pace with external changes.”

Development of board communication policies should not only involve directors and senior management, but also experts from risk management, governance and IT.

Take an organisation-wide approach to cybersecurity

With a fragmented approach to sanctioning and administering board communications, it is little wonder that boards are often out of step with the rest of the organisation.

Steven Bowman says that strong governance processes need to involve every level of an organisation. “Companies with continuous disclosure obligations have deep and broad processes to manage the identification and elevation of information that may require disclosure. Effectively managing cyber risk takes a similarly embedded approach across the organisation.”

INSIGHT:

Directors agree that board communications need greater security

What the data revealed

There is growing awareness among Australian directors about cyber risk. While not everyone agrees with the scale of the threat, there is universal agreement that the security of board communications can be improved.

Fewer than three in 10 respondents felt confident that their board communications were currently secure (29%).

Consensus is strong that more could be done to secure board communications, with only 4% of respondents disagreeing. Among the majority, more than half (54%) feel strongly about their view.

Those findings mirror the ASX 100 Cyber Health Check, which found that 80% of boards believe companies should do more to protect themselves from cyber threats – even if they're currently doing enough.

Forty per cent (40%) of surveyed organisations have implemented a secure board portal. However, many of those have yet to fully embed the solution, with only 57% of organisations with a board portal saying it is used regularly. Directors acknowledge this takes time and requires changes to behaviour, with some highlighting a need for ongoing training.

Despite widespread agreement that board communications require greater security, the perceived impact of a breach is surprisingly low. Only one-third of respondents (32%) believe that a leak of board communications would have a significant impact on their business.

Larger organisations believe the damage would be stronger, with over half of respondents (54%) saying it would have a significant business impact.

FIGURE 9

BOARD MATERIAL SHARING EFFECTIVENESS

Despite using fast and efficient methods to share board meeting materials, security was a concern in two-thirds of cases.

BELOW DATA SHOWS RESPONSES WHEN ASKED: "HOW WOULD YOU RATE THE FOLLOWING FACTORS WHEN DISTRIBUTING BOARD MATERIALS?"

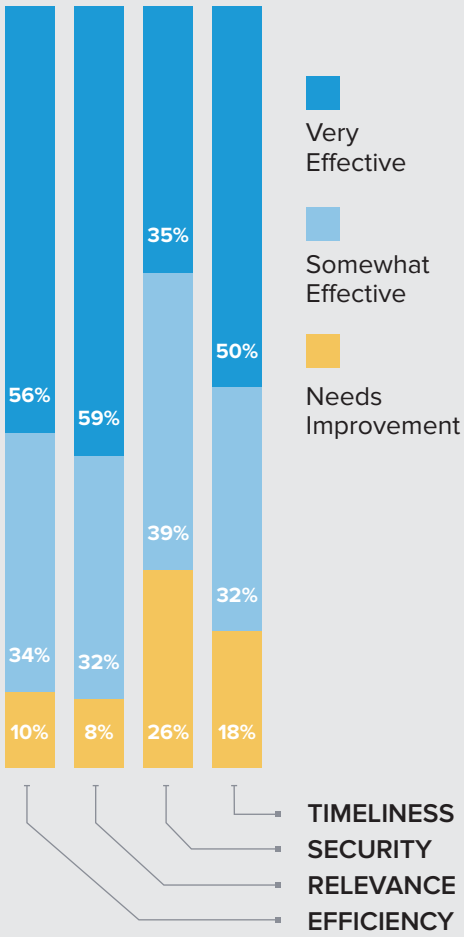
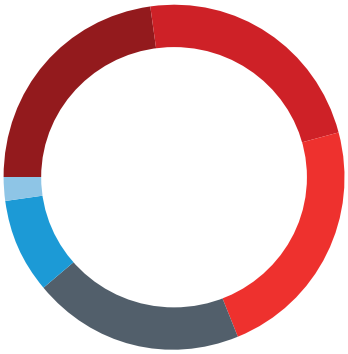


FIGURE 10

PERSONAL DEVICES

Data reveals the frequency with which board members download board books or company documents onto personal devices.

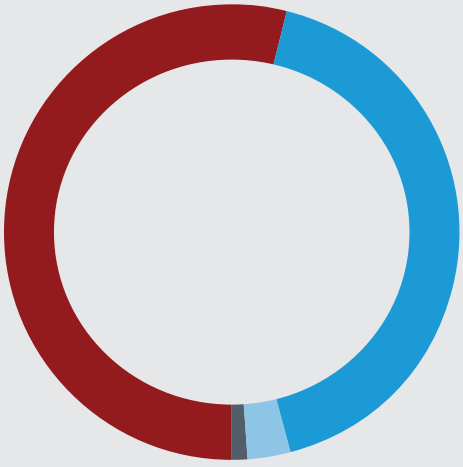


- Never **23%**
- Occasionally **23%**
- Most of the Time **23%**
- Always **20%**
- Half of the Time **9%**
- Not Applicable **2%**

FIGURE 11

RESPONSIVENESS TO FEEDBACK

The following data looks at how responsive management is to board members' feedback or requests related to enhancements to board communications.

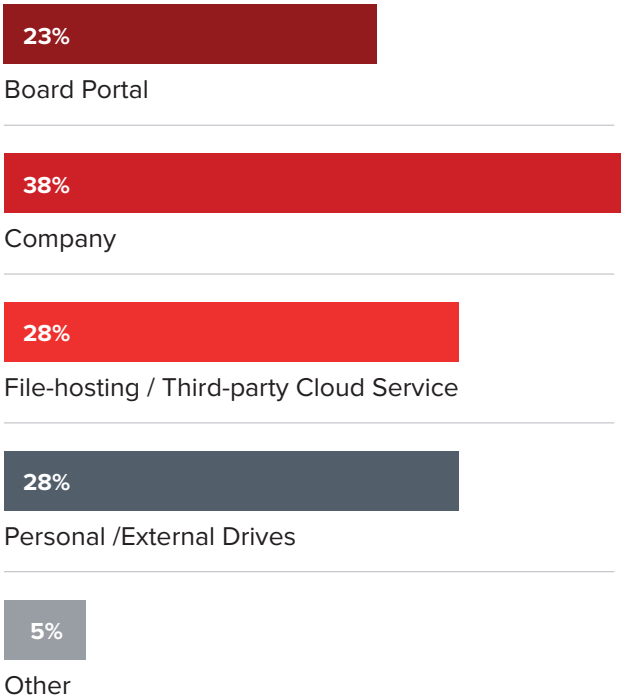


- Very Responsive **54%**
- Somewhat Responsive **42%**
- Not Applicable **3%**
- Not Responsive **1%**

FIGURE 12

COMMUNICATION MATERIALS STORAGE

Communication materials were stored in a wide variety of locations, as shown below.



Board Communications Security

Why organisations should be concerned

Not only is the scale of cyber risk continuing to grow, but also the impact of data breaches is about to get bigger.

Australia's new mandatory data breach notification laws take effect beginning in February 2018. Under the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, businesses and government agencies must promptly notify affected individuals and the Office of the Australian Information Commissioner of data breaches relating to personal information. Penalties for failure to comply are up to $1.8 million for companies and $360,000 for individuals for serious or repeated breaches.

"These changes mean it is critical for all organisations to have strong governance in place around data security, including effective board oversight," said Bowman. "Not only commercial information and intellectual property need to be properly protected, but data on their employees, customers, clients and donors."

How organisations can strengthen their practices

Prepare for cyber incidents as an inevitable part of business

Implementing strong defences is an essential part of risk management – but it only goes so far. The organisations that will emerge the strongest in the fast-changing cyber environment are those that acknowledge the increasing probability that they will be struck by a cyberattack.

"There's still a common mentality for people to say a cyber incident won't ever happen to them," said Schindlinger. "They think the odds are small, the scams are obvious, and they don't have anything worth stealing. Unfortunately, all three of those assumptions are wrong – and increasingly so."

It's not just big companies that fall victim to cyber incidents. A number of major data breaches in Australia have had widespread impact beyond the corporate sector. One of the largest occurred in 2016, when a technology provider inadvertently made records affecting more than half a million donors to a leading not-for-profit organisation public. More recently, more than 50,000 employees at a range of federal government departments and private companies were affected by a security breach involving an external contractor responsible for staff expense management.

Recognise the value of information assets

Conscious Governance's Steven Bowman says these incidents should be a call to business, government and not-for-profits that cybersecurity incidents are a genuine threat to all organisations.

"When directors don't perceive cyber risk as a significant threat, that can stop it translating to changes in personal and organisational behaviour. The idea that a board communications breach would only have a low impact on an organisation is something that should make directors sit up and take notice. It also speaks volumes about the usefulness of their current board information, which may benefit from scrutiny along with their cyber risk practices."

INSIGHT:

"I am unsure about the level of protection we have from hackers. Given we hold confidential health data on people, this presents a potential issue."

BOARD CHAIR, MIDSIZE NOT-FOR-PROFIT ORGANISATION

INSIGHT:

Directors need more information about cyber risk for effective oversight

What the data revealed

Cyberattacks are becoming more pervasive and directors are becoming increasingly alert to the organisational risks they present. The risk of external breaches and malicious cyberattacks is a common concern among survey respondents.

More than half of respondents (53%) said the move to digital file sharing by organisations has increased the risk of sensitive information being improperly handled.

Despite this, cybersecurity has yet to become a regular topic of discussion in the boardroom. A scant 15% of respondents said that their board is required to participate in cybersecurity training. For those few, annual training is most common (50%), while a significant minority undertake it as a one-off activity (22%).

Large organisations are twice as likely to require their directors to do cybersecurity training (31%), although that level is still far below ideal. Directors' feedback indicates that they see this as a key development opportunity.

FIGURE 13

DIGITAL TRANSMISSION OF BOARD MATERIALS

Frequency that hard copies are printed from files transmitted digitally to conduct board business.

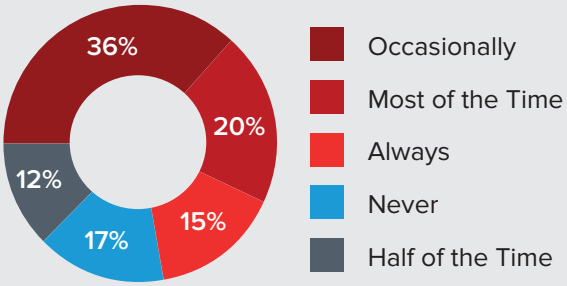
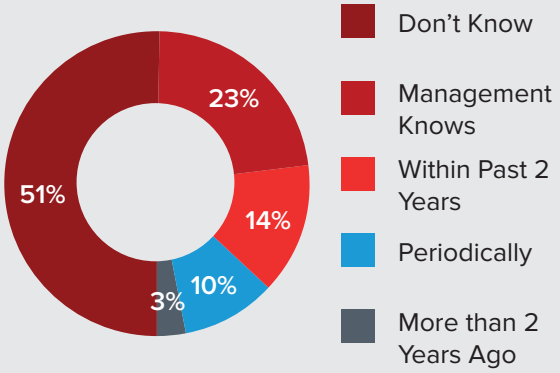


FIGURE 14

SECURITY AUDITS

Just over half of all board members were unaware if a security audit of board communications had taken place when asked.

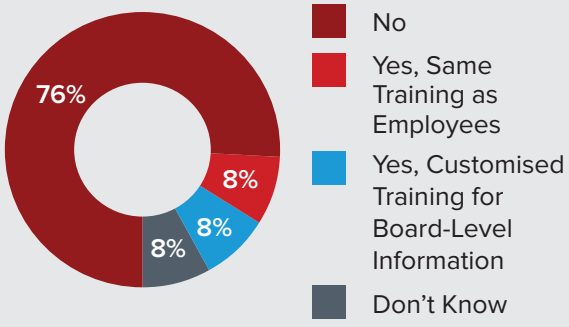


Cyber Risk Training

FIGURE 15

CYBERSECURITY TRAINING

Asking if board member were required to undergo cybersecurity training revealed that just over two-thirds of all board members had not participated in any cybersecurity training.



INSIGHT:

"The main gap is a lack of regular communication and training on cyber security risks. This can be remedied through ongoing training."

RISK MANAGER, LARGE GOVERNMENT ORGANISATION

Similarly, directors' knowledge of cyber response plans has room for improvement, especially among smaller organisations.

The extent of preparedness for a potential breach was significantly higher at large organisations, with 77% having a crisis communication plan. Those results are in line with the ASX 100 Cyber Health Check, which found that 75% of companies have considered how they would notify their customers of a data security breach.

It should serve as a warning to many smaller organisations, which may not have considered the extent of the cybersecurity risks they are facing. Hackers and other rogue operators specifically target those organisations which are unprepared, unsecured and untrained because they know their odds of success are higher.

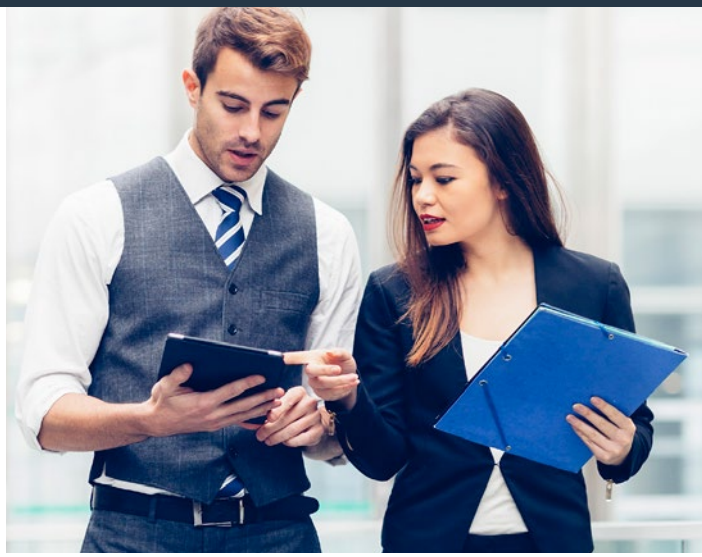


FIGURE 16

MONITORING INSIGHT

Only 18% of board members were aware that their organisation monitored security and adherence of communication guidelines.

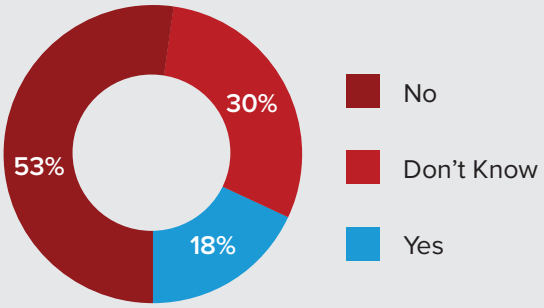
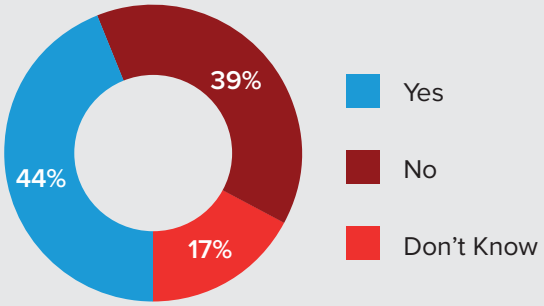


FIGURE 17

CRISIS PLANS

Less than half of all board members were aware of a crisis plan being in place in the event of a data or security breach.



Why organisations should be concerned

The pace of cyber threats is relentless, evolving as fast as – if not faster than – the technology that spawns them. In addition, the number of attempted malicious attacks is escalating. So is the cost to organisations of addressing the few incidents that penetrate their defences.

Directors acknowledge that the risk is increasing, but their responses indicate that there is much they still don't know.

Most directors aren't IT experts, nor do they need to be. But to effectively oversee risk management of cyber issues, they need sufficient knowledge and understanding of the changing digital environment and how it forms part of a wider business context. Without that insight, it is harder for them to leverage the opportunities afforded by changing technology, and organisations may face a struggle to remain relevant as others move faster.

While it's important for board conversations about cyber risk to have a strategic perspective, they can't do without a degree of operational information. It's essential for directors to know the key elements of their organisation's cyber risk protection and responses, as part of their role overseeing the adequacy of risk management.

How organisations can strengthen their practices

Make cyber risk a regular agenda item in the boardroom

Cybersecurity should become a regular component of each board meeting. Inviting your organisation's chief data security personnel to present regular briefings to the board will help reinforce the board's role in overseeing a strong cybersecurity posture and managing cyber risk across the enterprise.

"The greater transparency digital technology is bringing to the flow of information between management and directors is yet to translate to the issues of data security and cyber risk," said Schindlinger. "Directors need the right information to ask the tough questions about how these business risks are being managed."

Cybersecurity is a whole of business risk, and warrants regular reporting by senior management, Bowman said. That should involve risk and governance professionals, as well as subject matter experts in the IT function.

"It's not enough for directors to only hear from IT in an annual update and when a major new system is proposed," said Bowman. "Cyber issues should be part of integrated and ongoing reporting, just like work health and safety, legal and regulatory matters, and financial risks."

Step up director training on cybersecurity

Training is crucial to keep up with the pace of technological change. New threats are emerging constantly, which can only be met with new, and smarter, ways of working. Consistent cybersecurity practices must be applied across the entire organisation – it only takes one weak link to lead to a potential breach. Directors need to 'walk the talk' if they are to provide true leadership.

Partner with your chief data security personnel to design a training program specifically for directors and executive leaders. The training should be conducted annually at a minimum, with best practice including training that happens more frequently.

Conducting an annual tabletop exercise to simulate a breach and test the board's crisis response plan is an excellent way to zero in on areas for additional training and development for board members.

"It's far better to practice having a breach, than to learn how unprepared you really are in the middle of a cyber incident. An annual exercise – especially one that is unannounced – helps to reveal where the board needs additional training and support."

Provide broader IT training where needed

A number of respondents identified directors' broader technological literacy as an area for skills development.

"A board skills matrix can help identify targeted areas for training, as well as mapping the mix of skills on the board to the major strategic issues and risks the organisation is facing. That can be used to determine the characteristics for future board appointments and also pinpoint where external experts can contribute value," said Bowman.

Board Communications Technology

INSIGHT:

Technology is driving more communication between directors and management – but is it better?

What the data revealed

Digital technology means directors are receiving more information, more often. It's also contributing to that information being more relevant.

The vast majority of respondents (80%) agreed that there is more frequent communication between the board and management due to digital technology, while 68% said that the volume of information has also gone up. Almost two-thirds (64%) said that the relevance of information has improved.

"The greater relevance is something that's very heartening to see," said Schindlinger. "It suggests that management is resisting the temptation to use board portals as a dumping ground for data, and is mindful of the appropriate level of communication with directors. It also shows a much greater positive impact on relevance than we saw in our US report, where nearly 60% of directors found digital technology didn't make a difference in that regard."

However, the growth in information provided to the board means quality must increasingly be accompanied by brevity. Over one-quarter of respondents said they receive too much detail and not enough summary highlights. More dashboard reporting was a popular request, along with greater use of executive summaries in longer reports.

"The breadth of directors' roles has expanded over recent years, and that trend shows no signs of slowing down. Introducing dashboard reporting is one way that management can help directors oversee their increased responsibilities," said Bowman. "Dashboards provide a snapshot of the key metrics that underlie organisational performance and culture, enabling directors to monitor trends and rapidly pinpoint issues for further investigation."

INSIGHT:

"We need to strike the balance between keeping the board informed between meetings (very important) and ensuring the information provided is relevant and appropriately highlighted."

BOARD CHAIR, MIDSIZE NOT-FOR-PROFIT ORGANISATION

Most directors are positive about management's processes for board paper distribution. Half or more of respondents rated their efficiency, relevance and timeliness as effective (56%, 59% and 50%, respectively).

For the most part, there is strong dialogue between directors and management about improvements to board information. More than half (54%) said management is very responsive to their feedback and requests for changes. Only 1% of respondents said management isn't responsive to their comments.

FIGURE 18

CRISIS MANAGEMENT

Most board members were likely to be involved in a crisis management or recovery plan execution.

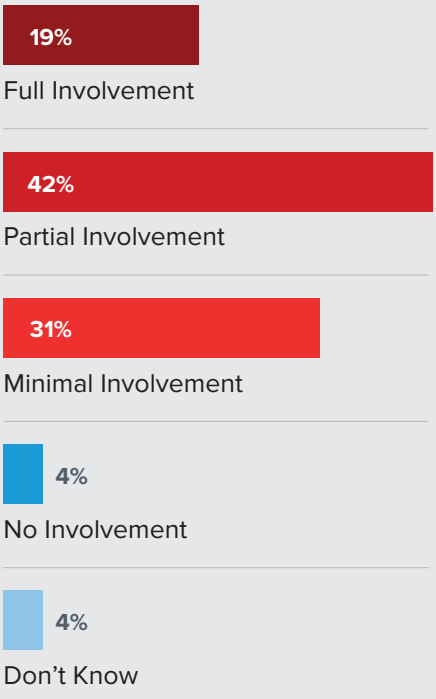


FIGURE 19

DIGITAL FILE-SHARING IMPACT

The majority of board members perceived an increase to the risk of improper handling of sensitive information since moving to digital file-sharing technologies.

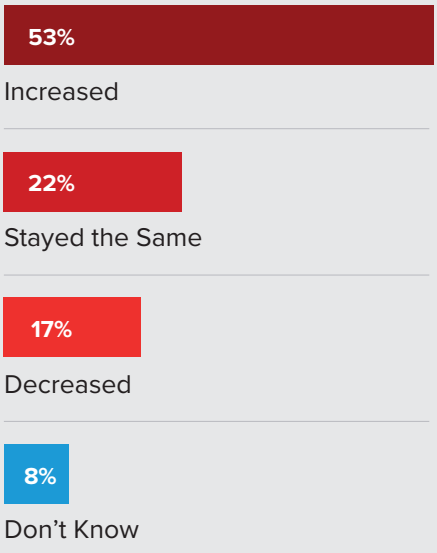
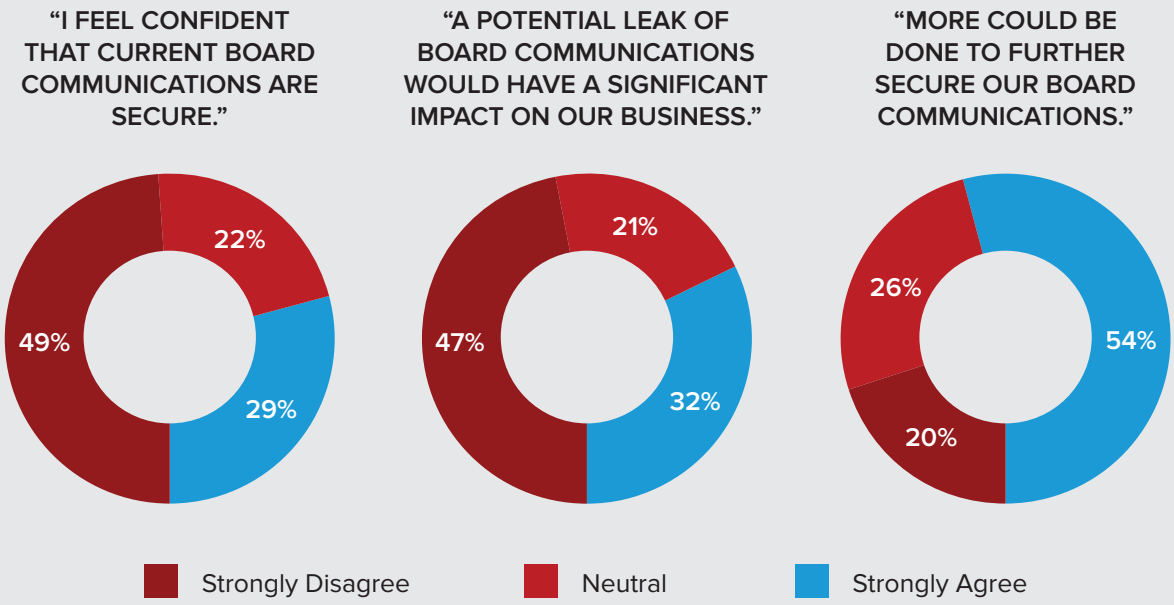


FIGURE 20

SECURITY CONCERNS

About half of all board members flagged concerns with current security measures and felt that more could be done.



Why organisations should be concerned

Boosting productivity is a significant challenge for organisations. Technology has the potential to drive productivity gains but, in many cases, it also takes away what it gives. For example, the internet brings ready access to a world of relevant information that would have taken days to collate in previous decades, but it also brings distractions that can waste time, even in the boardroom. Technology needs to be used for specific goals and its impact measured.

The increased ease of providing information to directors and the ability to keep them up-to-date in real time needs to be tempered with caution. Just because it's possible doesn't mean that it's adding value, either to directors or management.

Meanwhile, most organisations are still at the basic level of implementing technology in ways that would enhance the governance process. Simply putting board papers online doesn't necessarily transform the way the board operates. Boards can benefit from leveraging technology to automate routine business and free up time on the agenda for more strategic discussion – leading to better outcomes for the organisation.

How organisations can strengthen their practices

Provide concise, high-quality board reports

For most people, the rising tide of information we're exposed to means we become more selective. Content that doesn't grab our attention and continue to engage us is quickly bypassed.

Unfortunately for directors, they have no such luxury. They must consider all the information provided to them as part of discharging their legal responsibilities to act with care and diligence.

Technology can be part of the solution – or part of the problem. It all depends on how it's used.

"It can be tempting for management to take a 'kitchen sink' approach to board reporting for fear of leaving out something that a director then asks about," said Conscious Governance's Steven Bowman. "But too much detail can frustrate directors, overcomplicate the key issues, and distract boards with operational minutiae."

"Management needs to exercise judgement to determine the information to provide in board materials – but equally, the information that should be left out. That becomes increasingly important with more open channels of communication."

Use technology to encourage collaboration and evolve board practices

Boards derive their power from their collective authority. The most effective boards are greater than the sum of their parts, with robust discussion generating both insight and oversight.

While individual meetings and briefing sessions are often important, it is essential for board communication channels to support effective collaboration. Text messages and emails don't readily lend themselves to ongoing conversations involving multiple people.

Technology needs to supplement, not replace, the role of face-to-face meetings in communication between directors and management. Secure online messaging platforms can help directors collaborate before, during and between meetings.

"I think we're still in our infancy in terms of how boards use technology," said Schindlinger. "There's a giant difference between using technology to replicate exactly what you were already doing on paper, and using new tools to do things that weren't possible before. Using secure board messaging is one example – if directors can collaborate securely between meetings about routine matters, perhaps more time can be freed up for strategic discussions in face-to-face meetings."

Where Do We Go From Here?

INSIGHT:

"Directors in Australia and New Zealand are increasingly embracing digital technology to help them discharge their expanding set of responsibilities. Governance software is contributing to more open channels of communication between directors and management, and increasing the quality of information boards receive. While there is sound awareness of cyber risk at board level, that awareness has yet to fully translate to directors' own communication practices."

DOTTIE SCHINDLINGER, VP & GOVERNANCE TECHNOLOGY EVANGELIST, DILIGENT

No organisation can afford to be complacent in this climate of growing cyber threats. Directors are talking about cybersecurity, but that isn't enough to protect them and the organisations they serve. They need to 'walk the talk'. Otherwise, they risk being the weak link that exposes critical business information.

Board communication practices can leave organisations vulnerable to data breaches, leaks, litigation, regulatory fines, sanctions, and financial or reputational losses. Directors have an obligation to increase their understanding of the risks involved and to embrace the fact that information security must take precedence over common practices.

Directors should adhere to the same IT security protocols that apply to regular employees, including undergoing regular cybersecurity training, testing and audits.

Organisations can help by giving their directors practical tools and support to make it easy for them to embrace strong digital security habits. That can include using governance software that pairs increased convenience with strong security.

Boards and executive teams need to work together to ensure that enough time and resources are devoted to selecting, implementing and monitoring a company-supported infrastructure that features secure and convenient ways of communicating.

Diligent is dedicated to being a trusted partner that can make that vision a reality.

Methodology & Scope

The survey was conducted online from September to November 2017. Invitations to participate were sent to Governance Institute of Australia members, Conscious Governance clients and subscribers, and Diligent Corporation clients in Australia and New Zealand.

Participants were asked 18 questions across a mix of multiple choice, rating scale and free response formats. The questions related to the following four topics:

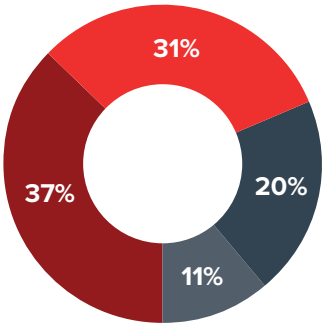
1. Board communication methods
2. Interaction between the board and management
3. Board communication behaviours
4. Cybersecurity

Respondent profiles

A total of 118 people participated in the survey, from across a variety of industries and types and sizes of organisations.

The majority of participants (63%) were directors, with the remainder made up predominantly of CEOs, company secretaries, and senior risk, legal and governance managers.

MARKET CAPITALISATION



- Not-for-profit
- Up to $20M
- $20M - $100M
- > $100M

INDUSTRY

Not-for-profit/ community services	**47%**
Health care and social assistance	**14%**
Education/training	**8%**
Industrial	**7%**
IT/professional services	**5%**
Finance	**5%**
Resources/utilities	**4%**
Consumer goods and services	**3%**
Government	**3%**
Other services	**3%**

ROLES

Non-executive director	**24%**
Executive director	**23%**
Board chair	**11%**
Committee chair	**5%**
Company secretary	**22%**
Legal/risk/governance manager	**7%**
CEO/senior executive	**6%**
Other	**3%**

Diligent