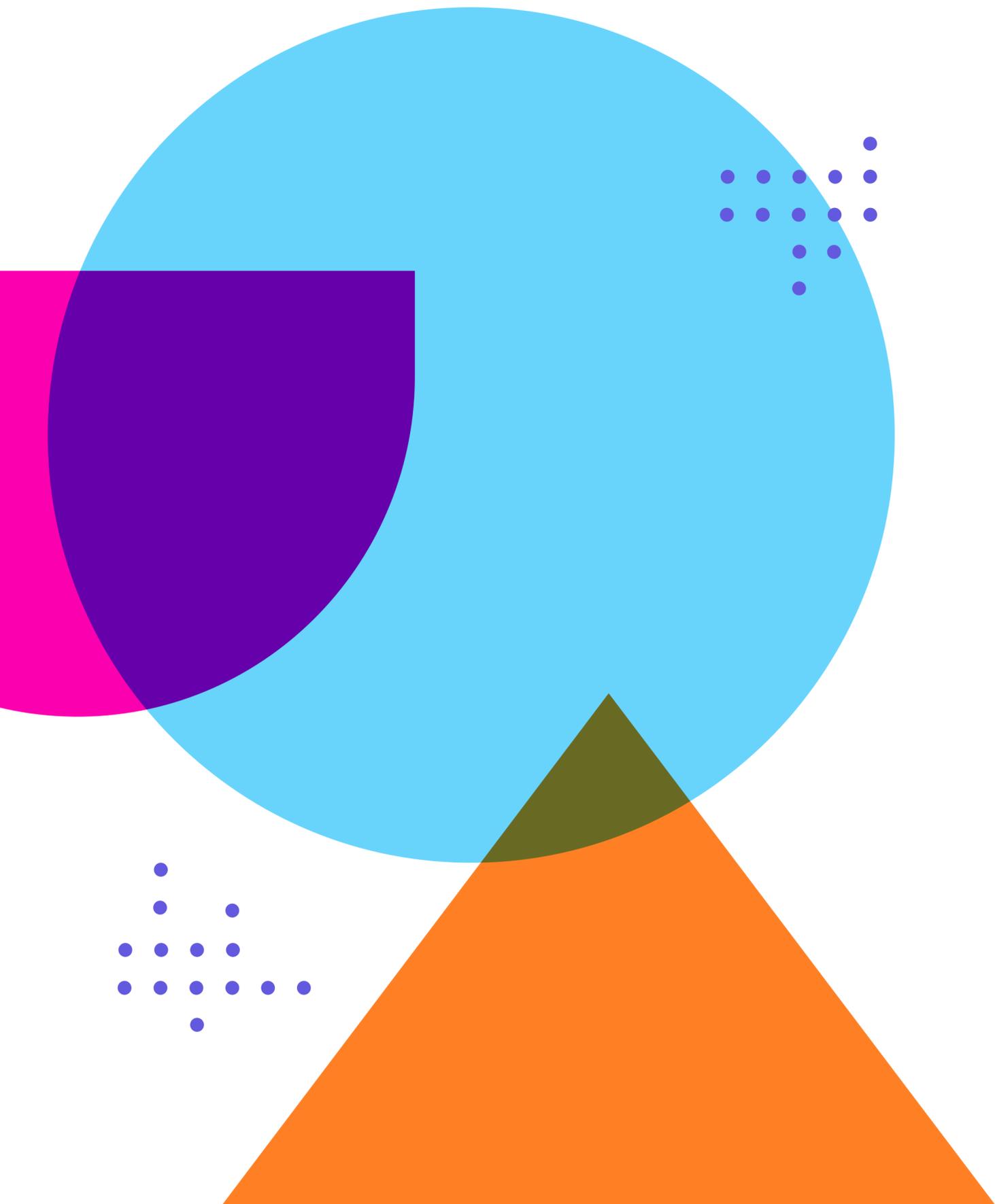


OnBoard's Guide to

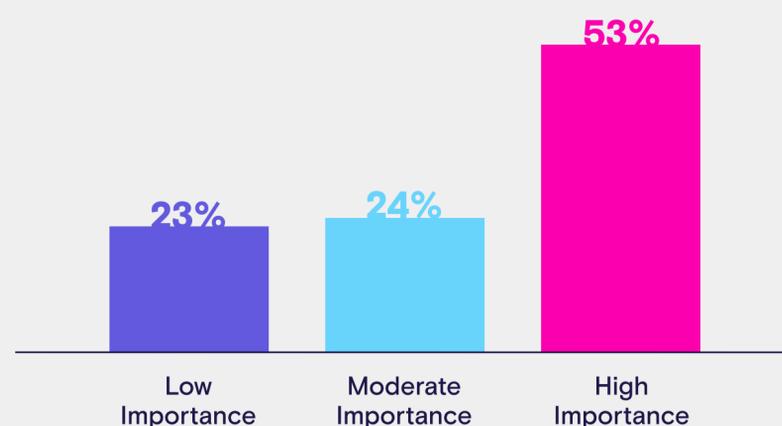
# Cybersecurity for the Boardroom



Just as millions of tiny meteoroids and other space debris shower the Earth's atmosphere each day, many organisations cope with a near-constant barrage of cyber incidents. Emboldened by anonymity and increased reliance on digital formats — especially with broad shifts to remote work and virtual meetings throughout much of the pandemic — hackers have become more prolific, relentless, and brazen in their attacks.

For boards, threats of cyberattacks or other cyber intrusions loom large in today's digital age, as they are routinely entrusted with sensitive data and information to fulfill their leadership responsibilities. Those threats seem to deepen daily regardless of industry, sector, or geographic location. A data breach involving confidential board information can devastate an organisation's reputation and cost millions of dollars in incident response, recovery, ransoms, or litigation.

## How important is cybersecurity to your organisation?



Source: OnBoard 2021 Board Effectiveness Survey

OnBoard's latest survey found that 89% of board directors, administrators and staff members see cybersecurity as a vital issue.

More than three-quarters (76%) of CIOs expect to have increased involvement with cybersecurity over the next year, and 57% indicate a need for security improvements at their organisations, according to a recent IDG Communications report. Gartner estimates 40% of boards of directors will have dedicated cybersecurity committees by 2025.

Executives and professionals who sit on boards are common targets for cybercriminals because of their access to large amounts of sensitive information.

## 40% of boards will have a dedicated cybersecurity committee by 2025.

As one example, IBM Security X-Force uncovered a global phishing campaign in 2020 that targeted more than 100 high-ranking executives.

In this report, we discuss the rising risks of cyber intrusions, their potential impacts, and tools and best practices that can help boards prevent, reduce, or otherwise mitigate these risks.

# Rising Cybersecurity Risks for Boards

Businesses and organisations around the globe underwent a rapid shift to remote work and virtual meetings with the onset of the COVID-19 pandemic in early 2020, and those formats have become permanently ingrained in their processes in the years since. This increased reliance on digital tools has led to more incidents of data breaches, phishing, malware and ransomware attacks, identity thefts and other forms of cyberattacks or cyber intrusions.

The Australian Cyber Security Centre (ACSC) found in its latest ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021 that in the 2020–21 financial year, cybercrime reports increased to 67,500, a 13% increase over the previous year. That increase equates to a cyber-attack every eight minutes instead of one every 10 minutes in 2019–2020.

Further, a higher proportion of attacks – nearly half – were categorised as having a ‘substantial’ impact. Australian organisations reported almost 500 ransomware attacks and approximately 25% affected entities associated with Australia’s critical infrastructure.

**\$33 billion**

**Cost of self-reported cyber-attacks in Australia**

The most-targeted sectors were professional, scientific and technical services (17%); health care and social assistance (14%); manufacturing (8%); education and training (8%) and state, territory and local government (7%).

**8 minutes**

**Time between cyber-attacks in Australia**

Self-reported losses for cybercrime totalled more than \$33 billion, and there were more than 1500 reports of malicious cyber activity related to the COVID-19 pandemic (approximately four per day). More than 75% of these involved Australians losing money or personal information.

The cyber threat environment is complex and evolving. The pandemic played a role as businesses extended their networks to accommodate remote working arrangements; so too did Australia’s geostrategic environment. The threat environment and critical cyber security trends included:

- **COVID-19:** Typically remote-access schemes, where criminals gain access to a computer, device or network remotely through a network connection.
- **Ransomware:** Where sensitive files are compromised and encrypted, with threats to release, withhold or destroy the information unless a ransom is paid.
- **Exploitation of security vulnerabilities:** Where criminals target vulnerabilities in unpatched or unprotected systems, devices or software, often installing malware or other exploits.
- **Software supply chain compromises:** Where criminals access a software vendor’s network and covertly modify its software, which will make customers and users vulnerable to exploits.
- **Business email compromise.** Where criminals compromise email and IT systems and identify opportunities to divert funds to their accounts, often by impersonating email accounts and their users.

- **In-portal messaging.** Enables groups and individuals to send messages and share documents within a secure platform, and automatically notifies directors via email when they have a message waiting for them in the portal.
- **Intrusion detection.** Continuously monitors the system and quickly alerts administrators of potential breaches.
- **Records security.** Allows organisations to control how they handle and store sensitive data and documents. For example, administrators lock access to the portal or specific records when needed, or automatically purge all notes and annotations when board books are archived.

Business email compromise is a significant and growing threat, which expanded considerably during the pandemic. The ACSC reported more than 4600 BECs, with more than \$81 million lost as a result. One Australian hedge fund was caught in a BEC scheme that resulted in false invoices being issued and \$8.7 million transferred to bank accounts controlled by criminals. Despite recovering most of the lost monies, the attack damaged the fund's reputation, and its key client withdrew, forcing it to go into receivership and declare bankruptcy.

The number of organisations that have fallen victim to ransomware attacks has increased exponentially since the start of the pandemic. Such attacks involve a computer criminal using malicious code to infect and paralyze computer systems, essentially holding organisations hostage until a ransom is paid.

The ACSC has observed an increase in “sophisticated, high-impact ransomware incidents against critical infrastructure organisations globally”. Further, it notes that tactics and techniques continue to evolve. This evolution demonstrates “ransomware threat actors’ growing technological sophistication and an increased ransomware threat to organisations globally”.

Australia has not been immune. The Australian Computer Society (ACS) notes that “Australia continues to be an easy target for ransomware groups who profit from poor corporate accountability and a culture of secrecy”.

Attackers often threaten to release sensitive data online unless the ransom is paid. Businesses can take many steps to reduce the threat and severity of a ransomware attack (such as keeping systems updated, using multifactor authentication and making offline data backups). Australia's security agencies strongly advise reporting incidents immediately and not paying ransoms as doing so perpetuates the ‘business model’.

Data breaches or cybersecurity incidents aren't the only risks. Boards also face risks due to unforeseen leaks. In one prominent case, leaked emails from long-time Salesforce board member and former Secretary of State Colin Powell revealed confidential details about the San Francisco cloud-based software company's M&A plans.

Staying on top of current laws and regulations is essential. Board directors are subject to e-discovery, and personal or board email accounts are “fair game” when it comes to litigation. In one recent case, a Delaware court found that corporate employees and directors negated their privilege when they sent emails to individuals at another company, making those emails discoverable to the courts.



**“Cybersecurity risk is pervasive and has only grown as we've transformed into a digital world. This has become very clear in the past 15-plus years as we've seen cyber attackers successfully infiltrate companies in all industries, even those with robust IS programs... As cybersecurity risk escalates, so too do our expectations for boards and companies to manage this risk effectively.”**

- Lisa Ropple, Practice Leader for Cybersecurity, Privacy, and Data Protection at Jones Day, speaking at the Society for Corporate Governance 2021 National Conference

The ACSC has observed an increase in “sophisticated, high-impact ransomware incidents against critical infrastructure organisations globally”. Further, it notes that tactics and techniques continue to evolve. This evolution demonstrates “ransomware threat actors’ growing technological sophistication and an increased ransomware threat to organisations globally”.

Australia has not been immune. The Australian Computer Society (ACS) notes that “Australia continues to be an easy target for ransomware groups who profit from poor corporate accountability and a culture of secrecy”.

Attackers often threaten to release sensitive data online unless the ransom is paid. Businesses can take many steps to reduce the threat and severity of a ransomware attack (such as keeping systems updated, using multifactor authentication and making offline data backups). Australia’s security agencies strongly advise reporting incidents immediately and not paying ransoms as doing so perpetuates the ‘business model’.

# Board Best Practices for Preventing Cyberattacks

Executives, management teams, and other organisational leaders to invest in education, preparation, and defense related to ransomware, data leaks, and other types of cyber incidents. Appointing a board member with cybersecurity expertise, such as a security specialist or chief information security officer (CISO), can provide a knowledgeable and informed voice on the board to help guide these discussions.

Boards should ensure they're informed about the full scope of cyber threats at their organisations, including the frequency of smaller events, and how quickly their organisations are able to respond and recover from more significant attacks.

Some best practices for mitigating cybersecurity risks include:

1

## Invest in a solid cybersecurity infrastructure

Boards should include cybersecurity as part of an organisation's full risk management framework in order to defend against potential incidents, and secure operations now and into the future.

Boards and executive leaders should support and empower CIOs and IT teams with appropriate resources and budgets to meet or exceed cybersecurity best practices – for example, backing up data, using multifactor authentication for remote work and meetings, using robust spam and phishing filters, conducting routine vulnerability checks and providing regular security training for employees.

2

## Securely manage all board materials digitally

Avoid use of printed board books, disclosures and other important materials. Printed materials can easily fall into the wrong hands, especially as more boards meet virtually or send documents in the mail. Some institutions choose cloud-based services like Google Drive and Dropbox to share materials, but these solutions can be difficult to secure. Google Drive, for example, has few options for securing files, making it a poor choice for sharing sensitive board documents. While Dropbox has more security options, vulnerabilities can quickly arise without consistent management. Both solutions lack centralised security measures that are easy to set up and implement.

While no solution is impenetrable, having a secure digital portal goes further to help stop cybercriminals looking to tap into workflow processes to extort money, disrupt operations or steal sensitive data by enabling directors to access relevant documents from a single source. Security measures for a board portal should be easy to use and should include encryption, two-factor authentication and biometric scanning devices, such as voice, fingerprint, facial or iris recognition (see following section for more details). Additionally, tracking which documents each board member accesses and shares gives boards the power to thwart insider attacks and more quickly contain them if they occur.



3

### **Set appropriate permissions**

Board members need access to the right information to fulfill their duties, but not all board members need the same level of access. For example, board members in many industries are required to annually report any personal conflicts of interest. A conflict of interest might limit a member's access to information on certain topics. Assign appropriate permissions to board members to give them access to what they need to succeed — no more and no less.

4

### **Protect meeting minutes**

Meeting minutes represent the official record of a board meeting and are an important way to protect against liability, provide evidence of decisions, and create a clear list of actions and next steps. All too often, however, meeting minutes are distributed via email attachments or a service like Google Drive or Dropbox.

While these methods are convenient, their security options can be insufficient and difficult to use in a way that consistently enhances protection. Minutes can easily end up in the wrong hands and expose confidential information that could lead to legal and financial problems, not to mention damaging the organisation's reputation.

Make it a priority to protect meeting minutes. Ensure the method you're using to compile and distribute meeting minutes is safe and secure, destroy notes used to compile them, and make minutes available to board members in a read-only format.

5

### **Require directors to communicate via a secure portal**

Personal email accounts lack adequate security for sensitive information, and even company email accounts could have vulnerabilities as they offer additional access points for phishing or other forms of cyber incidents. Ideally, all board communications would take place within a secure board platform. Such platforms typically include automated notification systems that alert directors via email when they have received a message within the portal, without transmitting sensitive information.

6

### **Wipe vulnerable apps**

Board members often access information on a number of electronic devices, from laptop computers to mobile phones. It's important to ensure these busy professionals can work while on the go, but it's also critical to insist that board business be conducted only on trusted devices.

There's always a chance that a device could be lost or stolen, or board members may replace a personal device for various reasons. According to Statista, consumers replace smartphones about every three years, and enterprise devices are replaced more frequently.

Old devices might be donated, gifted or trashed – and in all these cases, data could be compromised. Organisations should be sure to wipe any stored data from such devices, as well as from idle devices that haven't been connected to the internet within a certain amount of time, such as 90 days.

## 7

### Prepare for the inevitable

The sheer volume of cyberattacks occurring today mean the odds are high that most organisations ultimately will be affected. Developing a robust incident response plan and training on that plan in advance of a cyber incident allows boards and organisations to respond quickly and effectively when needed.

This includes identifying which data is most valuable and most likely to be targeted, and clearly defining response team roles and responsibilities, including board directors' roles. Organisations also should invest in tools to monitor the web for breaches or other vulnerabilities, and run phishing tests to ensure employees, board members, and other stakeholders are aware of what to monitor.

The Federal Trade Commission also recommends that boards build a multi-disciplinary team of stakeholders to manage cybersecurity organisation-wide, establish board-level oversight of cybersecurity efforts, and hold routine security briefings to stay informed on the latest risks affecting their organisations.

## Choose a Board Portal to Improve Cybersecurity and Mitigate Risk

Cyberattacks, data breaches, and other cyber incidents can lead to costly consequences. The increased complexity and frequency of attacks has dramatically elevated the importance of the board's role in overseeing cybersecurity efforts. Boards and other organisational leaders should act now to mitigate cybersecurity risk.

Board management portals, such as OnBoard, provide a number of capabilities and benefits to help organisations streamline and protect essential board information and processes. By providing universal security measures and a single access point for all board business, these portals reduce potential vulnerabilities. They also allow organisations to better control the flow of data, documents, and other information, and reduce the likelihood of accidental leaks.



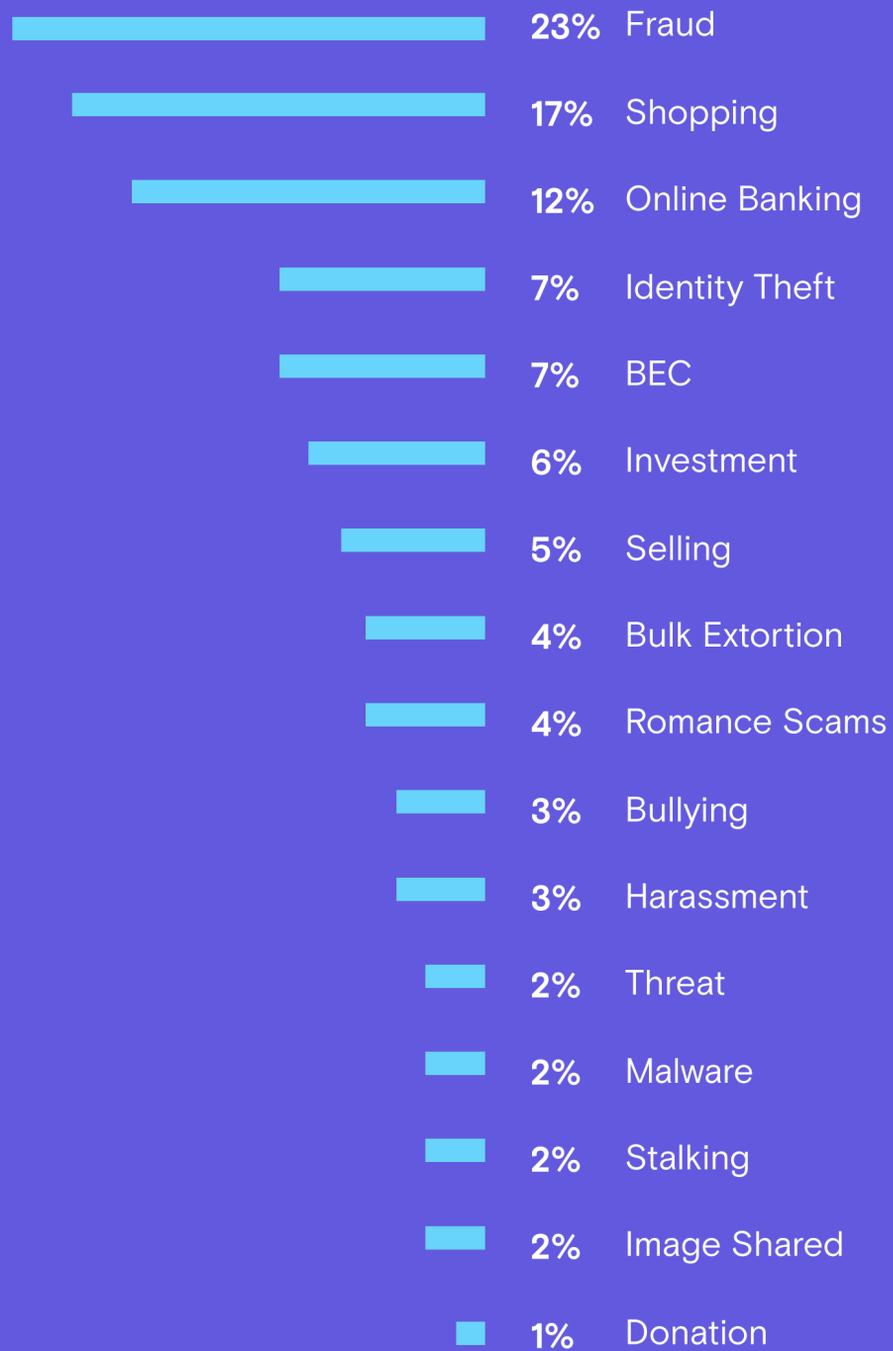
## What to seek in selecting a board management portal

- **Cloud-based security:** Microsoft Azure is widely accepted as the gold standard in cloud security. It includes full disaster recovery and active geo-replication to store and protect data at geographically distributed data centers.
- **Granular permissions management:** Organisations should have full control over assigning user and group permissions to limit who has access to specific documents or information within the portal.
- **Multi-factor authentications.** Requiring users to verify their identity using two or more methods provides greater protection against would-be hackers.
- **Biometric security.** Allows users to login using touch or facial identification.
- **Remote wipe capabilities.** Organisations can remotely delete sensitive data from mobile apps should devices be lost, stolen, or replaced, or if they appear to no longer be in use for a predetermined period, such as 90 days.
- **In-portal messaging.** Enables groups and individuals to send messages and share documents within a secure platform, and automatically notifies directors via email when they have a message waiting for them in the portal.
- **Intrusion detection.** Continuously monitors the system and quickly alerts administrators of potential breaches.
- **Records security.** Allows organisations to control how they handle and store sensitive data and documents. For example, administrators lock access to the portal or specific records when needed, or automatically purge all notes and annotations when board books are archived.

Boards also should be selective in seeking a board management solution provider. Some things to search are whether a provider has SOC 2 Type II certification, ISO 27001 certification and industry-specific certifications. Solution providers should provide documentation on their insurance information, recent audits, and the security measures included with their products. They also should have a robust “Trust Center” with documentation on important data/breach/disaster recovery processes, including their disaster plan for major security events or other disasters.

Regardless of size or cost, cybersecurity incidents have the potential to wreak havoc on an organisation’s reputation, tarnishing the trust it’s worked so hard to earn. Regaining that trust can be challenging. Boards should be actively involved in establishing their organisation’s priorities around cybersecurity.

## Cybercrime reports by type for financial year 2020–21



ACSC Cyber Threat Report  
1 July 2020 to 30 June 2021

Cybercrime reports by type for financial year 2020–21 | Note: Percentages rounded to the nearest whole number.

The increasing frequency and severity of cyber incidents is unlikely to abate anytime soon. The ACSC's report shows the diverse range of potential threats facing both individuals – including business managers and company directors – and organisations. Directors should seek to build their knowledge about cybersecurity issues, and be forthright and willing to ask probing questions. Boards can work to preserve their organisations' critical data and operations by ensuring they are prepared and able to respond according to best practices.

**Onboard's best-in-class security capabilities ensure every customer, large or small, benefits from an enterprise-grade, industrial-strength, penetration-tested architecture**



Learn how OnBoard seamlessly blends best-in-class cybersecurity with intuitive ease-of-use for more informed and more effective board meetings.

[LEARN MORE](#)