OnBoard's Guide to

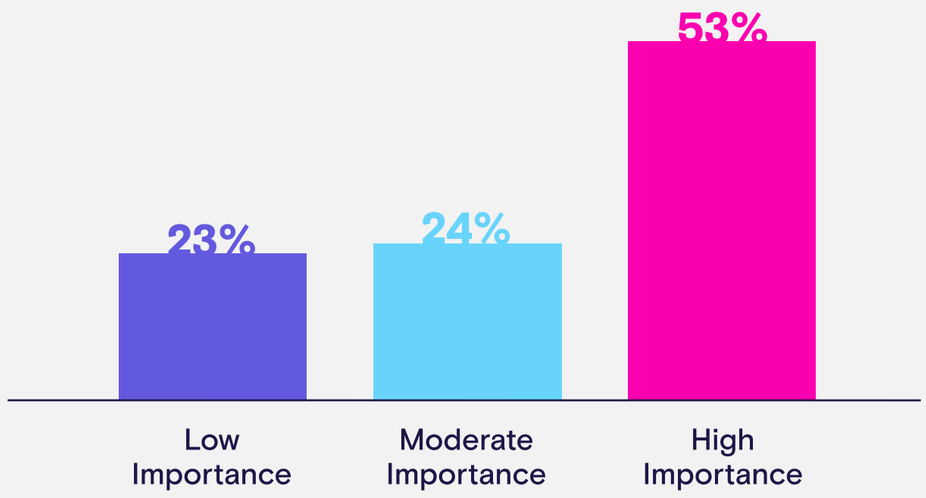
Cybersecurity for the Boardroom

OnBoard
BOARD INTELLIGENCE PLATFORM

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 Cyber Security Breaches Survey 2021 notes that modern organisations have significant digital exposures, including online bank accounts; social media pages or accounts; personal information about customers; network-connected devices; and the ability for customers to transact online.
According to the Survey, more than nine in ten UK businesses (96%) and charities (88%) have at least one of the abovementioned exposures. Most have more than one: six in ten businesses (59%) and half of charities (50%) have three or more.

These exposures can lead to security incidents (breaches or attacks). Four in ten businesses (39%) and a quarter of charities (26%) reported cyber security incidents in 2021. Among charities, seven in ten (68%) with incomes exceeding £5 million and half (51%) with income exceeding £500 000 recorded incidents.

70% of Businesses
(and 70% of charities)
Reported more than one cyber incident in 2021

The Survey notes that, the number of businesses reporting incidents fell slightly from 2020 (from 46% to 39%), while the charities result remained unchanged (26%). The reduced business result may be due to several factors, including COVID-19-related reductions in trading activity. There is also some evidence indicating that criminals focused more attacks on mid-sized businesses, which are less likely to detect or report incidents.

68% of high-income charities
(income £5 m or more)
(and 51% with income £500 k or more)
Reported cyber incidents in 2021

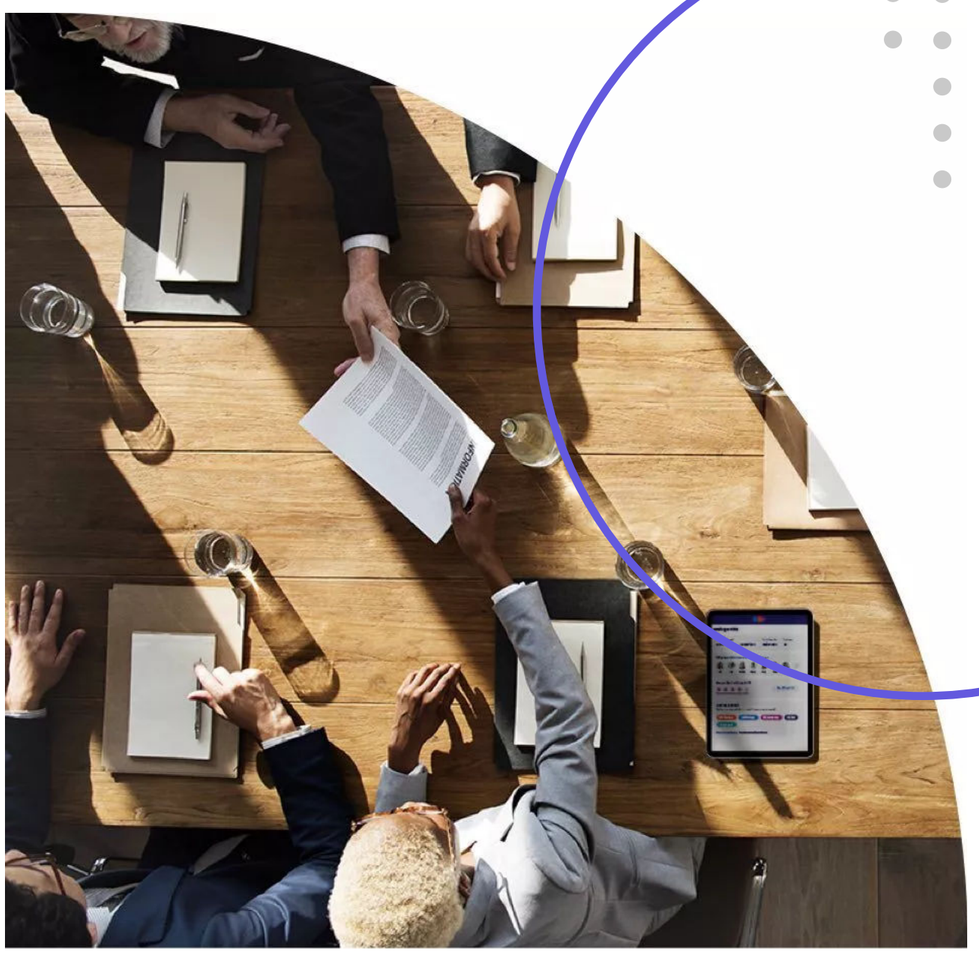
These two factors have likely compounded each other. As businesses extended their networks to facilitate remote working, new vulnerabilities likely arose, yet “the emphasis on more immediate service continuity needs at the outset of the pandemic has left a backlog of cyber security tasks and projects in some organisations. This has led to cyber security teams facing competing priorities”, the Survey says. The Survey further notes that “end users may be less receptive to any cyber security approaches that involve locking down user activity, and instead expect IT and cyber security staff to place more emphasis on functionality and flexibility.”

With majorities of both businesses (79%) and charities (70%) reporting more than one incident, and nearly half both of businesses (49%) and charities (44%) reporting attacks at least monthly, the problem remains significant.

Outcomes include temporary loss of access to files or networks; website, or online services taken down or made slower; software or systems corrupted or damaged; money stolen; and loss of access to relied-on third-party services.

Yet the Survey does contain some good news; three-quarters of businesses (77%) and seven in ten charities (68%) said cyber security was a “very” or “fairly” high priority for senior management.

Crucially, there is an awareness of governance’s important role in cyber security; two-thirds of businesses (64%) and six in ten charities (61%) update senior managers about cyber security at least once a year; four per cent of each are updated every time there is a breach.



Jeremy Fleming, head of the Government Communications Headquarters (GCHQ) noted in an address to the 2021 Cipher Brief Threat Conference that ransomware is proliferating:

“We’ve seen twice as many attacks this year [2021] as last year in the UK … Criminals are making very good money from it and are often feeling that that’s largely uncontested.”

“It’s not rocket science to defend against [ransomware]”, he said. “If you do fairly basic cyber security, if you are really clear at an organisational level about things that you need to protect and if you are very diligent … then you’re going to protect yourselves.”

“Back up your data, make sure you’ve got your admin right, sorted out, make sure your passwords are properly protected exercised all of this, work out where your thresholds are have thought in advance how you would respond if you were approached for ransom, all those sorts of things, it’s just basic stuff.”

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

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.

- M**ulti-factor authentication**s. 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.

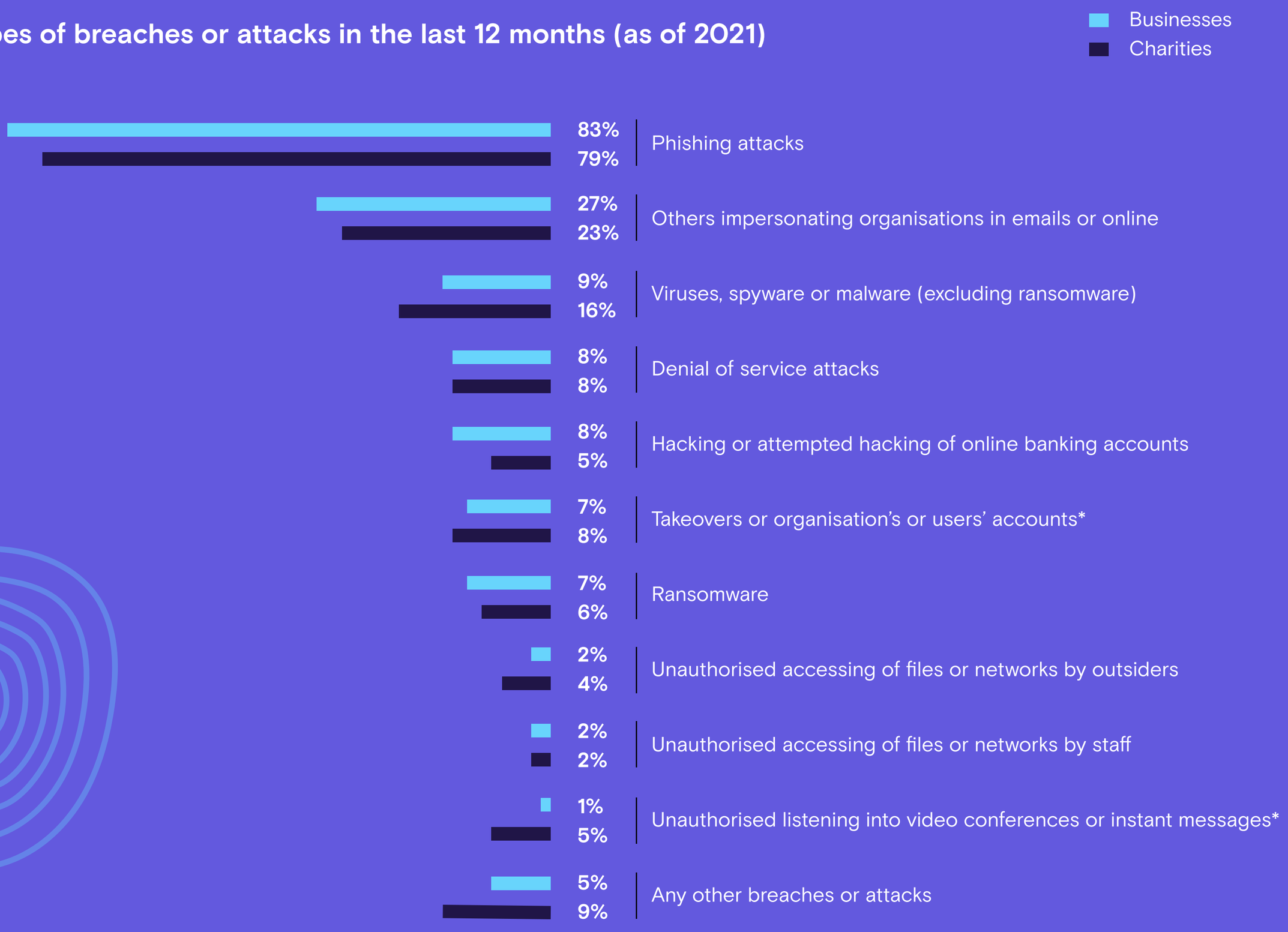
- **Intrusion detection.** Continuously monitors the system and quickly alerts administrators of potential breaches.

- **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.

Types of breaches or attacks in the last 12 months (as of 2021)



Cyber Security Breaches Survey 2021 | Bases: 654 businesses that identified a breach or attack in the last 12 months; 183 charities.
*New codes for 2021

Percentage that have identified the following types of breaches or attacks in the last 12 months, among the organisations that have identified and breaches or attacks.

The increasing frequency and severity of cyber incidents is unlikely to abate anytime soon. The Cyber Security Breaches Survey 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