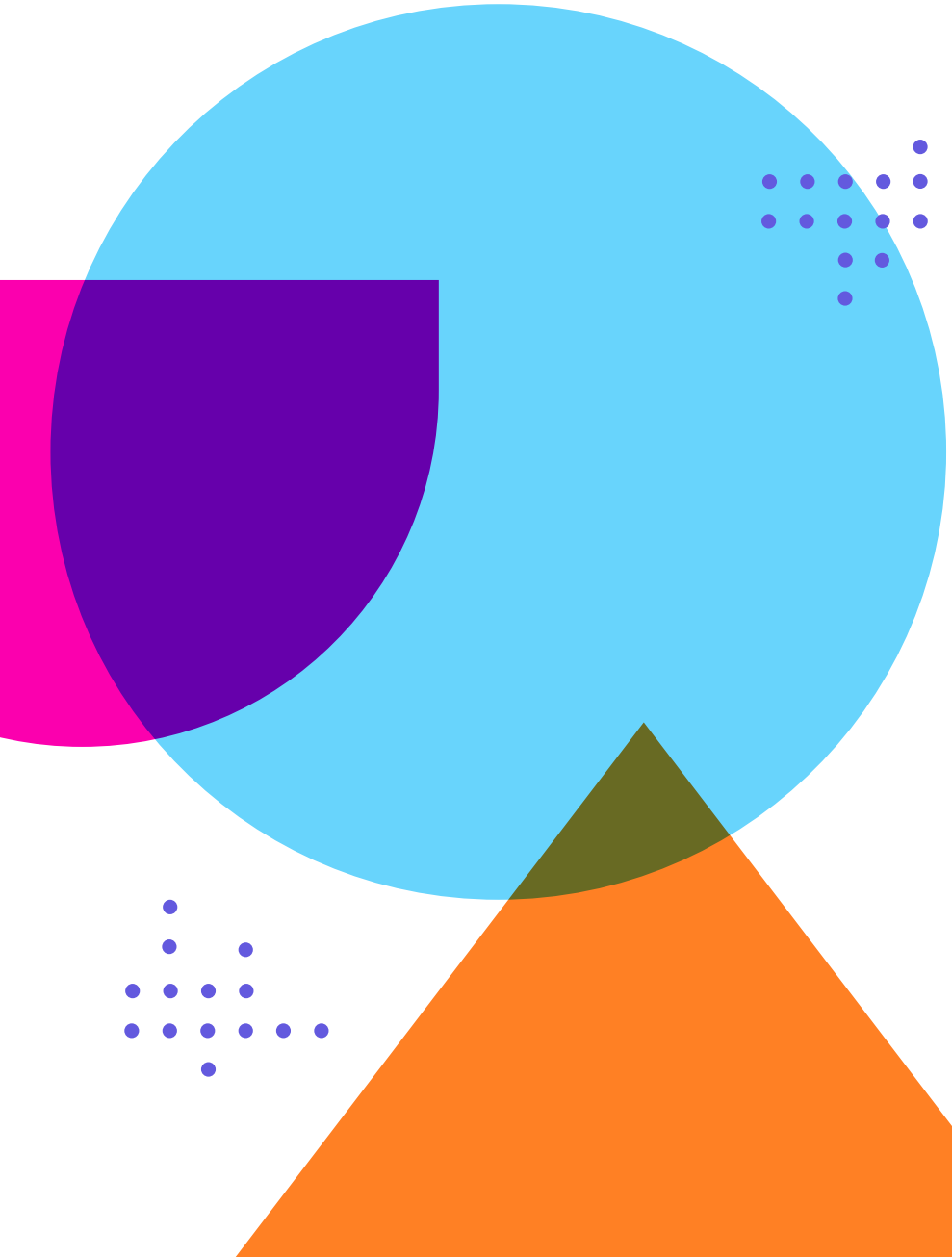
OnBoard's Guide to

Cybersecurity for the Boardroom

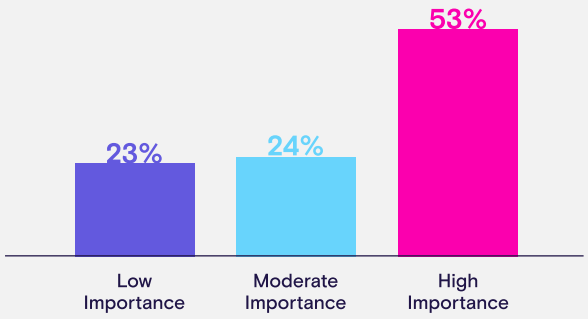


OnBoard
BOARD INTELLIGENCE PLATFORM

Just as millions of tiny meteoroids and other space debris shower the Earth's atmosphere each day, many organizations 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 organization's reputation and cost millions of dollars in incident response, recovery, ransoms, or litigation.

How important is cybersecurity to your organization?



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 organizations, 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 organizations 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.

Complaints of internet crimes jumped nearly 70% from 2019 to 2020, with reported losses exceeding $4.2 billion, according to the FBI's Internet Crime Report 2020. Such attacks come at a high cost for organizations, both in terms of time, resources, and other repercussions.

The average cost of data breaches for companies worldwide rose to an all-time high of $4.24 million per incident in 2021, as security was unable to keep pace with brisk adoption of digital tools, according to a recent report from IBM Security and the Ponemon Institute.

The cost was higher for the estimated 20% of data breaches that involved remote work, with an average cost of $4.96 million per incident compared to $3.89 million for cases where remote work wasn't a factor.

That same analysis of breaches at more than 500 organizations found that companies in the U.S. had the highest cost per incident compared to those in other countries, at an average of $9.05 million per incident. The average time to detect and contain a data breach was 287 days.

$9.09 Million

Average cost of data breach in the US

287 Days

Average time required to detect and contain data breach

According to Verizon's 2021 Data Breach Investigations Report, outsiders were responsible for 70% of all breaches. Breaches take many forms, including human error, compromised credentials, abuses of privilege, or engineered cybercrime on known software vulnerabilities, such as remote meeting tools. There may be malicious intent involved, such as a hacker or disgruntled employee or former employee trying to sabotage or disrupt company operations. In one case, a vengeful former employee deleted more than 20,000 files, 3,500 directories, and more than 21 gigabytes of data from shared files at a New York-based credit union, including everything from mortgage loan applications to board meeting minutes.

While a majority of cyberattacks continue to target industries such as health care, finance, and government, organizations of all sizes across all sectors are experiencing attacks. Attacks on U.S. schools, for example, are becoming more frequent and more significant. In 2021, hackers posted nearly 26,000 files stolen from Florida's Broward County Public Schools' servers after the district — the sixth-largest school district in the country — refused to pay a $40 million ransom. In early 2022, Albuquerque schools were forced to cancel classes for two days after a ransomware attack blocked access to the district's student database. Similar attacks have disrupted classes in other districts nationwide, including school systems in Maryland, New Jersey, and Wisconsin.

The number of organizations 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 organizations hostage until a ransom is paid.

The NACD estimates the total number of ransomware attacks in 2021 likely is much higher than the 4,000 company breaches reported on ransomware sites, as many companies never publicly report incidents. The association predicts ransomware groups "will become more brazen and sophisticated in 2022," and cause increasing levels of disruption, cost, and liability for boards of all sizes. Such attacks once primarily involved threats of permanent encryption of an organization's data, but the coming months likely will see an increase in multipronged threats to exact compliance from victims — such as tying events to a public offering or merger, publishing victims' names and confidential information, or data sell-off auctions.

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 organizational 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 organizations, including the frequency of smaller events, and how quickly their organizations 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

The NACD recommends that boards include cybersecurity as part of an organization'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 centralized 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 organization'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.

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:** Organizations 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.** Organizations 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.

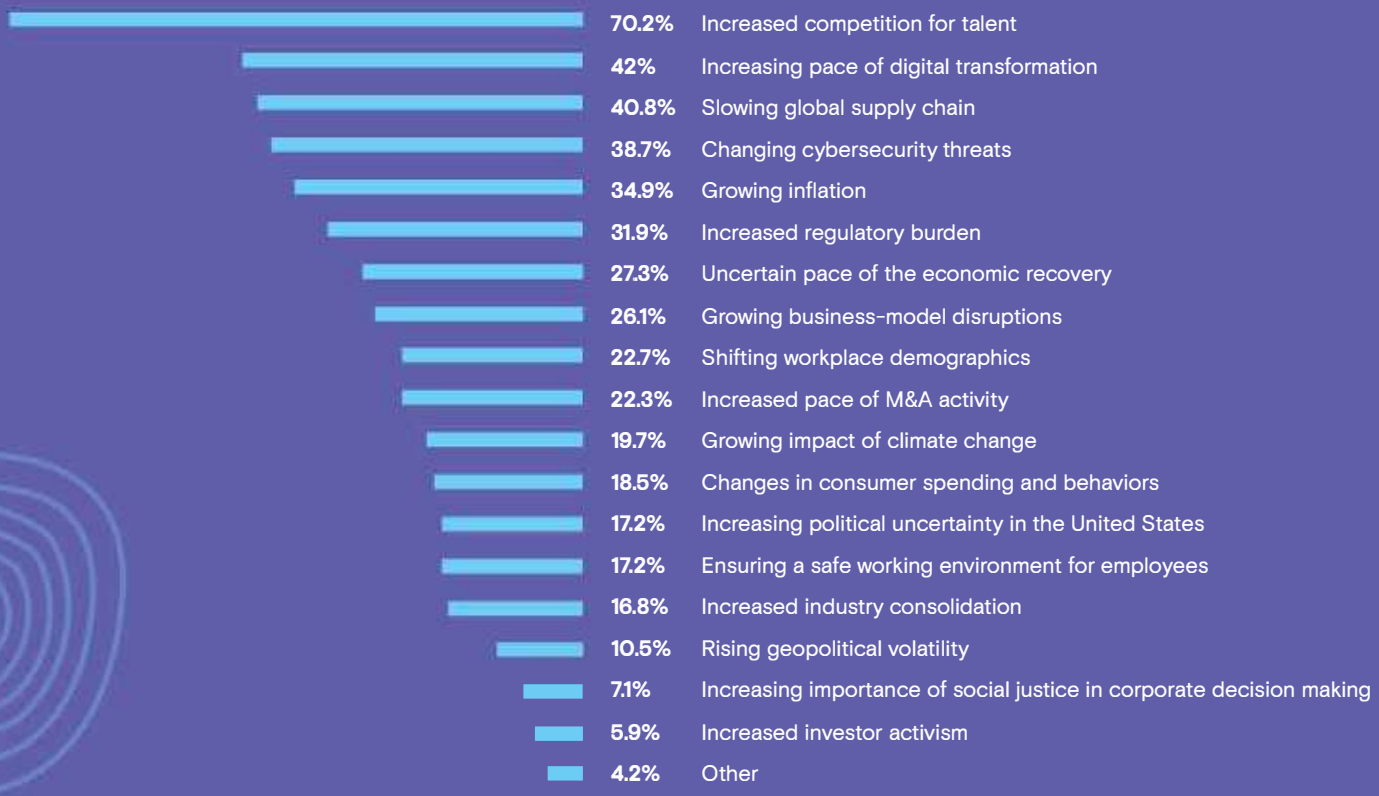
- **Intrusion detection.** Continuously monitors the system and quickly alerts administrators of potential breaches.

- **Records security.** Allows organizations 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 (e.g., HIPAA compliance for health care). 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 organization’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 organization’s priorities around cybersecurity.

What five trends do you foresee having the greatest effect on your company over the next 12 months?



2022 NACD Trends and Priorities Survey, n=238

The increasing frequency and severity of cyber incidents is unlikely to abate anytime soon. According to the NACD's trends report for 2022, cybersecurity is the fourth-most concerning challenge for corporate directors over the next 12 months. 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 organizations' 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