



REMOTE WORKING PRACTICES: A CYBERSECURITY CONCERN FOR BOARDS





The COVID-19 crisis has led to the widescale adoption of remote working practices in a way that business-continuity plans had not envisioned.

The migration to remote working was sudden and immediate, with little room for trial, study, and planning. This has brought about a new set of risks and challenges.

Cybersecurity is one of them.



THE HEADLINES

- 📰 [Interpol reveals “alarming rate” of cyberattacks during COVID-19](#)
- 📰 [500,000 Zoom accounts hacked and being sold on the dark web](#)
- 📰 [COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes](#)
- 📰 [Cybercrime ramps up amid coronavirus chaos, costing companies billions](#)
- 📰 [Why Covid-19 is a gift for cyber criminals](#)

REMOTE WORKING IS CHANGING THE LANDSCAPE OF CYBER-RISK MANAGEMENT

Cybercriminals now have an "expanded landscape of attack" as organisations shift to remote working

- + Remote workers are being targeted as they are deployed outside of the organisation's usual IT security perimeters.

Use of personal devices ("Bring Your Own Device")

- + Data interception becomes a risk as remote workers use their own devices for business-related purposes.

Easier access to network traffic

- + Remote workers are made vulnerable as they work with less-than-secure applications, hardware, and network connections (e.g. home/public WiFi).

Lack of social control

- + Click-through rates for phishing emails will increase if employees no longer maintain a "human protection shield" by asking coworkers about suspicious emails and calls.



REMOTE WORKING IS CHANGING THE LANDSCAPE OF CYBER-RISK MANAGEMENT

Potential delays in cyberattack detection and response

- + The detection of malicious activities will be more difficult and the response will be more complicated.

An increase in cybersecurity spending

- + Companies will continue to prioritize short-term spending on security for remote workers .
- + There has been a strong demand for endpoint security systems (i.e. securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from malicious actors and campaigns).

Social engineering ploys are on the rise

- + Attackers attempt to gain information, money, or access to protected systems by tricking legitimate users.
- + Email phishing campaigns "use" identities of health, aid, and other benevolent organisations.
- + Email scams have been targeting executives to move money to fund vendors, operations, and virus-related response activities.



POPULAR TYPES OF ATTACKS



Corporate/Cyber Espionage

Stealing of classified, sensitive data or intellectual property to gain competitive advantage.



Hacktivism

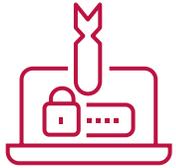
Gaining unauthorized access to/ exposing data for politically or socially motivated purposes.



State/Nation-Sponsored Cyberattacks

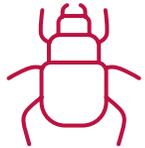
Stealing of sensitive data for political, commercial, or military interests. For example, probing for and exploiting national infrastructure vulnerabilities, gathering intelligence or exploiting money from systems and people.

REMOTE WORKING: COMMON METHODS OF CYBERATTACKS



Distributed Denial of Service (DDoS)

- + Hackers attempting to make websites or computers unavailable by flooding or crashing the website with too much Internet traffic.



Malware

- + Blanket term for viruses, worms, trojans and other harmful programs that hackers use to wreak destruction and gain access to information.
- + "Ransomware": form of malware that encrypts a victim's files. The attacker then demands a ransom to restore access to the data.



Zero-Day Exploit

- + A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched.
- + An exploit that attacks a zero-day vulnerability is called a zero-day exploit.
- + Discovered before security researchers/developers became aware of vulnerability (and before they can issue a patch).



REMOTE WORKING: COMMON METHODS OF CYBERATTACKS



Phishing

- + Targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data.



Spear phishing

- + Bespoke emails being sent to well-researched victims. It is hard to spot these without close inspection and difficult to stop with technical controls alone.



Whaling

- + "Reeling in the big fish" .
- + It involves scouring technologies for loopholes and opportunities for data theft.
- + Hackers exploit specific networks where powerful individuals work or store sensitive data.



POTENTIAL IMPACTS OF CYBERSECURITY FAILURES

Financial Cost

- + Data breaches leading to the exposure of personal information can run into the millions (USD).
- + [How a Ransomware Attack Cost One Firm £45 million.](#)

Reputational Damage

- + Leading to loss of business which in turn impacts the company's valuation.
- + [Capital One Shares Dive After Data Breach Affecting 100 million.](#)

Legal Ramifications

- + Potential exposure to lawsuits due to the failure to safeguard information.
- + [Facebook Settles Data Breach Class Action Lawsuit.](#)

Regulatory and Compliance Violations

- + Potential penalties (e.g. violation of the E.U.'s General Data Protection Regulation [GDPR], and the California Consumer Privacy Act [CCPA]).
- + [After a Data Breach, British Airways Faces Record Fine.](#)



WHAT DOES THIS MEAN FOR ORGANISATIONS?

"Cybercrime is the greatest threat to every company in the world."

- Ginni Rometty, Executive Chairman of IBM

"...Criminals are taking advantage of the increased security vulnerabilities arising from remote working to steal data, generate profits and cause disruption."

- Interpol, "COVID-19 Cybercrime Analysis Report August 2020"

"Business leaders have a heightened responsibility to set clear expectations about how their organizations are managing security risk in the new work environments...."

*"It's important that **messages on security come from the very top of an organization, and that good examples are set from the start....**"*

- World Economic Forum, "How to protect yourself from cyberattacks when working from home during COVID-19 2020"

In a nutshell

A wake-up call for business leaders to address the security risks and impacts of remote working practices for employees.

Business leaders—and corporate boards, for that matter—set the tone for the adoption of secure remote working policies and practices.

SECURITY IMPLICATIONS OF REMOTE WORKING PRACTICES FOR COMPANY BOARDS

Prime targets of attacks due to the sensitivity of information they share, deal with, and exchange

- ✓ Prevent becoming “whaling” victims

Must now adopt a “security-first” mindset towards remote working practices. Use encrypted (or better, end-to-end encrypted) services for board communications such as:

- ✓ Virtual meetings
- ✓ Instant messaging/video calls
- ✓ Secure email

Must ensure all board directors practice good digital hygiene

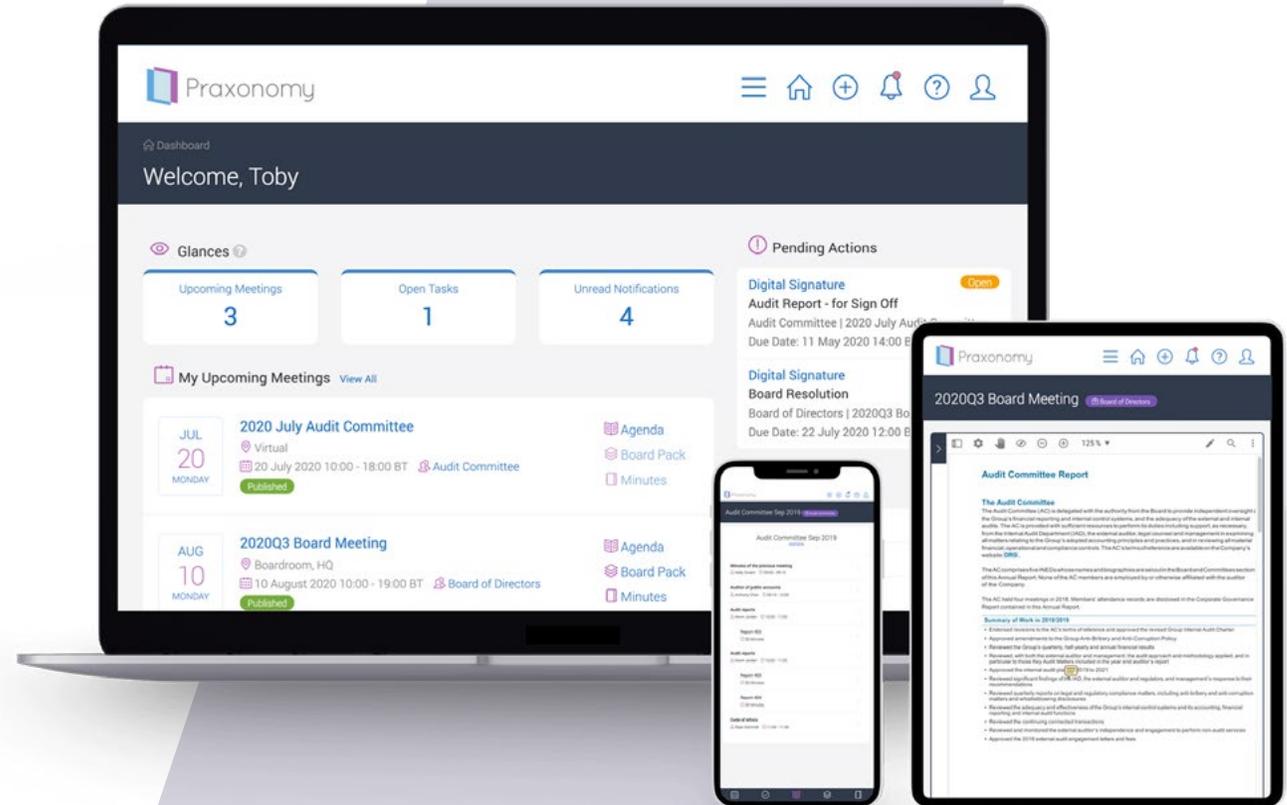
- ✓ Encrypt and backup computer hard drives
- ✓ Use a password manager + multi-factor authentication
- ✓ Use a VPN service
- ✓ Use a privacy-friendly web browser
- ✓ and more: [Praxonomy Blog: Digital Hygiene for the Board](#)

Should use technology solutions and platforms that enable secure collaboration, document sharing, and record retention, such as a board portal.



WHAT IS A BOARD PORTAL?

A **board portal** is a secure platform for board administrators and directors to organize and manage meetings, access materials, communicate with each other, and execute their governance responsibilities.



THE (SECURITY) CASE FOR A BOARD PORTAL

Printed board packs can be lost, stolen, and are impossible to track.

Email and attachments are not a secure (and efficient) channel and method for sensitive documents/information exchange.

Mass-market collaboration platforms may lack the functionalities, security, or compliance features designed for how boards function.

If possible, the board should be on a separate system from the rest of the company to minimize risk of internal breaches, and for crisis management and business continuity purposes in case the company's systems are attacked or breached.

A background image showing a group of business professionals in a meeting room. They are seated around a table, looking at documents and charts. The scene is brightly lit, suggesting a modern office environment.

KEY CONSIDERATIONS WHEN SELECTING A BOARD PORTAL PROVIDER

- ✓ Secure by design software and secure data hosting with data and document encryption at all times.
- ✓ Third party security certifications/audits to show, for example, ISO27001-certified, GDPR compliance, privacy-certified, independent penetration test reports.
- ✓ Data residency: is your data hosted in jurisdictions that offer sufficient legal protection against secret government data requests/surveillance?
- ✓ Not paying extra for features or services you won't need.
- ✓ Easy to use software with minimal training requirements for directors.
- ✓ Scalability and reasonable total cost of ownership.



ESSENTIAL FEATURES OF A BOARD PORTAL

- ✓ Meeting agenda creation
- ✓ Board pack compilation and instant distribution including when making updates and changes
- ✓ Minutes-taking and attendance tracking
- ✓ Meeting records retention and archiving
- ✓ Meeting notifications
- ✓ E-signatures for board resolution signings and approvals
- ✓ Granular information access control and flexible user role permissions
- ✓ Private and shared markups and annotations on documents
- ✓ Ability to group meetings and contents by groups (e.g. committees) or even companies
- ✓ Works on all devices

CONCLUSION

- ✓ Remote working has changed the landscape of cyber-risk management and assessment.
- ✓ Remote workers are now targets of malicious actors and campaigns.
- ✓ Secure remote working practices need to be adopted across all levels of the organisation, with leaders setting the tone for a “security first” mindset.
- ✓ Boards of Directors can be prime targets of exploits because of the information they collaborate on, exchange, and share.
- ✓ The use of a well-vetted board portal not only addresses the need for efficient, remote, and mobile workflows, but also ensures the security of board sensitive information.



GET SECURED NOW

The Praxonomy board portal provides a centralised and secure platform for board administrators, executives and directors to organise and manage board and committee meetings, access documents, communicate and execute their governance responsibilities. The platform offers security features such as granular permission controls, user roles and advanced data encryption. Praxonomy is ISO 27001 certified and GDPR compliant, and client data are solely hosted in secure data centres in the E.U.

[LEARN MORE](#)