Sri Lanka Institute of Information Technology

IE3072 - Information Security Policy and Management

Group Assignment

A Review: Ensuring information security while employees work from home

Group Number: ISPM_2022_020

IT Number	Name
IT20229320	Medawatte T.C
IT20251796	J.A.O.D Jayarathna
IT20246082	W.A.N.P.B. Ariyathilake
IT20250560	R.M.P.S. Rajapaksha

Abstract

The Covid-19 pandemic of 2020 brought a significant change to the corporate sector worldwide. All physical work was put to a hold for almost a year and the work environments shifted to remote environments. The Work from Home concept brought many challenges to corporate organizations that made them fear for the safety of the information security of their organizations which in turn caused them to make decisions to protect Information Security. This review paper will be critically evaluating the Information Security policies that were imposed in order to secure the organization's information covering critical areas of remote working, such as technical, policy and procedural, communication and employee awareness. It will also be discussing about the challenges in maintaining Information Security in remote working environment along with recommendations to improve Information Security while working remotely. The review paper will be referring the current Information Security Policies imposed and practiced by reputed institutions in Sri Lanka.

I. Introduction

The massive spread of Covid-19 locked down countries causing an abrupt change to all working institutions and organizations. Houses became the new office environments, where all employment work were transferred to office provided IT assets and personal IT devices. This bought up new concerns for Information Security as the company's critical operations were to be carried out in remote environments to ensure the business continuity throughout the pandemic period. All these critical operations were carried out through company provided assets and personal devices, the majority being personal devices. Each and every employee handles information in a different manner [1] and during the pandemic even critical and sensitive information were also handled by these employees while working remotely. This spurred the companies into strengthen their Information Security by adjusting the existing IS policies to match a remote working scenario.

With employees working remotely from their houses, put the company through immense pressure as the organization's infrastructure, equipment and information security were exposed to potential risks [2] [3]. Many workers accessed their respective organizational databases and work sites using their personal internet connections which were insecure in nature. This put high

demand on securing the institute's network. Virtual Private Networks (VPN) were used to address this concern as it provided encrypted communication. But the downside of it was, connecting a large number of devices to these VPN services, foregoing the recommended number of 20 devices, would be unsecure and not regularly updated [2]. This could have led to compromising the network and making it more vulnerable to access during cyber-attacks. There was also the concern on secure information accessibility of employees without compromising the information security.

2020 was the year Sri Lanka was converting to digitalization and all companies were adjusting to digital platforms. This was also the year the concerns about information security arise severely as almost all the industry data had to be made available for employees to access in order to continue their work. The threat was not just from the cyber criminals but with fraud employees as well. Therefore, strengthening the information security became a necessity and adjusting and adding policies to ensure information security during remote working was done by each and every institution. In the following sections, the importance of Information Security for remote working, policies imposed by institutions to ensure information security while working from home and further recommendations will be comprehensively discussed.

II. Significance of the topic

By reducing the impact of security incidents, information security is supposed to ensure company continuity and reduce potential corporate loss [4]. Large amounts of information are handled by organizations of all sizes, therefore different technical and administrative safeguards must be in place to maintain the highest degree of information security, availability, and confidentiality [5] [6] [7]. The property that information is not made available or given to unauthorized people, organizations, or systems is referred to as confidentiality. Also included in the concept of integrity are the qualities of accuracy and completeness. Finally, availability is described as being reachable and useable at any time by a legitimate organization. In the end, information security is the safeguarding of data and its essential components, such as any hardware or software that utilizes, stores, or transmits information [6] [7].

Even though the corporate sector is adjusting back to the physical working environments in the current context, remote working is still encouraged by companies in Sri Lanka. Many employees are using a hybrid working method, performing their work duties in both physical and remote environments. As more the corporate sector converts to digital platforms, accommodating employees through remote environments, the potential risk for Information Security stands higher than before. Therefore, evaluating the information security while employees work from home is timely and quite significant in the current context.

III. Critical Evaluation

Information security is a key factor to consider in each corporate institute/organization, more so in remote working environments. The management together with the IT department are responsible in developing the information security policies according to the ISO 27001 Information Security Management standards that matches the organizational structure and would provide the maximum security to the information assets of the company. This review paper comprehensively analyses the IS policies imposed by reputed companies in Sri Lanka, mainly LB Finance PLC, to ensure the information security in following areas of a work from home environment.

- Remote Connectivity
- Remote Collaboration tools
- IT asset security (Laptop/mobile security)
- Effective Communication

In an organization the information is classified as public and confidential. Public information is data that has been made known to the public by a person with the legal capacity to do so and that can be freely shared with anyone without risking harm to the organization's systems. All other information is contained in the Confidential. It is a continuum since it is known that some data should be safeguarded in a more secure way because it is more sensitive than other data. Included are details that need to be kept under lock and key, like trade secrets, development plans, potential targets for acquisition, and other details crucial to our business's future. Information that is less crucial and doesn't require as strict a level of protection, such phone

directories, general company information, personnel information, etc., is also included in an organization's Confidential [8].

Confidential information is again classified according to its sensitivity, namely, minimal sensitive, more sensitive and most sensitive. The approval level for this sensitive information are segregated as below [9].

Sensitivity Level	Requester	Approval Officer
Minimal Sensitivity	Department Staff	Executive grade and above
More Sensitive	Department Staff	Manager grade and above
Most Sensitive	Department Staff	Head of the Department

To secure both public and confidential information in both physical and remote environments, organizations have imposed Information security policies. Remote working is a vast field in enterprise security. Security needed to be taken care of multiple approaches. Here is a list of areas needed to be taken as a baseline.

- Securing remote working devices
- Using a secure network connection
- Restricting to minimal access level to internal systems and data
- Enabling strict monitoring
- Implementing proper incident response mechanism
- Properly enforcing adopted enterprise IT security practices and remote working policies [9]

There is malpractice allowing all IT systems made available to the WFH workforce. Some system administrators make access to the entire high-security zone network subnets while WFH user needs to access only a single URL. Therefore, make proper user groupings and allow only what they need to carry out a business function. Always adhere to the Principle of Least Privilege (POLP) which is an important concept in computer security. POLP states the practice of limiting access rights for users to the bare minimum permissions they need to perform their work [9].

In the coming sections, the remote aspect of information security will be discussed.

1. Securing Information Security in Remote Connectivity

Remote Access Policy

If your firm permits remote employees, you must establish a clear cybersecurity policy to ensure the security of each employee's access to company data. Without a plan in place, any employee might quickly turn into a hacker's point of access into your company's network. Make a cybersecurity policy that specifies rules for adhering to security protocols at home or when traveling to prevent this from happening. Policies might specify that encryption-enabled messaging apps like Signal or WhatsApp be used as much as possible, that antivirus and anti-malware software be updated on a regular basis, and that lost devices should be remotely erased [9].

This is the most crucial point in securing the organization's information. Every employee who is working remotely should have to company's information in order to perform their work duties efficiently and properly. It is the company's duty to provide access to this information alongside policies to secure the information accessed by the department staff. The following are some of the remote access policies imposed by LB Finance in order to secure information security while remotely accessing company's information [9].

- IT shall ensure that the access to the Internet is controlled by monitoring the Internet access usage logs [9].
- Audit logs recording user activities, exceptions, and information security events must be generated and stored for a defined period of time for future investigation and monitoring purposes [9]
- Access to system audit tools, such as scanning and monitoring software, data extraction and manipulation software and system utility programs, shall be restricted and the usage of these shall be subject to authorization. Such authorization shall only be granted by CISO, as well as the respective Asset Owners [9].

It is important to keep log reports of access to information systems of an organization. It helps identify who access the system and what happened during the session until the user logs out of the system. It is the responsibility of the CISO to grant the necessary permission when it comes to accessing critical systems while working remotely. It is important to log in to work systems using virtual private networks (VPN) to ensure secure communication and this should be encouraged by the responsible personals of the IT departments and raise awareness among employees [9].

Another method to use for information security is privilege management using role based access control. The theory and practice of limiting network access based on the responsibilities of specific users across the company is known as role-based access control (RBAC). The theory and practice of limiting network access based on the responsibilities of specific users across the company is known as role-based access control (RBAC). RBAC stops employees from accessing information that is not pertinent to them or required to perform their responsibilities by granting them access privileges only to the information they require to complete their assigned tasks based on their job roles. Employees are prohibited from accessing information that is not pertinent to them or required for them to complete their responsibilities by limiting their access permissions to the information they need to execute their assigned tasks based on their job roles [2].

Role-based access control implementation enables IT security teams to monitor what end users may do at all organizational levels, from the board of directors to the manager of the call center. Users are typically divided into one of two types by role-based access control: administrator or normal user. Then, based on the user's unique place within the organization, roles and permissions are allocated and positioned accordingly.

There are several benefits of Role Based Access Control. Access control minimize the risk of data breaches. Implementing RBAC can be very important in limiting the damage caused by an attacker who has stolen an employee's user credentials because it not only lowers the danger of cyber-attacks and misuse by malevolent insiders. It improves operational productivity and efficiency. When hiring and onboarding new employees or changing the roles of existing employees, RBAC enables firms to minimize paperwork and requests for password changes. It also provides greater visibility for administrators. RBAC ensures that authorized users and

visitors on the system are only granted access to what they need to conduct their tasks while also providing network administrators and managers with greater visibility and oversight into the organization. RBAC helps in conserving resources. Employees are kept focused on the current task by limiting user access to only certain activities and programs.

Two-factor authentication

Users submit two distinct authentication factors as part of the security procedure known as two-factor authentication. In order to better safeguard user credentials and the resources they can access, two-factor authentication is used. When compared to authentication strategies that rely just on one factor, two-factor authentication offers a higher level of security.

factor 1 -- typically, a password or passcode. Two-factor authentication methods rely on a user providing a password as the first factor and

factor 2 -- usually either a security token or a biometric factor, such as a fingerprint or facial scan.

By making it more difficult for attackers to access a person's devices or online accounts, two-factor authentication adds an extra layer of security to the authentication process. This is because, even if the victim's password is compromised, a password alone will not be enough to pass the authentication check.

There are several ways in which someone can be authenticated using more than one authentication method. A knowledge factor is anything the user is aware of, such as a shared secret, a password, or a personal identification number (PIN). An item the user possesses, such as an ID card, a security token, a cellphone, a mobile device, or a smartphone app, is known as a possession factor. The user's physical self contains a biometric factor, also called an inherence factor. These could be physical traits matched to personal traits, such fingerprints verified by a fingerprint reader. The location from which an authentication attempt is being made is typically used to identify a location factor. This can be enforced by restricting authentication attempts to devices in a specific location or by tracing the geographic origin of an authentication attempt using the source Internet Protocol address or other geolocation data, such as Global Positioning System (GPS) data, derived from the user's mobile phone or other device. A time restriction

limits access to the system outside of a predetermined time window and limits user authentication to that window.

The following are the IS Policies imposed by LB Finance PLC to secure IS through two-factor authentication [9].

- LBF shall apply appropriate controls to prevent opportunities for information leakage. Such controls include considerations for the regular monitoring of personnel activities, system activities and resource usage.
- Secure Passwords + MFA - Use Unique & Strong passwords for all accounts and use Password Managers to properly secure them. In reality, it is not possible to remember so many passwords without a password manager. With excellent password hygiene, use Multi-Factor Authentication every possible occasion. Multi-Factor Authentication is often called Two-factor Authentication or Two-Step Verification.

Two factor authentication is essential when it come to remote working. Employees who are accessing company information assets should be authorized to access the necessary information according to their role in the organization. The authentication can be done through login credentials and passwords, OTPs and internal emails. This way the company can make sure that only the authorized employees access the relevant data according to their role in the organization. It also helps identify if a fraud user is accessing organization's information systems without the knowledge of a legitimate user.

How does two-factor authentication work?

Depending on the application or vendor, different two-factor authentication options may be available. However, the general, multi-step procedure for two-factor authentication is the same:

1) The program or website prompts the user to log in.
2) The user inputs their login and password, which they typically know. The server for the website then discovers a match and recognizes the user.
3) The website generates a special security key for the user for procedures where passwords are not necessary. The key is processed by the authentication mechanism, and it is verified by the website's server.

4) The website requests that the user start the second login process. The user must demonstrate that they own something only they would possess, such as biometrics, a security token, an ID card, a smartphone, or another mobile device, however this step can take many different forms. This is the possession or inherited factor.
5) The user may have to enter a one-time code generated during step four.
6) After providing both factors, the user is authenticated and granted access to the application or website.

Security monitoring

An audit log may contain any event that occurs in an IT system. What data you are consistently logging and evaluating should depend on the demands and hazards involved with each application and server instance, which will vary substantially. However, it's safe to state that these components should be included in almost all instances in your audit logs:

- User ID
- Terminal identity
- Log on and log off time and date
- Systems, data, applications, files, and networks accessed
- Failed attempts to access systems, data, applications, files, and networks
- Changes to system configurations and use of system utilities
- Alarms and other security events
- Activity from cybersecurity tools like the firewall or antivirus software

The retention of audit logs depends on the kind of log you're storing, you should archive event logs for a specific amount of time. Regarding audit logging, customer or organization might have specifications and recommendations, and most logging techniques are governed by laws. However, logging best practices advise preserving everything for at least a year if you're unsure how long the organization ought to preserve a specific audit log.

In terms of active security measures, implementation of firewalls, antivirus software, and several user authentication methods at our disposal. Network security experts can use these techniques to stop unauthorized users or malicious users from stealing or damaging assets on a network while safeguarding those who are permitted to access those networks. But what happens if an attack

still takes place despite all these precautions? Security experts can go to their event logs for information.

But just like security cameras won't be able to provide you with any intelligence if they aren't trained on the region you're attempting to defend, the simple existence of audit logs isn't enough to shield you from cyberattacks. Here are some loggings and monitoring best practices to follow to make sure you're not only recording important IT events, but that you're also doing it in a way that will make it simple to analyze them in the event of a security breach.

1) **Automate reviews**

Any IT manager must have a log management software solution, yet it is insufficient on its own. Not only must logs be gathered, but they must also be carefully examined; in the case of very high-risk applications, these inspections should be carried out automatically every hour. The ideal method for doing this would be one that not only identified security threats in logs but also automatically implemented countermeasures like blocking IP addresses, altering rights, and terminating accounts.

2) Maintain manual administrator logs

Because administrators have so many more permissions than other users, their accounts must be monitored and protected with more vigilance. These users could exercise caution by manually logging their activities, including the times they logged on and off. These manual logs should be handled and analyzed with special attention if possible.

3) Frequently review fault logs

Administrators' accounts need to be watched and safeguarded with greater care because they have access to so many more resources than regular users. By manually recording their activity, including the times they logged in and off, these consumers might exercise prudence. If possible, these manual logs should be handled and examined carefully.

4) Create log redundancy

Cybercriminals frequently attempt to access your log files to remove any records of the breaches they were responsible for. To avoid breaches from going undetected, it's critical to record logs both locally and to a distant server that will be more difficult for criminals to access. Any disparity between the two files will set up an alarm.

5) Make sure system clocks are synchronized

In the field of forensics, it is crucial to comprehend the sequence of events in order to piece together an accurate narrative of the crimes that were committed and who committed them.

2. Securing Information by using secure collaboration tools

With the change of work environments, organizations turned to virtual collaboration tolls to ensure business continuity of the organization. Some of the well-known collaboration solutions used by corporate sector are Microsoft Teams, Slack, Zoom, and Citrix Workspaces. Many security challenges have arisen as a result of the shift to remote labor for businesses. The increasing usage of collaborative tools has heightened the demand for better security because firm data is at danger. Securing a remote work setup includes establishing policies for vulnerability management and incident handling, properly configuring devices remotely, putting in place suitable authentication and authorization measures, securing data in transit and at rest, and minimizing the possibility of data leaks or exposure to third parties. In this part, the following crucial aspects of safe remote collaboration tools are examined.

- Collaboration governance controls
- Access to the collaboration tools
- Data security.

3. Ensuring Information Security by securing corporate laptops/use of personal devices for remote work

Organizations are being forced to quickly adapt to new working methods as the world deals with the COVID-19 pandemic. They are battling the difficulties of working from home under extremely constrained circumstances. Numerous businesses in the area have enabled remote access and collaboration capabilities in reaction to the disturbance. The use of personal devices and home networks is permitted for extended periods of time by many employers. The following are some of the steps that can be followed to ensure information security in corporate IT assets and personal devices used for office work.

- Secure remote workers by persuading them to lock computers when they are physically moving around, to start with. There is less possibility of theft if their equipment is not physically accessible.
- Second, remind staff members to be mindful of any bystanders when entering sensitive data, such as logins or passwords, when working in public areas. Shoulder surfing is a phenomenon that is more prevalent than it first appears to be.
- Give your staff the instructions to always log off or turn off their laptops when not in use. A computer that is not password-protected can be accessed as easily by leaving it on as it can by virus.

KPMG in Sri Lanka has identified key controls for several risk sectors. As a result, we are waiting to talk about the regulations other companies have developed in compliance with those risk areas. The following are the identified risk areas [10].

1. VPN-based remote access
2. MDM Solution and User Authentication
3. Endpoint Security Solution
4. Rooted device restrictions, Outdated OS restrictions, Anti-malware protection and Security updates

1) VPN-based remote access

Millions of people continue to labor remotely around the world to serve the pandemic-related needs for shelter-in-place. Many workers want to work remotely, therefore this practice will likely become more popular. Businesses have responded by using VPNs more frequently to provide widespread remote access, but is this the best option going forward [10]?

VPN use can be dangerous even though it is meant for safe, encrypted communication. Policies that safeguard credentials cannot be established by or enforced by third-party VPNs. Sharing login information with coworkers or using easily cracked passwords from personal accounts If a large workforce is linked by VPN and the VPN becomes corrupt, doss attacks and other things could happen. The IT division lacks visibility into what happens on these equipment. The user experience degrades when problems occur, and the root cause is not identified [10] [11].

Safeguard web gates can be used to secure VPN connections, keeping data from leaving company-controlled networks and screening out hazardous information to keep remote workers safe. Additionally, internal infrastructure and data can be hidden from all unauthorized users by using a software-defined boundary. The Presidential Secretariat Work From Home Security Guidline For VPN Using issued by Sri Lanka CERT is as follows.

- If you have been provided with an official secure connection facility such as a VPN, use only that to connect to work systems.
- Always disconnect VPNs when not in use

2)End-point security solutions

The home networks should be protected from intrusions in order to maintain endpoint and data security. Because our home network is connected to the endpoint when we work from home, that is the cause. Employees may be given configured routers by an enterprise if using the home network is deemed improper. The software and operating system of the computer we use while working from home must be up-to-date because otherwise the computer may be vulnerable to cyber-attacks. In the event of a threat to the endpoint, the potential of losing data, and a middle-man attack may also occur. As a solution data loss prevention method can be used.

3)MDM solution and user authentication

BYOD policies are secured with MDM Security. Many firms enable employees to use their own devices at work under the Bring Your Own Device (BYOD) policy. Employees that adopt BYOD also use their devices when working remotely. Employees can't unintentionally log onto a public wifi network or a VPN by using an MDM solution. Any mobile device linked to the MDM server is a client. Remotely from the MDM server, each attached device receives configurations, applications, and policies. The MDM server is used by IT administrators to remotely manage all endpoints. Endpoints include devices like iPods, PCs, tablets, and smartphones [12].

The biggest advantage of automating everyday tasks is the time savings. For instance, asking employees to install specific software and manually configuring 100 devices' Wi-Fi settings both take time. MDM systems offer complete automation of these processes. even on personal devices, more effective and productive When a personal mobile device is managed by the MDM

server, non-essential applications cannot be used while at work. As a result, access to social media and other applications for employees would be restricted. satisfying regulatory requirements such as HIPAA, PCI-DSS, and GDPR. Remote management: Devices linked to the MDM server can be remotely patched, updated, and managed without disrupting the user's experience [12].

4. Secure Communication to ensure Information Security

While working remotely it is important have secure communication methods to keep in touch with the internal staff of the organization who are working from home. Secure communication in the sense, is having effective communication method or a channel for remote working employees with the organization, to inform the about cyber-attacks and raise concerns about information systems and assets. From the organization's side, having secure communication helps spread awareness among employees on cyber threats and conduct training sessions on cyber security. Having an Incident Management Policy aids a company in securing communication which in return ensures information security. The following are some actions that can be taken to ensure secure communication.

- Imposing policies and raising awareness among employees about them

It is important to have a proper method of communication to raise awareness among the employees on changes in Information Security Policy for remote environments. Most of the companies use internal email as the communication channel for employee awareness on such changes done on policies and procedures [13].

- Having proper communication Plans

All organizations who support remote working should have a proper communication plan to manage internal and external communication related to cyber security incidents. All remote working employees should be provided with contact numbers of responsible personals for reporting cyber security incidents. Following is the IS policy imposed by LB Finance PLC for incident reporting [3].

- LBF users shall report information security events as soon as possible to the CISO by using an appropriate communication channel and recorded in the IT Helpdesk System

- Types of information security incidents that may include, but are not limited to the following:
  - ✔ Unauthorized access to LBF information processing facilities
  - ✔ Misuse of information assets
  - ✔ Unauthorized disclosure of information
  - ✔ Falsification of information
  - ✔ Malicious code and hacker intrusion
  - ✔ Destruction and damage to information assets
  - ✔ Theft/loss/misplace of information, computer equipment or information services
  - ✔ Unavailability of critical information asset
  - ✔ Installation of equipment not authorized by LBF. [9]

- Communication Infrastructure

The organization should provide the remote working employees with proper communication channels. There should be an official communication tool to report incidents via raising a ticket or sending an email. For other official work meetings, it is better if the company has a proper meeting platform such as MS Teams.

- Raising awareness on Phishing attacks among employees

The biggest cyber threat to information security in remote environments are phishing attacks. In 2020, the highest number of phishing attacks were reported with credential theft phishing attacks gaining the highest percentage among them. It is the responsibility of CISO and the IT department to conduct stimulated phishing attacks and carry out phishing attack awareness sessions to all employees to ensure the cyber safety of both the company and the employee.

- Remote working safe practices

Conducting refresher sessions on best practice for remote working is important. Conducting these types of session can raise awareness among employees on the dangers of using public wi-fi, benefits of physically securing unattended equipment/IT assets and not using office laptops for personal work.

IV. Conclusion and Recommendations

Covid-19 pandemic bought the world an abrupt change, limiting all activities of the day-to-day life to the geological area of one's home. It affected the corporate sector just the same. All physical aspects of the working environment were abruptly changed to a virtual environment, reducing the office into a virtual platform. This definitely raised major concerns about the safety of the organization's critical information. It was clear that companies, during the last two years have adapted quite successfully to the new normal, adjusting their existing information policies to match the current context that serves and covers the information security aspect in remote environments. Every organization has a responsibility in changing, modifying and imposing information security policies and procedures to secure their organization's information assets while the remotely working employees has the responsibility to adhere to the policies and procedures and secure the organization's information.

It is highly recommended for organizations to polish up their information security policies to cover every aspect of information security while improving the information security standards to properly secure company's IT assets. Companies should give more attention to raise awareness and conduct training sessions to employees on how to secure them selves from cyber threats and how to prevent themselves from endangering the organization's critical data. It is recommended to all employees who works from home to follow the guidelines and procedures provided by the company that ensures information security while working from home.

References

[1] M. A. S. p. Distans. [Online].

[2] "Secure Work From Home - Security Awareness Guide," TechCERT, 2020. [Online]. Available: http://techcert.lk.

[3] "How secure are your remote working arrangements?," KPMG, 2020. [Online]. Available: https://assets.kpmg/content/dam/kpmg/lk/pdf/2020/how-secure-are-your-remote-working-arrangements1.pdf.

[4] R. Von Solms and J. van Niekerk, "Information Security to Cyber Security," in *Comput. Security*, 2013, pp. 97-102.

[5] J. Isaksson and T. S. K. E. d. a. e. 1. A. Sanne, " intelligent IT," 2006. [Online]. [Accessed 5 September 2022].

[6] "International Organization for Standardization ISO/IEC 27000: 2018.," 2018. [Online]. Available: https://www-sis-se.libraryproxy.his.se/. [Accessed 5 09 2022].

[7] I. O. f. S. I. 2. 2013, 2013. [Online].

[8] M. Whitman and H. Mattord, "Principles of Information Security," Boston, MA, USA, Cengage Learning, 2014, pp. ISBN 978-1-111-13821-9.

[9] L. Finance, "LB Finance Information Security Policy," LB Finance, Colombo, Sri Lanka, 2021.

[10] "nformation Security Guidelines for Working from Home," CERT, 2020.

[11] V. Prajapati, "Top 5 Cyber Threats that a VPN can Handle," [Online]. Available: https://www.techprevue.com/cyber-threats-a-vpn-can-handle/.

[12] "VPN security: How VPNs help secure data and control access," [Online]. Available: https://www.cloudflare.com/learning/access-management/vpn-security/. [Accessed 03 09 2022].

[13] "What is Mobile Device Management (MDM)," [Online]. [Accessed 03 09 2022].

[14] "How secure are your remote working arrangements?," KPMG, 2020.