CRITICAL EVALUATION OF THE TOPIC

Evaluation of the Work from Home Concept

The societies of industrialized nations have seen tremendous transformations in the previous half-century, which has led to significant shifts in the workplace. Women now make up almost half of the workforce in the United States, and nearly half of all households are now headed by two working parents1. Additionally, an increasing number of working adults are providing care for elderly relatives and are enrolled in higher education courses. 2. To give workers more flexibility, more and more employers are allowing their employees to work from home.

Working from home may have several benefits for businesses and communities, including a positive impact on work-life balance, potential savings for rent and staff turnover, and reductions in congestion and emissions caused by commuting. Even though it might have a number of positive effects, many businesses have been hesitant to use the procedure because they are unclear of how it would influence the productivity of their employees. Employees who work from home may find it easier to concentrate in a more peaceful setting. They may also miss less work if they arrange personal activities, such as doctor's visits, in the time they save by not traveling, which might make it easier for them to concentrate. On the other side, the absence of supervision may provide employees the opportunity to multitask by engaging in activities.

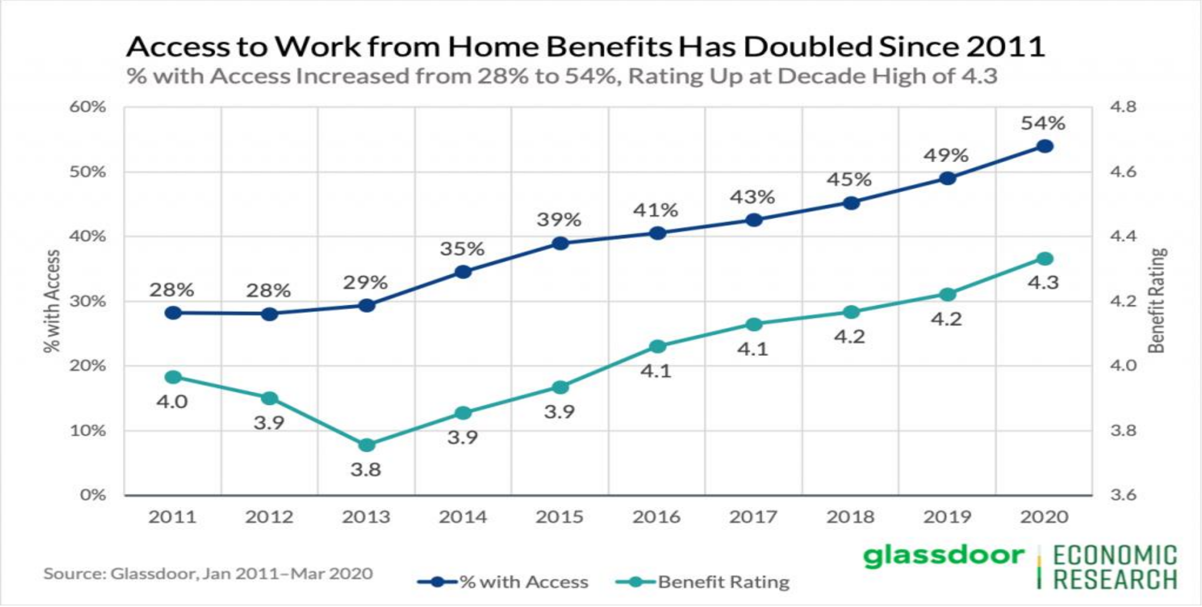
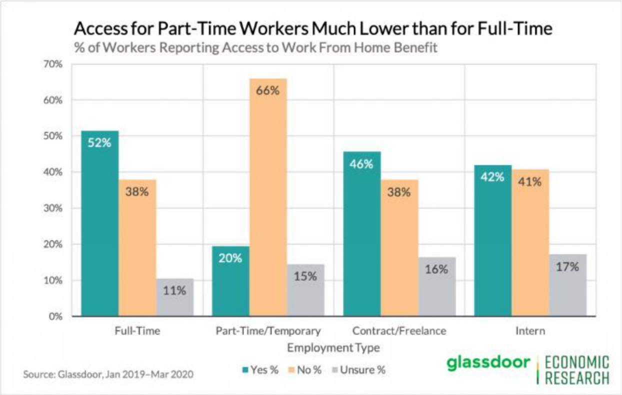
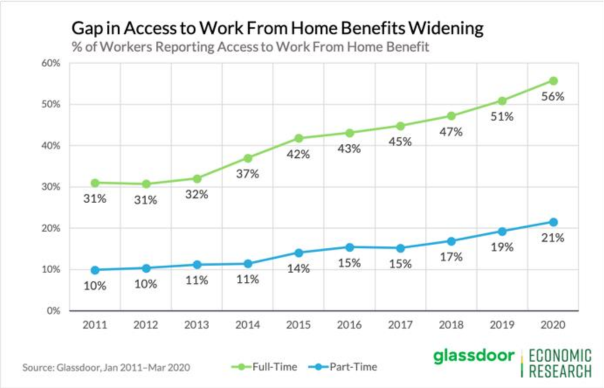


Figure 1

According to the statistics provided by Glassdoor, there are now 54 percent of employees in the United States who claim having access to work from home privileges. This is a significant improvement from 2011, when just 28 percent of employees reported having access to the benefit, when it was only 28 percent. Access has continuously grown every year since 2011, as seen in the figure below, all the way up to its current high point in 2018.

Since the beginning of the 2020s, employees' levels of contentment with the advantages of working from home have improved, hitting 4.3 out of a possible 5. In instance, the opportunity to work from home rates far higher in terms of employee satisfaction than some of the most recognized perks, such as health insurance (3.7 out of 5), vacation and paid time off (3.8), and 401(k) plans (3.8).





As a reflection of the varied nature of contract employment, contract and freelance employees report an equally high incidence of work-from-home possibilities as full-time workers. There are numerous contract jobs available in white-collar professional services like graphic design and copywriting that can be done remotely. While some contract employees are engaged in industries that need them to be physically present, there are also many contract jobs available in other fields.

Even while part-time workers claim to have far less access to work-from-home possibilities than full-time employees, the number of opportunities available to them has still increased by a factor of two over the last decade. On the other hand, the quick speed of development for both part-time and full-time employees has expanded the gap in access to benefits associated with working from home. The difference in access to benefits associated with working from home for full-time vs part-time employees began the decade with a margin of 21 percentage points in 2011, which has since grown to 35 percentage points and will remain in place in 2020.

Security Evaluation of the Work from Home

Secure home workstations and personal devices

Workstations, or the hardware that employees use to perform business, can take several shapes in a remote work environment. Laptops, tablets, and even mobile phones are examples of gear that need security in this instance. Work with your IT staff to verify that employees have antivirus software installed on any devices that have access to corporate data, including home computers.

- Locking The Device

The first step in protecting your devices is to keep them locked. When not in use, set each device to automatically lock after a certain amount of time and require a password to reopen. full disc encryption must be installed and activated.

- Disk Encryption

Full disc encryption, like the key that locks your door, safeguards the hardware if an employee's gadget is lost or stolen. Passwords alone are insufficient to protect firm data. Between 2005 and 2015, approximately 41% of all data breaches were caused by misplaced phones, PCs, and tablets.

- Firewalls

Strong firewalls should be installed on each device that has internet connection. A firewall safeguards your system by blocking threats from entering it. Firewalls are often incorporated into any operating system, but users should double-check to ensure they are activated. It may also be prudent for businesses to give staff with access to a tried-and-true firewall solution. This ensures that everyone receives the same amount of protection.

- Antivirus

Strong firewalls should be installed on each device that has internet connection. A firewall safeguards your system by blocking threats from entering it. Firewalls are often incorporated into any operating system, but users should double-check to ensure they are activated. It may also be prudent for businesses to give staff with access to a tried-and-true firewall solution. This ensures that everyone receives the same amount of protection.

- Update devices regularly

It is critical to keep operating systems and applications up to date. They are responsible not just for keeping devices working properly, but also for installing new fixes that address serious vulnerabilities. Updates should be installed on a regular basis. Most updates may be scheduled to install automatically at predefined times. Set devices to update, for example, in the middle of the night while the device is not in use.

Employee Awareness

When employees labor outside the office, it is more difficult to monitor social engineering attacks. Criminals use this sort of cyber threat to trick people into disclosing personally identifying information (PII). Because of that its must to teach staff how to identify these threats. Begin by learning how to identify phishing emails. In a commercial environment, cyber thieves frequently replicate the identities and email addresses of top management, knowing that employees would respond to the CEO and inadvertently expose embarrassing information.

Vishing is a similar approach that relies on emotions. Scammers in this example employ an internet telephone service (VoIP) to perform Caller ID Spoofing, which results in the creation of bogus phone numbers. Apply the same action procedures for both phishing and vishing - always notify the IT department as soon as you suspect something is "odd." Make the risks of sharing personal information on any device or platform, including social media, clear. The risk is particularly significant during times of crisis, when attackers masquerade as groups striving to assist individuals in need.

Improve Home Network Security

Employees must work hard to safeguard their own home network while transitioning to a remote work environment. Home network infrastructures, such as routers, should adhere to manufacturer recommendations for system configuration. These networks have strict password policies that require at least 14 characters in capital, lowercase, digits, and symbols.

- Virtual Private Networks and Secure Remote Access

Typically, organization Provide employees with a VPN to use when working on a public network, such as at coffee shops, hotel lobbies, or airports. All internet traffic is encrypted using a virtual private network (VPN), rendering it unreadable if intercepted. This safeguards data transmitted over a Wi-Fi network and prevented eavesdropping by hackers, ISP (internet service providers), or even the government. An individual can choose their own VPN service on a budget, or the company can choose a VPN tool that can be made available to several users.

Many companies utilize remote desktop protocols (RDPs) to provide employees access to the company network. These can be secure, however recent research has discovered significant security flaws and several RDPs, particularly on Windows PCs.

- Multi-Factor Authentication

While strong passwords are the first line of defense, multi-factor authentication or multi-step verification offer an extra layer of security by requiring logins from new devices or places to go through additional verifications to ensure the login is from the proper person. This verification might take the form of an email, text message, or app message. A biometric approach, such as face recognition or fingerprint scanning, might also be used. Physical means are also permitted in some cases.

- EDR, XDR and SIEM solutions

Endpoint Detection and Response (EDR) is a type of classical technology protection that identifies attacks by comparing signatures to attack patterns. It blends real-time monitoring and endpoint data collecting with rule-based automated reaction and analysis. While XDR intended to detect highly sophisticated and concealed attacks, improve detection and reaction times, and monitor or detect threats across several system components such as networks, servers, and the cloud environment.

SIEM is a technology that provides next-generation detection, analytics, and response capabilities. The program analyzes security alerts produced by apps and networks in real time. SIEM does this by integrating Security Information Management (SIM) with Security Event Management (SEM).

Back Ups and Disposal of Data

Storage is a critical component of data security. Certain types of data must be preserved for a specific amount of time due to essential company activities and regulatory regulations. As a result, all employees who work from home must have an established and safe backup strategy. Encrypt an external disk and need a password to access it. Cloud storage is also an option for backup. However, cloud storage should be protected, and information access restricted to individuals depending on necessity.

When a device approaches the end of its useful life, it should not be stored in a drawer or box indefinitely. It should also not be resold unless special precautions are taken to make all data unreadable. Delete and factory reset do not destroy data; they only make place for fresh information. Even data-erasure software can leave data behind. We advocate smashing and shredding hard drives and memory chips to physically destroy them. Other device components can be recycled without fear of data being compromised.

Certain digital data must be kept for a predetermined length of time known as a retention period. When a document's retention term expires, it should be safely destroyed. Companies must offer clear directions to staff on what to preserve, how long to keep it, and how to appropriately dispose of the stored data.

Work From Home Policy

Employers confront additional challenges and concerns when their personnel relocate to a remote location. Technology aids in the productivity of operations: For the majority of businesses, a remote worker may make the most of their time and contribute from anywhere. However, the use of this technology may damage organizations, employees, and consumers sometimes. According to the 2019 IBM Cost of a Data Breach Report, the average cost of a data breach is 3.92M USD [1]. Due to that, proper set of guidelines and method of approaches needed.

Due to that work from home policies introduced. A work from home policy, also known as a telecommuting policy or a remote work policy, is a set of guidelines that allows employees to work from home under particular conditions. For instance, this document may contain details on tech packages, password sharing, time tracking, expense management, and other subjects. A more permissive work from home policy may not need a legitimate justification or a formal process, but it may stipulate the maximum number of days an employee may work remotely each week, month, or year. More significantly, a remote work policy establishes guidelines and expectations for employee behavior. Because a supervisor cannot immediately see a distant employee, virtual employment necessitates higher degrees of confidence. Telecommuting policies provide forth ground guidelines for employees to follow. A policy could, for example, specify how to utilize corporate equipment or what hours employees must be accessible.

When considering all the related variables for the WFH environment, bellow listed aspects are the critical once

- Working Hours

While virtual offices function at the discretion of the employer, traditional offices normally work from 9 to 5. While some companies prefer that employees stick to a certain schedule, others prefer to let they work whenever they choose. Workplaces in the middle allow employees to choose their own schedules or establish hours when everyone must be online.

- Technology usage

If your remote employees use business computers or other company-owned equipment at home, you should establish technology usage policies. Standards for permissible usage might differ from business to firm. Hustling on the work laptop can lead to conflicts of interest and other legal concerns later on and determining who is responsible for lost or damaged equipment is also crucial. Outlining repair processes is also very beneficial. The organization want to clarify if an employee may utilize any repair shop, must visit a specific approved vendor, or must send the equipment to the central IT office with a tracking number. Also, specify whether the corporation will pay for third-party repairs up front or refund employees.

- Security Protocols

You should include security practices in your remote work to guarantee that all company, customer, and employee data remains safe. Because there is no way to confirm the security of every employee's network connection, Sensitive information like trade secrets or customer payments are fully secured. To prevent interference, confidential virtual meetings should utilize secure virtual conference software, and employees should need to protect their own credentials. Employees should also need to save work data on business computers rather than personal disks. Addressing behavior is also recommended.

- Communication Guidelines

Remote teamwork is impossible without communication. Employees in various buildings may use online discussions to ask inquiries, provide updates, and develop ideas. Outline how and when employees should reply by include communication rules in your work from home policies. Teammates should be aware of which platforms to utilize, and employees should be aware of reaction time requirements.

- Timekeeping / Hourly reporting

Timekeeping might be more difficult since remote working hours are more flexible. Many remote managers use time clock software to ensure that offsite employees put in the required hours. Recording the hours can hold remote employees accountable to focus and work for the entire period of time; therefore, instructions and deadlines for submitting hours, as well as clarification of the approval process, are required.

- Approval Procedure

If employees do not work from home full-time, administrators should clarify the process for requesting remote workdays. employer may ask employees to make a written request at least 24 hours in advance. Employees should be aware of who to approach for permission and whether any supervisors or other departments must be contacted. Even though employees can take as many remote days as they desire without asking for permission, companies may want to establish some broad guidelines. Communicate, for example, if there is a monthly or weekly limit on work from home days, or whether employees must work from the office on certain days.

- Boundaries

Employees are human, and while home life may occasionally infiltrate the work, separating the two environments is in the best interests of both your company and your employee. Switching between activities takes too much time and brainpower, which reduces total productivity. Because remote employees often struggle to establish limits while working from home, due to that, organization may wish to recommend boundaries in work from home conditions.

Types of WFH Policies

- Hybrid Remote Policies

Hybrid remote models enable office workers to work from home on occasion. These companies may allow employees to telecommute from a few days per year to a few days per week. Enterprises used to be stringent about in-office attendance, but an increasing number of businesses are now allowing workers to work from home more liberally.

- Fully Remote Policies

Consider the companies whose employees work entirely from home. Certain roles in these businesses may be remote, or all employees may be telecommuted. In these cases, the work-from-home policy and the employee handbook are usually the same.