Scientific Research Publishing

Journal of Information Security, 2023, 14, 396-421
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A New Cyber Risk: How Teens Expose Corporations in WFH Era

Zahm Siyed

Diamond Bar, CA, USA
Email: zahmsiyed@gmail.com

How to cite this paper: Siyed, Z. (2023) A New Cyber Risk: How Teens Expose Corporations in WFH Era. *Journal of Information Security*, **14**, 396-421.
https://doi.org/10.4236/jis.2023.144022

Received: August 12, 2023
Accepted: October 13, 2023
Published: October 16, 2023

Abstract

We analyze the risks associated with teenagers' online activities and the potential migration of cyber threats originating from teenagers to their parents' work-from-home (WFH) devices, even when defensive measures such as VPN are employed. Furthermore, we examine the serious implications these risks have on corporate security. Of particular concern, parents who work with confidential corporate information, such as financial projections or product roadmaps, might find that their kids are targeted by hackers who seek an easier entry-point to home networks and eventually WFH devices. This paper is timely since there is a rising trend of hybrid work in white-collar professions, mixing traditional in-office work with WFH. The latter is increasingly done in split shifts, including work performed before breakfast or after dinner. While this shift offers numerous workforce advantages and helps teen-parent bonding, it also introduces a plethora of cybersecurity risks, especially when these devices and networks are shared with teenagers on home networks. We did a structured survey of 62 teens which confirms that risky online activity abounds, so the threat of risk migration onto corporate networks should not be ignored. We perform a migration risk assessment and identify which teen-origin risks are most likely to contaminate parents' WFH devices. We evaluate 20 attack vectors and generate 60 risk ratings. We classify 29 as high risk, 8 as medium risk, 13 as low risk, and 10 as not relevant. We offer recommendations to mitigate this new set of cyber risks.

Keywords

Cybersecurity, Remote Work, Teens, Vulnerabilities, VPN, Corporate Risk

1. Introduction

Corporations have always been at risk from insecure networks and from a lack of cyber hygiene in their workforce [1]. This risk has risen in recent decades due

to the prevalence of remote work, which spikes after the recent pandemic, and is likely to continue to rise over the next decade [2].

A new underappreciated risk is that remote workers share a home network with their teenagers, and the latter have notoriously poor cyber hygiene. This paper focuses on a teen-origin risk scenario: increasing sophistication of hacking methods can migrate risks from teen devices to WFH devices. Although the use of VPNs by remote workers can safeguard corporate networks [3], we believe they are not adequate to prevent the aforementioned teen-origin risks. There is a specific risk that should be of particular concern to both parents and corporations: parents who work with confidential corporate information, such as financial projections or product roadmaps, might find that their kids are targeted by hackers who seek an easier entry-point to home networks and eventually their WFH devices. Although it is not widely prevalent yet, this risk is not negligible. As teens leave more digital footprints, it is likely they will increasingly become soft targets to gain access to their parents' corporate devices.

1.1. WFH Increases Teen-Parent Digital Interaction

Although teens and parents have always occasionally interacted during the parent's workday, there has been a rise in such interaction. In the WFH era, hybrid work is more prevalent, and white-collar parents are more likely to intermix work and family activities, often splitting their workday into different periods, such as an hour of work before breakfast, a long workday broken up with a quick family lunch, and work again after dinner.

In the last decade, there has been a dramatic shift in the way employees work, with remote work becoming more and more common. This change has been accelerated by advancements in technology, global connectivity, and most importantly, the coronavirus pandemic, which forced organizations to adapt their operations to keep their business alive [4]. As employees grow accustomed to the convenience of working from the comfort of their homes, the use of personal devices, such as desktops, laptops, smartphones, and tablets, for professional tasks has become increasingly prevalent. While this transition has been beneficial in terms of flexibility, productivity, and work-life balance, it has also exposed corporations to more cybersecurity risks.

One significant and often overlooked aspect of the remote work environment is the presence of teenagers within the household. With schools adopting digital learning platforms and remote learning opportunities, teenagers spend a considerable amount of time online in activities on various internet-enabled devices [5]. However, the digital safety and online habits of teenagers significantly are far worse than those of their adult counterparts, making them susceptible to a range of cybersecurity threats.

By examining the behavior and online habits of teenagers, the factors that contribute to their elevated exposure to cybersecurity risks can be explored [6]. Teenagers are inherently more susceptible to falling victim to social engineering tactics, impersonation, engaging in risky online behavior, and illegal content access,

all of which can lead to the compromise of remote work devices and networks. Teenager's access to shared home Wi-Fi networks can serve as an attack vector on corporate devices, leading to data breaches, unauthorized access, backdoor access, and potentially jeopardizing lucrative and sensitive corporate information [7].

The research also highlights the need for increased and adapted security measures on both personal and corporate devices. Weak security practices, such as redundant passwords or lack of software patching, can worsen the cybersecurity risks associated with teen users, increasing the potential for corporate exposure and exploitation [8].

1.2. Home Networks Host Both Safe and Unsafe Devices

The interconnected nature of home networks also plays a critical role in amplifying the cybersecurity risks associated with teen users. Unlike the traditional office environment, where corporate networks are separate from personal ones, remote work setups often, but not always, rely on the same shared Wi-Fi networks used by teenagers for their online activities. A security breach on a personal device could inadvertently provide an entry point for hackers to access corporate systems and sensitive data [9].

While some attention has been given to securing corporate devices and networks accessed by employees, the potential implications of teen users on corporate security have not been researched. Therefore, it is crucial to understand how the behaviors and practices of teenagers can inadvertently expose corporations to cyber threats.

Adolescents, especially in their formative years, tend to be more socially active online and lack digital sophistication and maturity [10]. This makes them susceptible to falling prey to social engineering tactics, such as phishing scams and identity theft, which can lead to unauthorized access to work-related devices and sensitive corporate information. Moreover, the prevalence of risky online behavior among teenagers, such as sharing personal information on social media, engaging in unsafe browsing habits, and downloading unverified applications, can introduce malware and other malicious software onto shared home networks. As these devices potentially coexist within the same network environment, corporate devices become vulnerable to attacks, potentially paving the way for data breaches and compromising organizational security [11].

Teenagers, like many users, may practice poor cybersecurity habits, such as using weak passwords, neglecting software updates, and failing to employ encryption or multi-factor authentication. These vulnerabilities can significantly increase the potential for corporate exposure, as hackers can exploit the weakest link in the home network to infiltrate corporate resources.

1.3. Assess Teen Risk to Corporate Devices

We conducted a mixed methods survey with a variety of teens while respecting all applicable laws regarding contact with minors. A variety of questions were

asked regarding online habits and potential cybersecurity risks through negligence and exposure. The data collected from this survey provided valuable insights to decipher the prevalent cybersecurity risks and aid in formulating targeted strategies to enhance their digital safety and awareness.

To mitigate the risks arising from the presence of teen users in WFH environments, it is imperative for corporations to implement robust security protocols and proactive measures. Educating both teenagers and employees about the importance of cybersecurity best practices can foster a culture of vigilance and reduce the likelihood of falling victim to cyber threats.

By recognizing and addressing the specific risks associated with teen behavior online, organizations can strengthen their defenses and protect their valuable assets. This research seeks to raise awareness about this critical issue, encouraging stakeholders to prioritize cybersecurity education, employ appropriate security measures, and adopt strategies that safeguard against potential breaches and ensure the confidentiality and integrity of corporate data in the ever-evolving landscape of remote work [12].

In conclusion, this research underlines the urgent need for heightened awareness and proactive measures to address the cybersecurity risks arising from the presence of teenagers in WFH environments. Implementing robust security protocols, educating both teenagers and employees on cybersecurity best practices, and partitioning personal and corporate device usage are essential steps in safeguarding corporations against potential threats emanating from shared home networks. By understanding and addressing these risks, organizations can strengthen their defenses and minimize the likelihood of breaches, ensuring the safety and confidentiality of their sensitive data in the growing field of remote work.

2. Hypothesis

Teen-origin risks can migrate to WFH devices and eventually put corporate networks at risk. Despite the use of safeguards like VPNs, teen cybersecurity vulnerabilities present significant risks to WFH devices due to the migration of risks from the teen's to the parent's device over home networks. The problem arises from a combination of factors, including teen's limited awareness of cybersecurity risks, their inclination towards unsafe practices, and the lack of tailored education on safe online behavior. Despite some efforts to address the issue, our research contends that a comprehensive approach, encompassing targeted cybersecurity education for teens and the implementation of multi-layered security measures among corporations, is required to mitigate the risks effectively. The impact of this research extends beyond immediate risk reduction, fostering a more secure online environment and contributing to the creation of a cyber-aware generation capable of navigating the evolving cybersecurity landscape adeptly.

3. Survey Results

Quantitative and qualitative written surveys were used to survey 62 teens in the

age range of 14 - 18 years old. Teens were represented in a range of genders, socioeconomic status, and technological literacy. Surveyees participated voluntarily and provided personal information to provide credibility and ability for follow-up questions. All personal information is kept confidential. The study design allowed for administering the survey without violating any laws or customs regarding the surveying of minors. Teens were asked closed and open-ended questions about their online behaviors and cybersecurity practices. Our survey was based on a structured questionnaire. Teens were contacted through social networking and interviewed on phone or in person. Their responses were recorded and tabulated. If a question incorporated technical terminology, such as multi-factor authentication, additional information was imparted by the surveyor to clarify the question. Those surveyors who provided outlier responses were then contacted for a follow-up qualitative review to uncover the underlying reasons for their response and this information was useful in refining our aforementioned hypothesis.

The use of the surveys allows for the insight into specification of risks and quantification of vulnerabilities. The data collected through the survey can contribute to broader cybersecurity research, enrich the understanding of cybersecurity risks among different demographics and shed light on potential emerging threats.

Findings

As shown in **Figure 1**, a significant amount of teens live in households with access to WFH devices. Teens living in a household with WFH devices might expose those devices to potential cybersecurity vulnerabilities [13]. Given the growing prevalence of remote work setups, shared device and home network usage with family members worsen the risk of unintentional data exposure and unauthorized access to sensitive information.

Engaging in certain online activities carries inherent risks, including potential cybersecurity and legal concerns. For instance, accessing copyrighted content

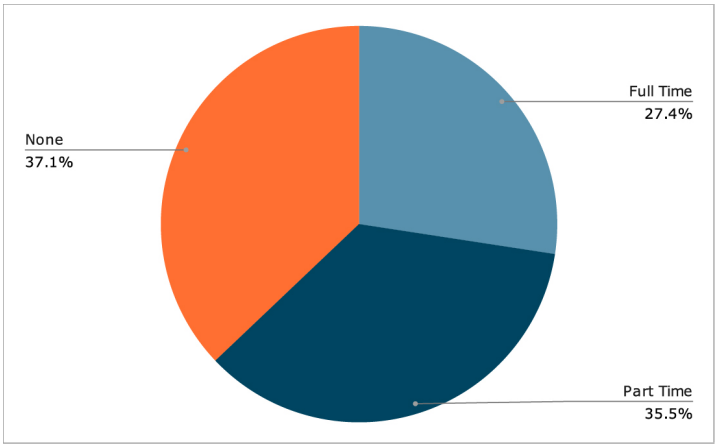

Figure 1. Teen's parents working from home.

through illegal streaming or downloads may lead to legal consequences due to copyright infringement. Similarly, downloading files from unauthorized sources could inadvertently introduce malware, viruses, or malicious software onto the user's device, jeopardizing its security and privacy. Additionally, clicking on foreign links, unknown texts, or emails poses a risk of falling prey to phishing attacks, wherein malicious entities attempt to steal sensitive information or deploy harmful software. Interacting with advertisements could inadvertently expose users to drive-by downloads or redirect them to phishing sites, leaving their personal data vulnerable [14]. Public networks may also be breeding grounds for cybercriminals, exposing users to eavesdropping and data interception. As illustrated in **Figure 2**, almost all teens surveyed access public networks. Even downloading free games from unofficial sources can lead to the inadvertent installation of malware, thus compromising device integrity. Furthermore, typographical errors in URLs can inadvertently direct users to malicious websites posing as legitimate ones, facilitating data theft or malware installation.

When drilling down the illegal access category, surveyors disclosed what forms of streaming and downloading they participated in. As shown in **Figure 3**, TV and sports streaming are common forms of illegal entertainment, which are accessed through disreputable and potentially malicious websites. Downloads are also potentially dangerous and are generally capable of delivering worse malware than attacks on a browser.

As shown in **Figure 4**, the majority of teens use just a couple of passwords for all their online accounts. Reusing passwords across multiple accounts presents an array of potential risks that users should be aware of. One significant concern is that a security breach on one platform may lead to unauthorized access to other accounts using the same password [15]. Cybercriminals are increasingly adept at exploiting this vulnerability, employing automated tools to gain access to various online services once they have compromised a single set of login credentials. This practice, known as "credential stuffing", puts users at heightened risk of identity theft, financial fraud, and privacy invasion. Furthermore, reusing passwords undermines the effectiveness of security measures such as two-factor

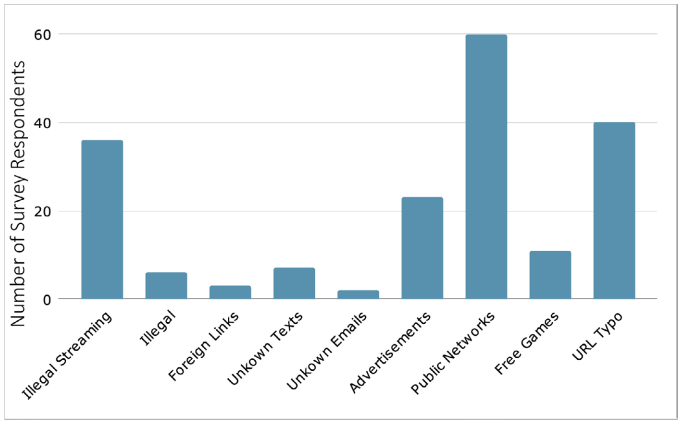

Figure 2. Teen vulnerability exposure.

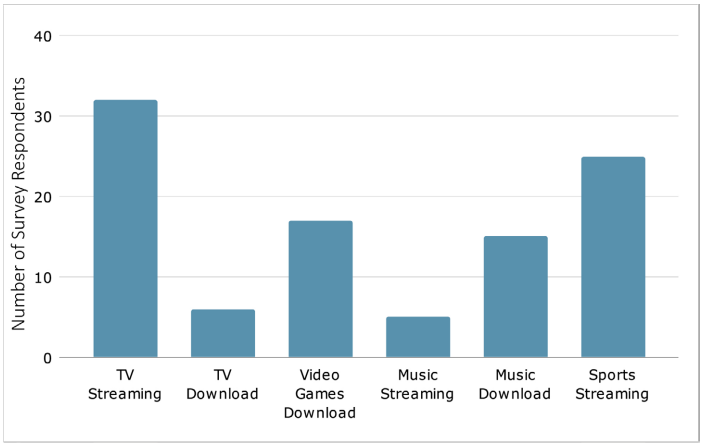

Figure 3. Illegal access of entertainment.

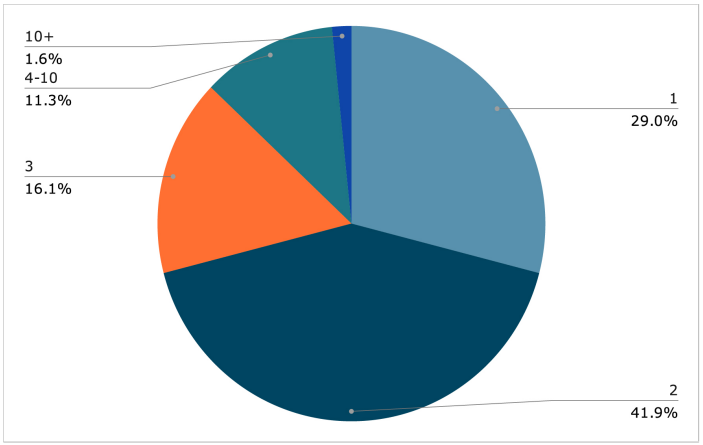

Figure 4. Number of passwords used.

authentication, rendering these additional layers of protection less effective against determined attackers.

As illustrated in **Figure 5**, the majority of teens do not use antivirus on their personal computers. When antivirus is used, it is commonly a free antivirus, and rarely paid for. Not utilizing antivirus protection or relying solely on free antivirus software introduces considerable cybersecurity risks that users should be cautious of. Without any antivirus, devices are left vulnerable to a wide range of malware, such as viruses, trojans, and ransomware, which can compromise sensitive data and harm system integrity [16]. Cybercriminals constantly exploit such unprotected systems, seeking to gain unauthorized access, steal personal information, or launch damaging cyberattacks. Moreover, opting for free antivirus solutions might provide basic protection but often lacks advanced features and timely updates that paid options offer. This limitation hinders the ability to detect and neutralize emerging threats effectively. As a result, users employing free antivirus software may be more susceptible to evolving malware and targeted attacks, potentially leading to severe consequences for both individuals and organizations.

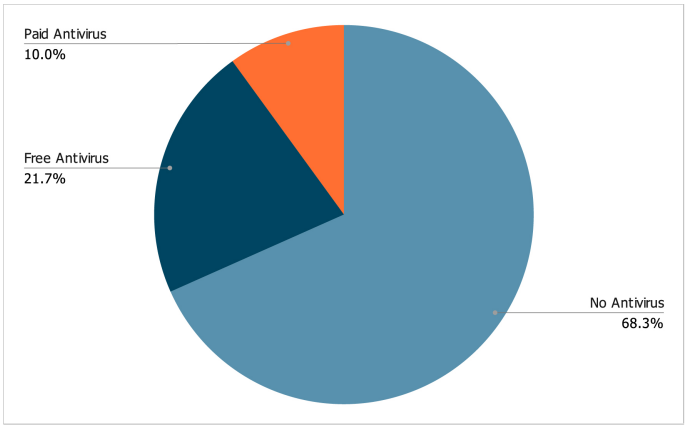

Figure 5. Antivirus use.

As presented in **Figure 6**, teens commonly accept friend requests from users with low numbers on mutual friends. This behavior exposes teens to potential social engineering attacks and privacy breaches [17]. Accepting requests from strangers or accounts with few mutual connections increases the likelihood of encountering fake profiles or malicious actors posing as friendly acquaintances. The percentage of teens who accept requests with no mutual relations are most vulnerable. These individuals may attempt to gather personal information or engage in phishing attempts, exploiting the trusting nature of teenagers. Furthermore, accepting such requests can lead to inadvertent exposure of private posts and personal details to unknown individuals, compromising online safety.

The variations in security levels among different internet browsers are a crucial aspect that necessitates careful consideration. As shown in **Figure 7**, teens use a variety of browsers, with Safari and Chrome as the most common. Each browser employs distinct security features and protocols to safeguard users from online threats. While some browsers may prioritize enhanced privacy and protection, others might focus on user-friendly features, which could potentially compromise security. Browser developers continually release updates and patches to address emerging vulnerabilities, but the effectiveness of these measures can differ significantly across browsers [18]. Moreover, some browsers may have more robust security extensions or built-in protections against malware, phishing, and other cyber risks. Browsers like Chrome and Safari have generally reputable security, while other browsers like TOR allow for access to disreputable or dangerous internet sites.

As illustrated in **Figure 8**, almost all teens surveyed do not use any form of VPN. VPN usage can offer security benefits for users, particularly when accessing the internet from public Wi-Fi networks or attempting to protect their online privacy [19]. The use of free VPNs comes with several notable downfalls. While they may appear appealing due to the absence of subscription fees, free VPN providers often have hidden costs. Some free VPNs might log and sell user's browsing data to advertisers or third parties, negating the very privacy they promise to protect [20]. The majority of teens surveyed use no VPN, indicating

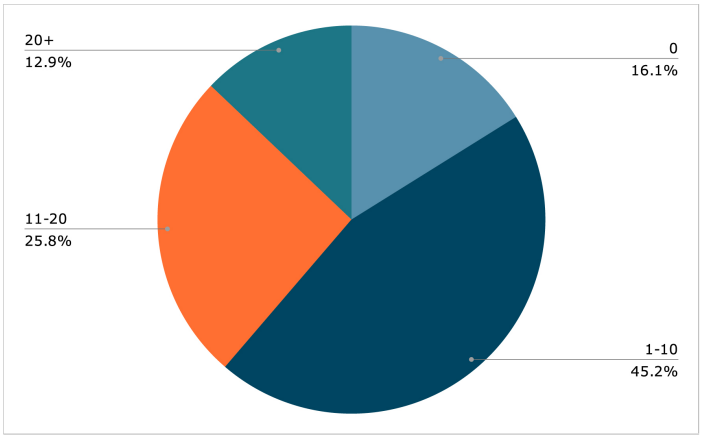

Figure 6. Number of mutual friends required to accept friend requests.

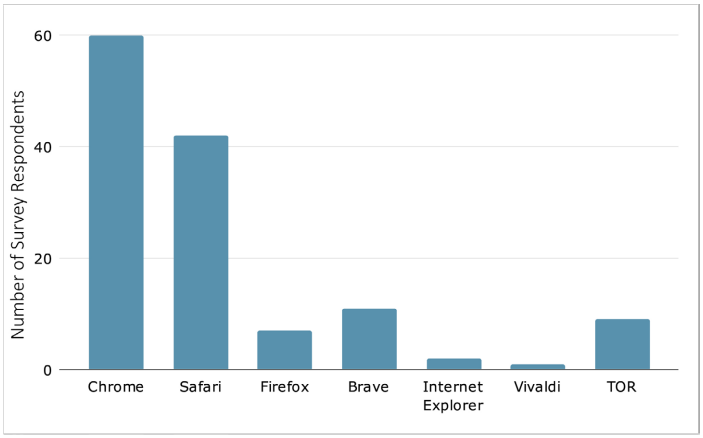

Figure 7. Internet browsers used.

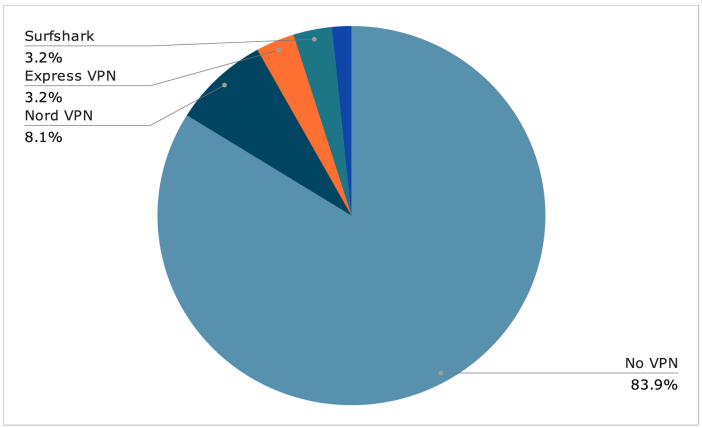

Figure 8. VPNs used.

they are at risk when accessing public networks or unsecured websites [21].

4. Migration Risk Assessment

For 20 unique attack vectors, the risk of migration of malware from a teen's device over a home network onto a WFH device can be categorized into Low, Me-

dium, and High risk categories. Different attacks are categorized into malware, social, distributed, parameter, and advanced. These 20 attack vectors are the most common and impactful attacks that are capable of exploiting this vulnerability. While other attacks exist, such as War Driving, Evil Twin, or Vishing attacks, the practical application of these attacks within the objectives of the research is negligible. War Driving attacks in which an attacker drives past buildings with insecure networks were responsible for corporate data breaches in the past, such as the Forever 21 data breach in 2017, but are likely ineffective against WFH devices due to the network overlap existing with residential communities. Evil Twin attacks where a malicious network access point is planted within a trusted network are effective, but usually require a technologically advanced malicious insider within a network, or in this case a household. While Vishing is a form of Phishing and is effective against employees, it requires a trained AI model to replicate the voice of employers which is a resource intensive operation unlikely to be used to coerce a base-level employee, and thus not relevant to our concerns about teen-origin migration risk.

The risk score is calculated based on the likelihood that a successful penetration by a given attack can fully compromise a user's device, then be sent through TCP and UDP packets in data streams over a WPA2 home network and being met with a three-way handshake FIN/ACK packet on a WFH device, regardless of VPN use. For example, teens may download games or entertainment from free distributors and unknowingly infect their devices. Without any actions by the teen, a teen's device infected with a worm can allow the worm to migrate to the home router. Thereafter it can travel over the home network onto a WFH device, infecting a corporation. A teen's personal device infected with spyware could be used to capture network traffic and compromise a WFH device, capturing corporate login information. When clicked, a link awarding a teen with money or any incentive can fully compromise any device. The teen may forward a compromised link to a WFH device, which in turn infects the corporation. A teen might purchase a used audio speaker or other auxiliary devices on eBay, unaware that it has corrupted firmware. When that device connects to WiFi it could exploit the home network and eventually the WFH devices.

4.1. Malware

Malware attacks refer to malicious activities in which cybercriminals use various forms of software or code to gain unauthorized access to systems, disrupt operations, steal sensitive information, or cause other harmful effects [22]. Malware is a broad term encompassing different types of malicious software, each with specific functionalities and objectives. Here are some common forms of malware attacks:

Trojans, being a staple attack vector, are a type of malware that cunningly masquerades as useful software. Teenagers, unaware of the risks, may inadvertently infect their devices when downloading games or entertainment from free dis-

tributors. Additionally, in their quest for better performance, teens might tinker with the home router's configuration settings, inadvertently compromising security and weakening firewalls. While WFH devices typically block downloads, the potential impact of a successful intrusion over the home network is immense and should not be underestimated.

Worms rank among the most destructive forms of malware, capable of autonomously traversing networks without user intervention. For example, if a teen's device becomes infected with a worm, it can spread to the home router without requiring any actions from the user. From there, it can easily propagate across the home network and infiltrate a WFH device, potentially infecting an entire corporation. Despite corporate VPNs aiming to keep connections private, worms and viruses often find ways to breach security before the transport layer of the OSI model, posing a significant threat to organizational cybersecurity [23].

Adware is a frequently encountered but relatively low-impact form of malware. However, when a trojan is downloaded, it may activate adware, leading to the display of intrusive ads and increased device resource usage. WFH devices are typically configured to block adware, minimizing the risk. For example, in the pursuit of time-sensitive shopping deals, teenagers might act impulsively. For instance, they may come across a lightning deal offering a significant discount on a popular sneaker. To capitalize on the opportunity, they could forward the deal link to a parent for purchase. Unfortunately, if the parent happens to be working from home at that moment, opening the link on a WFH device could inadvertently compromise both the device and the corporate network.

Spyware, a highly impactful malware, poses a significant challenge to detection. Operating stealthily in the background, it silently records and transmits all user input. If a keylogger is part of the spyware, it can clandestinely capture usernames and passwords as they are typed. For example, when a teen's personal device gets infected with spyware, it becomes a potential threat to the entire home network. The spyware could intercept network traffic, compromising a WFH device and gaining access to corporate login credentials. Although WFH devices are typically protected by VPNs, there are instances when the VPN may go offline, leaving the device vulnerable to spyware that originated from a different device within the home network [24]. Vigilance and robust security measures are essential to defend against such threats effectively.

Macro Viruses are a type of viruses that infect devices when viewing or editing text or photo documents. They are particularly prevalent in applications like Microsoft Word and Excel, where macros are commonly used. For example, while seeking homework or test answers innocently, a teen may open a seemingly harmless text document and unknowingly infect their device with a macro virus. Moreover, if a teen receives a fake email containing a document supposedly from their school, they might forward it to a parent's WFH device. If the parent opens the document, the macro virus embedded within it will be triggered, potentially causing harm to the WFH device. Awareness of this threat and cautious han-

dling of documents can help mitigate the risks posed by macro viruses.

In Table 1 below, we summarize the above discussion and perform a complete malware risk assessment.

Table 1. Malware risk assessment.

ATTACK VECTOR	TEEN'S DEVICE	HOME NETWORK	WFH DEVICE
Trojans	High	N/A	Medium
Worms	High	High	High
Adware	High	N/A	Low
Spyware	High	High	High
Macro Virus	Medium	N/A	High

VECTOR	WHAT	HOW
Trojans	Trojans are a staple attack vector. Trojans are malware that disguises themself as useful software.	Teens may download games or entertainment from free distributors and unknowingly infect their devices. To improve performance, the teen may also alter the home router's configuration settings, which inadvertently downgrades security or weakens firewalls. WFH devices are commonly configured to block downloads, but the impact of a successful intrusion over the home network is immense.
Worms	Worms are one of the most destructive malware. Worms are able to travel over networks without any action by users on devices.	Without any actions by the teen, a teen's device infected with a worm can allow the worm to migrate to the home router. Thereafter it can travel over the home network onto a WFH device, infecting a corporation. While corporate VPNs attempt to keep connections mostly private, worms and viruses often are able to infiltrate systems before the transport layer of the OSI model.
Adware	Adware is a common malware and generally low impact. A downloaded trojan may run adware, displaying ads and using up device resources. WFH devices are commonly configured to block adware.	A teen incentivized by a time-based shopping deal can act rashly. For example, a lightning deal on a hot sneaker at a deep discount. The link may be forwarded to a parent to purchase the product, and by chance, if the parent is on work hours, the link may be opened on a WFH device. This link can compromise the device and the corporate network.
Spyware	Spyware is a high-impact malware that is difficult to trace. Spyware may run in the background of a device, storing and transmitting all user input. A keylogger can capture usernames and passwords when typed in.	A teen's personal device infected with spyware could be used to capture network traffic and compromise a WFH device, capturing corporate login information. Although the WFH device is likely protected by the use of a VPN, sometimes the VPN can be offline and expose the device to spyware that originated on a different device within the home network.
Macro Virus	Macro Viruses are viruses that infect a device when viewing or editing a text or photo. Macro Viruses are most common in applications like Microsoft Word and Excel.	A teen looking for homework or test answers may open up a text document and inadvertently infect his device. A teen may also receive a fake email with a document that appears to be from school and forward it to a parent's WFH device, which will launch a macro virus when that document is opened.

4.2. Social Attacks

Social attacks refer to deceptive tactics used by cybercriminals to manipulate individuals into divulging sensitive information, providing access to systems, or performing certain actions that benefit the attacker. These attacks exploit human psychology and trust to bypass technical security measures and gain unauthorized access to data, systems, or networks [25].

Unsecured public networks present a significant risk for malicious actors, often referred to as black hats. Data transmitted over such networks is unencrypted, making it vulnerable to sniffing and various Man-in-the-Middle (MITM) attacks, like session hijacking. WFH devices connected to public networks become high-risk, high-impact targets. To mitigate these risks, it is essential to connect only to password-protected WPA2 or WPA3 networks. For example, teens accessing public networks at school or cafes may unknowingly expose themselves to sniffing and packet capture, potentially leading to data breaches or malware infections. Vulnerabilities exposed on public networks can extend to the home network, making WFH devices susceptible to attacks. Even when using Virtual Private Network (VPN) tunneling for corporate network access, complete security cannot be guaranteed, creating a false sense of safety. In cases where VPN kill switches fail, WFH devices may be temporarily exposed to public network traffic, offering malicious hackers the opportunity to intrude and establish back doors [26]. Careful network selection and reliable VPN solutions are crucial for maintaining cybersecurity while using public networks.

Phishing remains highly effective, especially among users lacking cybersecurity awareness, with youth and teens being common targets. Despite efforts to educate WFH users about detecting phishing attempts, it still accounts for the majority of corporate breaches. For example, a seemingly innocent link promising money or incentives can fully compromise a teen's device when clicked. If the teen unknowingly forwards the compromised link to a WFH device, it can then infect the entire corporation, creating a pathway for potential security breaches. Vigilance and continuous cybersecurity training are essential to combat this pervasive threat.

Social Engineering is a wide-ranging term covering malicious actions that target humans instead of computers. Its potency lies in exploiting the weakest link in cybersecurity: humans themselves. Often, teens fall victim to catfishing, where they unknowingly share personal details, leaving them vulnerable to exploitation. Such exploits enable attackers to traverse networks and gain access to WFH devices. Remote workers, in particular, are susceptible to instructions from an attacker impersonating a superior, potentially leading to actions that undermine the security of their own corporation. Heightened awareness and education on Social Engineering are essential to safeguard against these manipulative tactics.

In Table 2 below, we summarize the above discussion and perform a complete social attacks risk assessment.

Table 2. Social attacks risk assessment.

ATTACK VECTOR	TEEN'S DEVICE	HOME NETWORK	WFH DEVICE
Public Network	High	N/A	Medium
Phishing	High	N/A	Medium
Social Engineering	High	High	High

VECTOR	WHAT	HOW
Public Network	An unsecured public network is a ripe attack vector for black hats. Data in transit will be unencrypted, vulnerable to sniffing, and various MITM attacks like session hijacking. WFH devices on public networks will be high-risk, high-impact targets. Only join password-protected WPA2 or WPA3 networks.	A teen accessing a public network at school or at a cafe may inadvertently expose them to sniffing and packet capture. Vulnerability exposure can lead to infection, and WFH devices are susceptible once on a home network. WFH devices on public networks are susceptible as well. VPN tunneling to corporate network access is rarely foolproof and often gives a false sense of security. When VPN kill switches fail, WFH devices may be temporarily exposed to public network traffic, giving malicious hackers more than enough time to intrude and create back doors.
Phishing	Phishing is extremely successful with users uneducated about cybersecurity, and commonly targets youth and teens. WFH users may be educated to detect phishing attempts, yet phishing accounts for most corporate breaches.	When clicked, a link awarding a teen with money or any incentive can fully compromise any device. The teen may forward a compromised link to a WFH device, which in turn infects the corporation.
Social Engineering	Social Engineering is a broad term that encompasses all malicious actions targeting humans rather than computers. Social Engineering can be extremely powerful and effective, as it exploits the weakest link in cyber security, humans.	Commonly, teens are catfished into giving out personal details, allowing exploitation of a home network. This channel allows attackers to travel over the network to WFH devices. The malicious actor may then instruct remote workers to undermine their corporation by impersonating a superior.

4.3. Distributed Attacks

Distributed attacks are a type of cybersecurity threat in which multiple compromised devices, often referred to as a botnet, work collectively to carry out an attack. The distributed nature of these attacks makes them more challenging to defend against, as they leverage numerous resources and attack vectors simultaneously.

Denial of Service (DoS) attacks, while uncommon, can cause significant disruptions to corporations. These attacks are usually not directed at individuals, but a compromised device belonging to an individual can be weaponized to launch a DoS attack against a network or a WFH device, ultimately affecting the entire corporation's network. If a teen's device on a home network becomes infected with common malware, it can easily spread through the router and infect a WFH device. In scenarios where the malicious actor's objective is to bring down a corporation rather than steal from it, they may opt for a DoS attack. Even if a VPN safeguards the connection between the WFH device and the corporate network,

the VPN itself can fall victim to a DoS attack. Spoofing outgoing VPN connections via session flood can overwhelm the VPN's resource allocation, leading to potential service disruptions. Vigilance and strong cybersecurity measures are essential to protect against such attacks.

Ransomware is an extremely profitable method of attack that involves capturing sensitive information and demanding a ransom for its release. Even teenagers are not immune to this threat. For example, embarrassing or illegal messages, photos, or videos may be seized and used as leverage for extortion. In some cases, victims are coerced into carrying out secretive actions, like compromising their employers, such as a teen being manipulated into downloading malware on a parent's WFH device. Lucrative information is often transmitted through VPN tunnels, as users may falsely believe that VPNs provide complete security, unwittingly aiding black hat hackers in their data capture endeavors. Unfortunately, many corporations targeted by ransomware find themselves with little choice but to pay the exorbitant ransom demands to safeguard their sensitive information. Vigilance, robust security measures, and proper education on cybersecurity are essential in combating this lucrative and damaging form of attack.

A Watering Hole Attack involves a deceptive tactic where a commonly visited website suddenly becomes malicious or gets hijacked, leading to the infection of trusting users. Teens who frequent illegal movie streaming may come across a site that appears safe. However, teens may access the site and expose themselves to previously inactive malware. Once the user's trust is established, the attackers exploit it to inject malware into the teen's device. While WFH devices are sometimes configured to prevent Watering Hole Attacks, it's worth noting that the attack vector may still originate from a website trusted by the corporation. Vigilance and stringent security measures are crucial in defending against this stealthy and dangerous form of cyberattack.

IoT Attacks involve the manipulation of household network devices such as thermostats and AI assistants to target other devices connected to the same network. For instance, an unsuspecting teenager might acquire a second-hand audio speaker or other auxiliary gadgets from an online marketplace like eBay, without realizing that these devices have been compromised with malicious firmware. Once these compromised devices join the WiFi network, they can be used to exploit vulnerabilities within the home network and potentially compromise WFH devices [27]. Despite the use of VPNs, it's often challenging to prevent IoT attacks because the IoT devices have unrestricted access within the network using full credentials [28].

In **Table 3** below, we summarize the above discussion and perform a complete distributed attacks risk assessment.

4.4. Parameter Attacks

Parameter attacks, also known as injection attacks, are a type of cybersecurity threat that exploits vulnerabilities in applications or systems where user-supplied

Table 3. Distributed attacks risk assessment.

ATTACK VECTOR	TEEN'S DEVICE	HOME NETWORK	WFH DEVICE
Denial of Service	Low	High	High
Ransomware	Medium	N/A	High
Watering Hole Attack	High	N/A	Medium
IoT Attack	Medium	High	Medium

VECTOR	WHAT	HOW
Denial of Service	Denial of Service is an uncommon attack but can be disruptive to corporations. DOS is rarely used on individuals, but any individual's device may be compromised with malware to perform a DOS against a network or a WFH device to bring down a corporation's network.	Any common malware infected on a home network through a teen's device can spread through the router onto a WFH device. If the malicious actor's goal is to bring down a corporation rather than steal from it, then a DOS attack can be performed. If a VPN guards the connection between the WFH device and the corporate network, the VPN itself can be a victim of DOS. Outgoing VPN connections can be spoofed via session flood, overloading the VPN's resource allocation.
Ransom-Ware	Ransomware is a highly lucrative attack vector involving the capture of information for ransom.	A teen's embarrassing or illegal messages, photos, or videos may be captured and held for ransom. Victims may be coerced into performing clandestine acts, commonly compromising their employers, such as a teen being coerced into downloading malware on a parent's WFH device. Lucrative information is often passed through VPN tunnels due to a false sense of security provided by VPNs, allowing for better data capture by black hats. Corporations victim to ransomware often have no choice but to pay the egregious ransom.
Watering Hole Attack	A Watering Hole Attack is a website commonly used that suddenly turns malicious or is hijacked, and trusting users are infected.	Teens going to illegal movie streaming sites may trust one as it has never had malware. Once trust has been established, it is exploited to infect a user's device with malware. WFH devices are sometimes configured to prevent WHA, but many times the attack vector is from a site trusted by the corporation.
IoT Attack	Internet of Things Attacks uses home network devices like thermostats or AI assistants to exploit devices connected to the network.	A teen might purchase a used audio speaker or other auxiliary devices on eBay, unaware that it has corrupted firmware. When that device connects to WiFi it could exploit the home network and eventually the WFH devices. VPNs are many times unable to prevent IOT attacks due to IOT devices residing inside of the network with full credentialed access.

data is not properly validated or sanitized before being processed. In these attacks, malicious inputs are inserted into input fields or parameters, tricking the application into executing unintended commands or actions. The goal of parameter injection attacks is to manipulate the application's behavior to gain unauthorized access, extract sensitive information, or execute arbitrary code.

SQL Injection is an attack primarily directed at websites or services, with individuals rarely being targeted. However, a WFH device infected with malware can become a conduit for SQL code injection into a corporate website or database, potentially leading to privilege escalation and exploitation. Once a WFH device

is compromised, it may grant remote access to a malicious actor, enabling them to inject false queries into a corporate parameter. This can be further exacerbated if the attacker gains access using the WFH user's credentials, allowing for privilege escalation. However, it's worth noting that this path of attack is highly improbable, so there's no immediate need for significant concern. Nevertheless, it's crucial to maintain robust cybersecurity practices and implement security measures to safeguard WFH devices and corporate networks against potential SQL Injection and other cyber threats. Prevention and vigilance remain key to maintaining a secure digital environment.

Cross-Site Scripting (XSS), akin to SQL Injection, involves injecting malicious reference code into a parameter, primarily targeting corporate websites and databases, leading to insecure referencing of the user interface. Much like SQL Injection, an infected device on the network can open the door for a cross-browser directory traversal attack, potentially compromising a corporate device. The presence of appliance sprawl in corporate architecture can increase the vulnerability to XSS attacks, mainly due to insufficient patch management and application hardening. To bolster cybersecurity defenses, proactive measures such as regular patch updates and robust application hardening practices should be implemented across corporate networks. This will help mitigate the risks associated with XSS attacks and ensure a safer digital environment for both companies and their users.

Credential Stuffing is a potent attack method wherein a list of usernames and passwords obtained from one platform is used to gain unauthorized access to another platform. This attack proves highly effective, especially after a single data breach that exposes user credentials. For example, a teen who unknowingly uses their parent's username and password on a website with a known data leak could inadvertently compromise the parent's corporate login. Many remote workers fall into the habit of reusing the same password or a couple of passwords across multiple platforms, making them vulnerable to such attacks. As such, it's essential for individuals to practice good password hygiene, employing unique and strong passwords for each platform to mitigate the risks associated with Credential Stuffing.

A Brute Force attack is a method wherein random strings of characters are repeatedly input into parameters to gain unauthorized access. These attacks have low probabilities of success and are highly resourceintensive. While Brute Force attacks are not commonly employed against individuals, social engineering can be used to target a teen, granting access to their home network. Once inside, the attacker may proceed with a brute force attack on the corporate network's login or capture login elements to execute an offline brute force attack, evading detection. VPNs or firewalls often struggle to thwart Brute Force attacks, as attackers exploit legitimate surfaces of applications or websites for their malicious intents. Comprehensive cybersecurity measures, including strong authentication protocols and regular updates, are essential to safeguard against such attacks.

In Table 4 below, we summarize the above discussion and perform a complete parameter attacks risk assessment.

4.5. Chain Attacks

Chain attacks, also known as chained attacks, refer to cyber threats that involve the combination of multiple attack techniques or exploits in a coordinated manner to achieve a specific objective. These attacks are complex and sophisticated, leveraging various vulnerabilities and attack vectors to evade detection and accomplish their goals. The term "chain" signifies the sequential execution

Table 4. Parameter attacks risk assessment.

ATTACK VECTOR	TEEN'S DEVICE	HOME NETWORK	WFH DEVICE
SQL Injection	N/A	N/A	Low
Cross-Site Scripting	Low	N/A	Low
Credential Stuffing	High	Low	High
Brute Force Attack	Low	Low	Low

VECTOR	WHAT	HOW
SQL Injection	SQL Injection is an attack targeted towards websites or services and rarely targets individuals. Malware on a WFH device may allow SQL code injection into a corporate website or database, allowing for privilege escalation and exploitation.	An infected WFH device may allow remote access for a black hat to inject false queries into a corporate parameter, with the added bonus of privilege escalation from the WFH user's credentials. However, this is an extremely unlikely path of attack hence we need not worry about it.
Cross-Site Scripting	Cross-Site Scripting, similar to SQL Injection, may inject malicious reference code into a parameter. Corporate websites and databases are targeted to allow for insecure referencing of a user interface.	Similar attack methodology as SQL Injection. An infected device over the network may allow a cross-browser directory, compromising a corporate device. Teens accessing streaming websites with certain cookies enabled that run Javascript could allow for XSS attacks. Appliance sprawl in WFH corporate architecture can lead to XSS attacks due to a lack of patch management and application hardening.
Credential Stuffing	Credential Stuffing is an attack where a set of usernames and passwords is discovered on a platform, and those credentials are used to gain access to another platform. Credential Stuffing is highly effective for targeting users after a single data breach.	A teen who uses a parent's username and password on a website with a data leak may inadvertently compromise the parent's corporate login, as many remote workers reuse just a single or a couple of passwords for all platforms.
Brute Force Attack	A Brute Force attack is an attack that inputs random strings of characters into parameters to attempt to gain access. Brute Force attacks have low probabilities of being successful and are extremely resource intensive.	Although brute force attacks are not commonly used to target individuals, social engineering may be used on a teen to gain access into a home network, allowing the black hat to brute force attack the login to a corporate network or capture login elements and brute force attack offline to avoid detection. VPNs or firewalls struggle to stop brute force attacks as many brute force attacks are employed through a legitimate surface of an application or website.

of different attack stages, with each stage building upon the success of the previous one [29].

MITM attack has severe consequences as it enables a black hat to intercept, capture, and replay data exchanged between devices and networks. For instance, if teens access an illicit website, they could become a victim of a Man-in-the-Middle (MITM) attack. The attacker could then intrude on the home network and exploit a third-party VPN connecting the teen's WFH device to a corporate database. Once inside, the attacker gains access to outgoing connections, allowing them to capture or spoof data undetected. Vigilance in online activities and strong security measures are crucial in protecting against such dangerous MITM attacks.

This form of attack specifically targets user devices during product transit, wherein malicious services are uploaded onto legitimate products through physical capture or insider involvement. Imagine a scenario where a teen purchases a phone from a third-party seller offering a tempting discount. Unfortunately, the phone comes pre-installed with malware that, upon connection to the home network, spreads to the WFH device. Additionally, the WFH device could be intercepted while in transit, have spyware installed, and then be put back into transit. Such a supply chain attack may also occur at the software level, where corporate VPNs could be compromised before being implemented at client companies. As a result, VPN spyware or data capture could be covertly configured at the root level. To prevent and detect such attacks, heightened awareness, careful purchasing practices, and robust cybersecurity measures are crucial at both individual and corporate levels.

In Table 5 below, we summarize the above discussion and perform a complete chain attacks risk assessment.

Table 5. Chain attacks risk assessment.

ATTACK VECTOR	TEEN'S DEVICE	HOME NETWORK	WFH DEVICE
Man in the Middle	High	High	High
Supply Chain Attack	Low	High	Low

VECTOR	WHAT	HOW
Man in the Middle	This is a high-impact attack and allows a black hat to sniff, capture, and replay traffic between devices and networks.	A teen accessing an illicit website may be a victim of MITM, which may intrude on the home network and gain access to a WFH device's corporate connection through a third-party VPN connecting the WFH device to a corporate database. Once access has been gained, outgoing connections may be captured or spoofed.
Supply Chain Attack	This targets user devices while the products are in transit, and it uploads malicious services to legitimate products through physical capture or a malicious insider.	A teen that buys a phone through a third-party seller that offers a lower price may inadvertently expose the home network to malware pre-installed on the device. The malware can spread over the network to a WFH device, or possibly a WFH device could be captured in transit, have spyware installed, then put back in transit. A supply chain attack could also occur at the software level. Corporate VPNs could be hijacked before implementation at client companies, and a form of VPN spyware or data capture could be configured at the root level.

4.6. Advanced Attacks

Advanced attacks are highly sophisticated and stealthy cyberattacks carried out by skilled and well-funded adversaries, such as nation-state actors, organized cybercrime groups, or advanced hacking organizations. These attacks are characterized by their ability to remain undetected for extended periods, often spanning weeks, months, or even years, as the attackers meticulously plan and execute their objectives.

An Advanced Persistent Threat (APT) refers to a stealthy attacker that remains undetected within a network or device for an extended period. For instance, if a teen's device gets infected and becomes part of an APT, it could serve as the starting point for the attack, moving through the router to infiltrate the network. APTs typically target high-level entities and can traverse from a WFH device into a company's database, hiding within VPN tunnels or operating system rootkits. These APTs consistently gather sensitive company information while avoiding detection. Even after seemingly remedying the APT, backdoors installed at the kernel level may allow for re-entry, creating an ongoing security challenge. Vigilance, sophisticated cybersecurity tools, and regular security audits are essential in detecting and mitigating APTs to protect valuable company assets.

A Zero Day Attack (ZDA) represents the most perilous form of cyber attack. It involves a completely novel attack that lacks any known patches or preventive measures. Some of the largest and most notorious cyber attacks in history fall under the category of ZDAs, with the potential to cripple nation-states or sabotage critical infrastructure, like the infamous Stuxnet attack that targeted nuclear weapons centrifuges. A ZDA can manifest in various ways, making it extremely challenging to defend against. Large tech corporations are particularly vulnerable targets for such attacks. The ramifications of a ZDA can be catastrophic, ranging from theft of critical intellectual property to the compromise of entire company databases. Due to their unpredictable nature and lack of preventive measures, ZDAs pose an ongoing and formidable threat to cybersecurity worldwide. Proactive security measures, constant vigilance, and prompt responses are vital in minimizing the impact of these highly dangerous attacks.

In Table 6 below, we summarize the above discussion and perform a complete advanced attacks risk assessment.

5. Recommendations

To enhance the online safety of a WFH environment where teens are present, a multifaceted approach is essential. This is particularly important when parents work with confidential corporate information, such as financial projections or product roadmaps. They might find that their kids are targeted by hackers who seek an easier entry-point to home networks and eventually their WFH devices.

First and foremost, comprehensive cybersecurity education programs should be developed to equip teenagers with the knowledge and skills needed to protect themselves in the digital realm. These programs should prioritize topics such as

Table 6. Advanced attacks risk assessment.

ATTACK VECTOR	TEEN'S DEVICE	HOME NETWORK	WFH DEVICE
Advanced Persistent Threat	Low	Low	High
Zero Day Attack	High	High	High

VECTOR	WHAT	HOW
Advanced Persistent Threat	An Advanced Persistent Threat is an attacker that exists in a network or device for an extended amount of time without detection.	A teen's infected device on a network can be the starting point for an APT and may travel over the router. An APT generally targets high-level targets and may travel from a WFH device into a company database, residing inside of VPN tunnels or through operating system rootkits which are consistently collecting company information while avoiding detection. Even when an APT has been seemingly remediated, backdoors installed at the kernel level by APTs often allow for re-entry.
Zero Day Attack	A Zero Day Attack is the most dangerous cyber attack. A ZDA is an original attack that has no known patch or prevention. The largest cyber attacks in history are ZDA. A ZDA can bring down nation-states or self-destruct nuclear weapons centrifuges, such as the well-known Stuxnet attack.	On a home network that hosts both teen and parent devices, A ZDA can happen in almost any manner, and it is near impossible to defend against. Large tech corporations are prime targets of ZDAs. A ZDA can steal critical intellectual property or even the databases of companies.

password best practices, and teach teens the importance of using strong, unique passwords for each online account. Encouraging the adoption of password managers can further enhance security by generating and securely storing complex passwords [30].

Another critical aspect of safeguarding online activities is recognizing and avoiding phishing attempts. By educating teenagers about the telltale signs of phishing emails and malicious links, they can become more vigilant in their online interactions. To further bolster data protection, the use of corporate VPNs or reputable VPN services with strong encryption should be promoted, especially when accessing work-related materials or using public Wi-Fi networks. VPNs create a secure tunnel for data transmission, shielding sensitive information from potential cyber threats.

Moreover, staying vigilant against potential cybersecurity risks is paramount. Regularly updating the operating system, applications, and antivirus software on WFH devices ensures that known vulnerabilities are patched, making it more challenging for cybercriminals to exploit weaknesses. Caution should be exercised with emails and links, especially those from unknown sources, to avoid falling victim to phishing and malware attacks.

Teenagers should also be mindful of their online presence, avoiding oversharing personal information on social media platforms and other online spaces. Awareness of the risks associated with sharing sensitive details can protect them from identity theft and social engineering attempts.

Promoting safe browsing habits is equally crucial. Discouraging the down-

loading of apps from unofficial sources and encouraging the use of ad-blockers and avoiding suspicious websites helps reduce the likelihood of encountering malware and other cybersecurity threats.

In the event of cyber incidents, regular device backups serve as a safety net, protecting against data loss and minimizing the potential impact of such incidents. Encouraging teens to back up their important data regularly fosters a proactive approach to cybersecurity.

Beyond technical measures, fostering open communication and creating a supportive environment for teenagers to discuss cybersecurity concerns is vital. By providing accessible resources and helplines, teens can seek assistance when facing potential threats or cyber-related issues.

Through the collective implementation of these recommendations, teens can develop a strong cybersecurity mindset, enabling them to navigate the online world with increased safety and confidence. By empowering them with the knowledge and tools to protect their WFH devices, we can ensure that the younger generation engages responsibly in the digital landscape, safeguarding their personal data and minimizing cybersecurity risks.

5.1. Implementation of Mitigations

a) Device Segmentation and Network Isolation: Companies could implement strategies to segment and isolate home networks used for work from the ones used by teenagers. This could involve setting up separate network segments for work devices and personal devices. Access controls and firewall rules could be configured to limit communication between these segments, reducing the likelihood of risk migration.

b) Employee Training and Awareness: Companies should provide comprehensive cybersecurity training to employees, especially those who work with sensitive corporate information. This training should cover safe online practices for both work and personal use. Employees should be educated about the risks posed by their teenagers' online activities and how these risks can affect corporate security.

c) Endpoint Security Solutions: Deploying advanced endpoint security solutions on parent's WFH devices can help detect and prevent potential threats originating from teenagers' online activities. These solutions could include advanced antivirus, anti-malware, and intrusion detection systems.

d) Security Monitoring and Incident Response: Establishing continuous security monitoring of both corporate networks and WFH devices can help identify any unusual activities or potential breaches. A well-defined incident response plan should be in place to address any security incidents promptly.

5.2. Effects on Workflows

a) Workflow Adjustments: The implementation of these mitigations might require employees to follow new protocols when accessing corporate resources

from home. They might need to log in through secure virtual environments or use company-provided devices with enhanced security configurations.

b) Increased Security Awareness: Employees, especially those who are parents, will need to be more vigilant about their teenagers' online activities. This heightened awareness might lead to more cautious internet usage at home and increased communication between employees and their children regarding safe online practices.

c) Potential Productivity Impact: While implementing these measures is crucial for security, there could be a short-term impact on productivity as employees adjust to new security protocols and systems. However, over time, these adjustments should become part of the normal routine.

d) Enhanced Work-Life Balance: The implementation of these mitigations could contribute to a healthier work-life balance for employees, as the clear separation of work and personal network activities may reduce the stress of potential security breaches affecting both domains.

6. Conclusions

In conclusion, the expanding trend of remote work in corporations has led to a significant increase in the use of personal devices, introducing a multitude of cybersecurity risks, especially when shared with teenagers on home networks. This research has delved into the potential threats arising from teenagers' online activities and their implications for WFH devices and corporate security, even in the presence of defensive measures like VPNs. The survey of 62 teens provides valuable insights into the prevalence of risky online behavior, emphasizing the need to address these risks to protect corporate networks from potential risk migration.

The study underscores the importance of educating both teenagers and employees on cybersecurity best practices to foster a culture of vigilance and reduce the likelihood of falling victim to cyber threats. Furthermore, the interconnected nature of home networks, where personal and corporate devices share the same Wi-Fi, highlights the need for enhanced security measures on personal and corporate devices. Robust passwords, regular software patching, and encryption are essential to fortify the defenses against potential breaches and unauthorized access.

By recognizing and addressing the specific risks associated with teenagers' behaviors online, organizations can strengthen their security posture, safeguard valuable assets, and maintain the confidentiality and integrity of corporate data in the evolving landscape of remote work. As corporations prioritize cybersecurity education, implement proactive measures, and partition personal and corporate device usage, they can navigate the challenges presented by the presence of teenagers in WFH environments. The findings of this research serve as a call to action for stakeholders to address this critical issue, enhancing cybersecurity awareness and resilience to ensure a safe and secure digital ecosystem for remote

work operations.

WFH parents who have access to sensitive corporate data, such as financial projections or product roadmaps, are particularly at risk of teen-origin risks. Such parents and their employers should take extra precautions to mitigate the migration of threats from teen devices to WFH devices. They should be vigilant about the risk that their teens might be targeted by hackers who seek an easier entry-point to home networks and eventually their WFH devices.

This study makes a significant contribution to existing knowledge by addressing the evolving cybersecurity landscape in the context of teenagers' online activities impacting parents' work-from-home (WFH) devices. It sheds light on a novel risk migration phenomenon that has implications for corporate security. By analyzing the potential contamination of parents' WFH devices with risks originating from their teenagers' online behaviors, the study provides insights into an understudied area of cybersecurity. The research extends beyond traditional cyber threats and explores how personal online habits can inadvertently affect corporate networks, offering a new perspective on risk assessment and mitigation.

The practical significance of this study is twofold, both for the industry and academia. In the industry, the findings offer actionable insights for organizations grappling with the increasing trend of hybrid work models. The study's recommendations for implementing mitigation strategies provide a roadmap for companies to safeguard their corporate networks while enabling employees to work from home effectively. Moreover, the study emphasizes the necessity of cybersecurity awareness among employees who are parents, fostering a safer digital environment for both personal and professional activities. For academia, the research fills a gap in the understanding of risk migration and its intersection with the emerging hybrid work landscape. It establishes a foundation for further exploration and offers a framework for assessing and managing cyber risks that originate outside traditional threat vectors. In sum, this study contributes valuable insights to enhance cybersecurity practices and underscores the imperative of adapting to evolving technological and work patterns.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] De Smidt, G. And Botzen, W. (2018) Perceptions of Corporate Cyber Risks and Insurance Decision-Making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, **43**, 239-274. https://doi.org/10.1057/s41288-018-0082-7

[2] Popovici, V. And Popovici, A.L. (2020) Remote Work Revolution: Current Opportunities and Challenges for Organizations. *Ovidius University Annals, Economic Sciences Series*, **XX**, 468-472.

[3] Adeyinka, O (2008) Analysis of Problems Associated with IPSec VPN Technology.

2008 *Canadian Conference on Electrical and Computer Engineering*, Niagara Falls, 4-7 May 2008, 001903-001908. https://doi.org/10.1109/CCECE.2008.4564875

[4] Brynjolfsson, E., Horton, J.J., Ozimek, A., Rock, D., Sharma, G. and TuYe, H.Y. (2020) COVID-19 and Remote Work: An Early Look at US Data (No. w27344). National Bureau of Economic Research. https://doi.org/10.3386/w27344

[5] Selwyn, N. (2010) Schools and Schooling in the Digital Age: A Critical Analysis. Routledge, London. https://doi.org/10.4324/9780203840795

[6] Adorjan, M. and Ricciardelli, R. (2018) Cyber-Risk and Youth: Digital Citizenship, Privacy and Surveillance. Routledge, London. https://doi.org/10.4324/9781315158686

[7] Xiong, J. and Jamieson, K. (2013) SecureArray: Improving Wifi Security with Fine-Grained Physical-Layer Information. *Proceedings of the* 19*th Annual International Conference on Mobile Computing & Networking*, Florida, 30 September-4 October 2013, 441-452. https://doi.org/10.1145/2500423.2500444

[8] Mahmood, T. and Afzal, U. (2013) Security Analytics: Big Data Analytics for Cybersecurity: A Review of Trends, Techniques and Tools. 2013 2*nd National Conference on Information Assurance*, Rawalpindi, 11-12 December 2013, 129-134. https://doi.org/10.1109/NCIA.2013.6725337

[9] Berger, T. (2006) Analysis of Current VPN Technologies. *First International Conference on Availability, Reliability and Security*, Vienna, 20-22 April 2006, 8-115. https://doi.org/10.1109/ARES.2006.30

[10] Willard, N.E. (2007) Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn to Use the Internet Safely and Responsibly. John Wiley & Sons, New York.

[11] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015) Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, **22**, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

[12] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F. and Choo, K.K.R. (2022) The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. *Computers & Security*, **119**, Article ID: 102754. https://doi.org/10.1016/j.cose.2022.102754

[13] Haan, K. (2023) Remote Work Statistics & Trends. Forbes Advisor. https://www.forbes.com/

[14] Dhamija, R., Tygar, J.D. and Hearst, M. (2006) Why Phishing Works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Montréal, 22-27 April 2006, 581-590. https://doi.org/10.1145/1124772.1124861

[15] Florencio, D. and Herley, C. (2007) A Large-Scale Study of Web Password Habits. *Proceedings of the* 16*th International Conference on World Wide Web*, Banff, 8-12 May 2007, 657-666. https://doi.org/10.1145/1242572.1242661

[16] Sukwong, O., Kim, H. and Hoe, J. (2011) Commercial Antivirus Software Effectiveness: An Empirical Study. *Computer*, **44**, 63-70. https://doi.org/10.1109/MC.2010.187

[17] Herath, T.B., Khanna, P. and Ahmed, M. (2022) Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, **2**, 1-18. https://doi.org/10.3390/jcp2010001

[18] Ter Louw, M., Lim, J.S. and Venkatakrishnan, V.N. (2008) Enhancing Web Browser Security against Malware Extensions. *Journal in Computer Virology*, **4**, 179-195. https://doi.org/10.1007/s11416-007-0078-5

[19] Singh, A.K., Samaddar, S.G. and Misra, A.K. (2012) Enhancing VPN Security through

Security Policy Management. 2012 1*st International Conference on Recent Advances in Information Technology* (*RAIT*), Dhanbad, 15-17 March 2012, 137-142. https://doi.org/10.1109/RAIT.2012.6194494

[20] Khan, M.T., DeBlasio, J., Voelker, G.M., Snoeren, A.C., Kanich, C. and Vallina-Rodriguez, N. (2018) An Empirical Analysis of the Commercial VPN Ecosystem. *Proceedings of the Internet Measurement Conference* 2018, Boston, 31 October-2 November 2018, 443-456. https://doi.org/10.1145/3278532.3278570

[21] Szabo, N. (1997) Formalizing and Securing Relationships on Public Networks. *First Monday*, **2**, page. https://doi.org/10.5210/fm.v2i9.548

[22] Rieck, K., Holz, T., Willems, C., Düssel, P. and Laskov, P. (2008) Learning and Classification of Malware Behavior. In: Zamboni, D., Ed., *DIMVA* 2008: *Detection of Intrusions and Malware*, *and Vulnerability Assessment*, Springer, Berlin, 108-125. https://doi.org/10.1007/978-3-540-70542-0_6

[23] Geers, K. (2010) The Challenge of Cyber Attack Deterrence. *Computer Law & Security Review*, **26**, 298-303. https://doi.org/10.1016/j.clsr.2010.03.003

[24] Li, S.M. and Liang, H.Y. (2011) A Model of Path Fault Recovery of MPLS VPN and Simulation. 2011 *International Conference on Electric Information and Control Engineering*, Wuhan, 15-17 April 2011, 1925-1928. https://doi.org/10.1109/ICEICE.2011.5777806

[25] Siddiqi, M.A., Pak, W. and Siddiqi, M.A. (2022) A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, **12**, Article 6042. https://doi.org/10.3390/app12126042

[26] Sun, Y., Wang, B., Wang, C. and Wei, Y. (2021) On Man-in-the-Middle Attack Risks of the VPN Gate Relay System. *Security and Communication Networks*, **2021**, Article ID: 9091675. https://doi.org/10.1155/2021/9091675

[27] Radanliev, P., De Roure, D.C., Maple, C., Nurse, J.R., Nicolescu, R. and Ani, U. (2019) Cyber Risk in IoT Systems. https://doi.org/10.20944/preprints201903.0104.v1

[28] Zhang, Z., Zhang, Y.Q., Chu, X. and Li, B. (2004) An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN. *Photonic Network Communications*, **7**, 213-225. https://doi.org/10.1023/B:PNET.0000026887.35638.ce

[29] Miller, J.F. (2013) Supply Chain Attack Framework and Attack Patterns. The MITRE Corporation, MacLean VA. https://doi.org/10.21236/ADA610495

[30] Chen, W., He, Y., Tian, X. and He, W. (2021) Exploring Cybersecurity Education at the k-12 Level. In: Langran, E. and Rutledge, D., Eds., *Proceedings of SITE Interactive Conference*, Association for the Advancement of Computing in Education, Chesapeake, 108-114.