National College of Ireland

Remote working and Cyber Security threats in Ireland. Challenges and Prospective Solutions

MSc Research Project/Internship
Msc in Cyber Security

Marcia Patricia Fritzen
Student ID: 19139446

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Marcia Patricia Fritzen
Student ID:	19139446
Programme:	Msc in Cyber Security
Year:	2021
Module:	MSc Research Project/Internship
Supervisor:	Mark Monaghan
Submission Due Date:	16/08/2021
Project Title:	Remote working and Cyber Security threats in Ireland. Challenges and Prospective Solutions
Word Count:	XXX
Page Count:	37

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Marcia Patricia Fritzen
Date:	20th September 2021

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Contents

Remote working and Cyber Security threats in Ireland. Challenges and Prospective Solutions

Marcia Patricia Fritzen
19139446

Abstract

Remote work has become a reality recently for many people due to the pandemic crises created by the COVID-19. As a result, cybersecurity and information security have shifted into one of the main concerns and priorities for business in Ireland and around the globe. Overall, the pandemic has brought great opportunities and more significant challenges for organizations.

Employees from the most diverse business fields have worked from multiple locations out of the main offices. Since working from home, remote workers are more vulnerable to cyber-attacks. Hence, it is necessary to create new ways to protect the business assets, ensuring business continuity, and implement security measures online. In addition, businesses need to know how to manage risks and scale the challenges that may lie ahead.

The constant search for innovation is a great reality, but it needs extra attention, as this opportunity creates cyber risks, new and unforeseen. This paper aims to discuss remote working concepts, pros and cons, information security and cybersecurity, impact on cybersecurity caused by remote working, Internet of Things devices concepts, and security, the importance of training remote workers on how to react in adverse situations.

Through a survey instrument developed and distributed to remote workers in Ireland, it was possible to learn about the participant's thoughts about working from home, cybersecurity, information technology devices, information, IT infrastructure, and cybersecurity training.

This dissertation fills the gap by offering a novel cybersecurity training and awareness application for remote workers with comprehensive information about the security of the Internet of Things (IoT) devices.

1 Introduction

The coronavirus pandemic, also known as COVID-19, caused by a severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), has posed numerous challenges to businesses worldwide.

Suddenly, many companies had to implement the remote work regime, also known as a work from home (WFH), to adhere to the social isolation measures imposed by governments to mitigate the effects of contamination and prevent the health system's collapse.

Many companies had to implement remote working programs on a broad scale for all employees for the first time. This change resulted in a considerable technical challenge

since remote work on a large scale can increase companies' exposure to risks of privacy, data protection, and cyber attacks.

Working from home is a contentious topic. Some say it is the most effective and efficient way to increase employee and collaborator productivity, allowing remote workers to achieve a better work-life balance and spend less time traveling. Others, on the other hand, believe it will reduce productivity and lead to more distractions. However, due to technology improvements, it is now possible to work from anywhere in the world and complete the same tasks as if they were in an office, as long as they have access to the internet.

The pandemic has brought excellent opportunities and challenges for organizations. There has been a potential growth of the digital transformation process, with remote work being enormously enhanced and widespread, triggering a wide range of cyber threats.

As COVID-10 reaches across many countries, causing disruption to many sectors, it also pointed to a secondary threat, the threats to a technology-driven society.

Recently, on 14th May 2021, the Health Service Executive (HSE) experienced a cyber attack-ransomware intended to disrupt health care and computer systems, appropriate data, and require a ransom in exchange. This HSE attack made all of the HSE IT systems in Ireland to be shut down and may be impacted for six months.[1]

Another potential threat is the internet of things devices attacks. IoT devices continue to grow at an alarming rate. As a consequence of inadequate security protections, cybercriminals are using automated tools to exploit vulnerabilities.

A recent study from Zscalter examined over 575 million device events and 300,000 IoT-specific malware attacks in a period of only two weeks in December 2020. A 700 percent increase if confronted with analysis to pre-pandemic findings. Moreover, these attacks targeted 553 diverse device types, including printers, digital signage, and smart TVs, all connected to and communicating with corporate IT networks. At the same time, many employees worked remotely during the COVID-19 pandemic[2].

This paper will create a strategy to mitigate cyber threats and attacks through education, a specific training platform to help remote workers with all the information they need to work safely from home without risks of exposing themselves or their company's data.

The structure of this report will follow:

Section 1. Introduction the mindset behind the digital transformation growth, remote working, and Cyber Security threats caused by the COVID-19.

Section 2.A detailed review of previously published academic journals, papers, and articles on remote working and cybersecurity was conducted.

Section 3. Our research strategy is shaped by research methodology, which includes the subject area, data sources, and analysis.

Section 4. Our proposed idea, Design Specification, includes reasons based on the knowledge gained from the Literature Review and Research Methodology.

Section 5. Implementation, which includes a technical implementation of the proposed solution, is a justification of how and why choices were chosen.

Section 6. Evaluation, the effectiveness of our proposed/developed ICT solution in supporting the new workplace's home-based environment.

Section 7. Conclusion and Further Work, discussion on the topics and findings, with the opportunities for further works linked to this research context.

[1]https://www.gov.ie/en/news/ebbb8-cyber-attack-on-hse-systems/

[2]https://www.helpnetsecurity.com/2021/07/20/iot-malware-attacks-rose/

2 Reserch Question

The primary goal of this research work is to define how remote working has affected workers in Ireland since the start of the pandemic. In addition, the research explores the risks of internet of things devices in the work environment. Another goal is to identify if companies in Ireland provide enough support and appropriate cybersecurity training to remote workers in Ireland.

3 Related Work

Due to the COVID-19 crisis, several countries throughout the world are facing significant challenges. COVID-19 is an illness caused by the SARS-CoV-2 coronavirus, which is a novel coronavirus. Following a clustering report of 'viral pneumonia' cases affecting people in Wuhan, Republic of China. The World Health Organization first learned of this new virus on December 31, 2019.[3]

We now live and work differently as a result of the pandemic. New measures, such as wearing a mask and social distance regulations, were enacted for most organizations, universities, government institutions, and enterprises. With the objective to reduce the spread of the virus, working from home became ideal and the safest decision. In addition, business and schools have become more reliant on digital technologies and the internet. As a result, the risk of being exploited by hackers or cyber criminals has grown exponentially[1].

In this following paragraphs, it will be discussed some researches that have contributed to this paper and have the same purposes of improving Security and implementing a better structure for Cyber Security for remote workers and served as a foundation to this work.

Steven Funnel discusses home working and cybersecurity. In his study, the author looks at how thriving firms and their employees were likely prepared for the unexpected rise in home working, as well as the heightened cyber threats that came. As a result, the discussion around his studies was the UK-focused perspective. The author analyses the National Cyber Security established in 2012, providing ten recommendations that cover the key areas to protect organizations from attacks and breaches. Only 12 percent of the business have taken actions against all the steps.[2]

Figure 1:10 Steps to Security, National Cyber Security Centre's [4]

[3]https://www.who.int/news-room/q-a-detail/coronavirus-disease-covid-19
[4]https://www.ncsc.gov.uk/collection/10-steps

Steven compares the size of organizations to understand the response to comply with those steps. In his findings, Steve points out that there are no cyber security-framed rules where staff can follow when working from home. Additionally, the author reviews user education and awareness, saying that a significant amount of business does not have a formal policy that explicitly covers what remote workers can do on the organization's device.[2] He also covers the lack of remote workers' training. Only one in nine businesses, 11 percent in UK business, has provided cyber security training to non-cyber employees in the past year.[3] The weakness noticed in his paper was the lack of future work ideas to help with the continuity of other researches in this area.

Steven's article helped to view the importance of cybersecurity training for remote workers. For example, during the COVID-19 transition from working in the office to work from home at the start of the pandemic crisis here in Ireland, many employees had to start working from home and doing their home office set up only with their own IT skills to guide them. In addition, most workers received the tools, laptops, and other devices to work from home. Still, the companies lacked guidance and preparation to secure and train employees and ensure the secure configuration of their devices and network security. That motivated this research to implement a novel cybersecurity training and awareness application specific to the remote workforce. The cybersecurity training and awareness need to include all employees from all departments of an organization and not only limited to cybersecurity professionals.

According to John Grimm, organizations should also adopt strict guidelines and training programs for staff to highlight the problem of connected device security and disseminate best practices to mitigate human error in network integrity. These activities are necessary for organizations to safeguard a growing digital workforce and protect both the organization and the employees as remote working becomes more common, even post-pandemic[4].

The study Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic was another source of inspiration for this research. The study examines the COVID-19 pandemic from a cyber-crime standpoint, highlighting the wide spectrum of cyber-attacks that occurred around the world during the epidemic. The investigation then moves on to using the United Kingdom as a case study. In this publication, the author proposes a new timeline of assaults associated to the COVID-19 pandemic to aid ongoing research. This chronology and the analysis can help us to better understand those attacks and how they're put together, so we can better plan to counter them.[5]

After reviewing the research results, Cyber Security in the age of COVID-19 was possible to learn about the most common and uncovered a similar tactic used by many cyber-attacks during this period. Most cyber-attacks start with a phishing effort that directs victims to download a file or visit a URL. The file or URL acts as a delivery vehicle for malware, which, once installed, becomes a channel for financial theft. The investigation also showed that the phishing campaign uses media and government announcements to boost its chances of success. The limitations of the paper were around declaring the analysis is not necessarily novel, but the authors stated this is the first time that this has been covered with a context of actual live events

The Security vs. Flexibility: Striking a Balance in the Pandemic Era article examines the cybersecurity threats which have arisen during the pandemic. In addition, the work shows the difficulties faced by the employees and their employers in these challenging times. Furthermore, the authors present some challenges faced by employees working

remotely, such as the lack of technical background, lack of preparedness, limitation to use Virtual Private Network, using a personal application on their devices, lack of awareness, security policies, lack of employee's training, etc. Finally, in section four of the paper, the authors present excellent points to help the companies securely transition towards creating a secure flexible workplace[6].

This report served as a starting point for focusing this research on providing remote workers with more excellent information on securing their Internet of Things devices and educating them on the risks these devices can pose to a company. This article was essential to learn about the strategies that can assist firms in managing security and flexibility by reading the future work. The authors propose a model that considers both Internet Service Providers' various networking devices and employees' devices. It must safeguard the devices from the most common cyber-attacks and known risks. To provide new security protocols and standards, new security protocols and standards must be developed.

Ashwin Karale, addresses the challenges of IoT addressing security, ethics, privacy, and laws. Ashwin article's helped provide a comprehensive overview for this work about IoT security. As IoT applications continue to grow, this paper provides an excellent insight into how the threats and vulnerabilities of IoT influence our lives. Most of the research focused on highlighting IoT's challenges concentrates only on one or two significant challenges like security and privacy. Thus, the limitations of the study are more focused on challenges than solutions. This study demonstrates the threats and vulnerabilities of IoT, but it also raises the question of the current and possible answers to overcome these challenges[7].

This report spurred further investigation into remote employees' perspectives on how IoT devices have influenced workers in their work environments, as well as the threats these devices provide to businesses and remote workers.

Cybercriminals are taking advantage of the generalized chaos caused by COVID-19. As a result, cybercrimes are increasing day by day, and Cyber Security threats are growing and becoming a significant concern to the entire world.

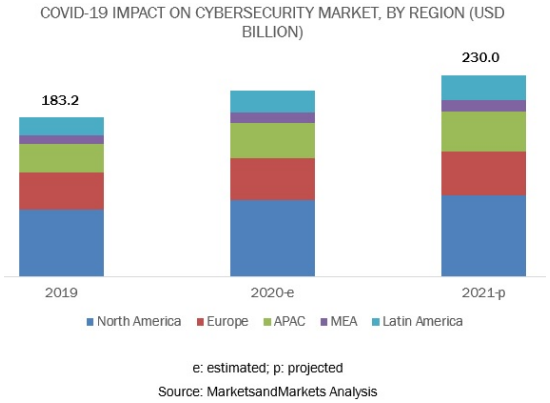

Figure 2: Picture extracted from article from Covid-19 Impact On Cybersecurity Market by Technology (Network Security, Application Security, Endpoint Security, Cloud Security, Database Security, Web Security, ICS Security), Vertical, Region - Global Forecast to 2021[5].

[5]https://www.marketsandmarkets.com/Market-Reports/covid-19-impact-on-cybersecurity-market-128702677.html

Social engineering is the ultimate con, a set of techniques fraudsters use to get past an organization's security systems by lying, cheating, and stealing. Their objectives are as follows: Theft, deception, or espionage[8].

All technology, including firewalls is vulnerable to social engineering. Moreover, it attracts hackers since people's lack of awareness frequently facilitates their work[8].

In addition, meeting apps become a target for hackers. For example, zoom is one of the most well-known tools for attending online conferences and lectures these days. As a result, cyber hackers have turned their attention to Zoom. They employed "Zoom bombing" to capture user data and may eavesdrop on ongoing Zoom meetings to listen in on any communication. According to one cybersecurity forum, around 50,000 Zoom accounts are for sale on the dark web. [9].

Similarly, other organizations such as Microsoft Teams, Google hangouts, Blue Jeans, Slack, and Skype face challenges during these critical times and become more vulnerable to cyber-attacks.

According to an INTERPOL study of COVID-19's influence on cybercrime, the target change from people and small enterprises to major organizations, governments, and critical infrastructure has occurred. Criminals use new security weaknesses to steal data, create money, and cause disruption as organizations and enterprises rapidly deploy remote systems and networks to enable workers to work from home. For example, one of INTERPOL's private sector partners detected 907,000 spam messages, 737 malware events, and 48,000 harmful URLs – all related to COVID-19 – over four months (January to April)[6].

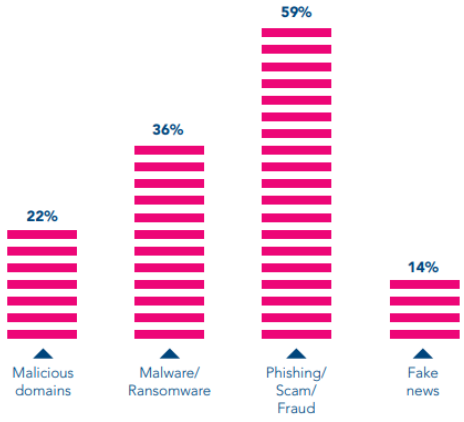

Figure 3: Distribution of the key COVID-19 inflicted cyberthreats based on member countries' feedback.[7]

According to Microsoft, 44% of employees in Ireland's businesses had battled hacking, phishing, or cyber fraud in 2019. In a recent PWC report, almost 80% of Irish companies struggle to keep up with the complexity of evolving cyber threats. At the same time, as healthcare professionals and industry are working to protect us and develop a vaccine to eradicate the COVID19 virus, cyber attackers are working around the clock to exploit businesses and governments worldwide.[8]

[6]https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[7]https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

[8]https://www.sogeti.ie/explore/sogeti-ireland-blog/coronavirus-covid-19-increased-risk-of-cyber-attack/

Malware has encrypted the data of Irish corporations and private individuals, mainly through targeted malicious emails or unsecured websites. The impact of ransomware attacks on businesses of all sizes may be devastating. It stops the victim from accessing vital information such as client information or performing even the most basic operations, such as sending an email. The cyber crooks would then communicate with the victims and require payments ranging from hundreds of euros to millions of euros, which they will generally decode in bitcoin.[9]

According to Infosec professionals, supply chain attacks, cyber warfare, and IoT as an attack vector were up by 38%. Additionally, ransomware was believed to be up by 31%, and DDoS attacks by 36%.[10]

The present research starts with an understanding of the Remote working background, types of remote working, and defining the remote working pros and cons before jumping into the cybersecurity impact, threats, and vulnerabilities posed by remote working.

3.1 Remote working

Teleworking, telecommuting, flexible workspace, home-office, working from home (WFH), and virtual working are all terms used to describe remote working. Remote working is possible because advancements in information and communication technology make electronic data transfer more accessible and allow workers to communicate and coordinate tasks from different locations and times. This working model denotes a method of conducting specialized labor in which employees are not required to commute or travel to a specific place to do their job.

Although the concept of remote working is not new, it has gained popularity due to the digital transformation.

During the early 1970s oil crisis, American Jack Nilles and colleagues produced projections on how much money the national economy would save if people commuted less; this was the birth of the concept of remote working.[11].

Currently, remote working has been considered a temporary agreement between employees and employers in Ireland that allows employees to work from a non-office location to minimize the spread of Covid-19. [10].

Precise data on the current prevalence of remote work in Ireland is currently unavailable. However, in 2018, the Central Statistics Office undertook a pilot survey to inform the 2021 Census. This pilot found that 18% of respondents worked from home, mostly one or two days per week. There have also been meaningful increases in job portal searches for remote work-related terms in recent years.[11]

3.1.1 Remote working Pros and Cons

Pros:

- Reduced commuting costs, new wardrobe purchases, gasoline use, and workspace savings, as well as pollution reduction[12].

[9]https://www.garda.ie/en/crime/cyber-crime/increase-in-the-number-of-ransomware-attacks-in-2021.html

[10]https://www.cipd.ie/news-resources/practical-guidance/guides/employee-remote-working#gref

[11]https://enterprise.gov.ie/en/Publications/Publication-files/Remote-Work-in-Ireland.pdf

- Remote work will increase productivity and morale. It can even lead to job opportunities outside the country or abroad for talent and workforce to carry out activities[13].

- Teleworking Proponents believe that teleworking causes a win-win situation. In other words, working from home has advantages for both employers and employees. Some have pointed out that working remotely is beneficial to society. Thus, it will be a win-win plan.[14].

- Some of these benefits include a wide range of employment opportunities, improved balance between life and work, flexible working hours, increasing employee productivity, and creating more jobs for disabled people.

- Increased job opportunities that in turn reduce stress behaviors caused by social interactions and risk of injury or disease[15].

- A reduction in the organization's overhead/facility expenditures is another significant benefit of telecommuting. For example, organizations can cut their investments and expenses on office buildings, parking lots, and additional physical capital as more people work from home or other remote locations.citep16.

Cons:

- There are some advantages of remote working. However, people also experience difficulties during this macro crisis. Everyone has different roles. Remote working brings together all roles for a person at the same time.[16].

- Even if it seems attractive at first look, the new format of working style has generated lots of difficulties, especially on employees' mental health. The workers' social life, private comfort zone, and working environment have mixed, and the balance between certainty and predictability is broken now. In addition, work-related issues cause occupational stress. [17].

- Remote Working presents issues that will have a direct impact on organizational work, as well as management ideas that will no longer be viable. Employee performance monitoring and measuring, for example, will be very poor and irrelevant in this new environment, according to normal employees.[18].

- A remote workforce comes with some risks concerning information technology and infrastructure, employees relying on their home networks uniquely and sometimes use their own devices to perform tasks.

- According to the Velocity Smart Technology Market Research Report 2021, 70% of remote workers said they had encountered IT problems during the pandemic, and 54% had to wait up to three hours to resolve the issue.[12]

- HP Inc. released its HP Wolf Security Blurred Lines & Blindspots Report, an extensive research assessing organizational cyber risk involving remote working. The report reveals that changing work habits and behaviors produce new vulnerabilities for companies, individuals, and their data. According to the results, 70% of office

[12]https://www.velocity-smart.com/en-gb/velocity-smart-technology-market-research-report-2021

workers examined consent to use their work devices for personal tasks, while 69% are using personal laptops or printers for work activities. Nearly one-third (30%) of remote workers surveyed have let someone else use their work device.[13]

- Information security experts have also categorized distinct hazards associated with working from home. For example, two-fifths of respondents believe that employees accessing untrusted networks pose a risk to their firm, and 38% believe that another individual gaining access to an employee company device is an absolute risk. But the dangers don't stop there. A little more than a third (37%) states that utilizing personal messaging platforms for professional and personal reasons is risky and that inadvertent company information disclosure is also a concern[10].

- Internet of things (IoT) devices lack of security.

3.2 Information Security and Cyber Security

Cybersecurity is a set of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, activities, training, best practices, assurance, and technology that can be used to protect an organization's and users' assets in the cyber environment. Organizations and users own connected computing equipment, staff, infrastructure, applications, services, telecommunications systems, and the entirety of information transferred and/or stored in the cyber environment.Cybersecurity aims to secure the attainment and maintenance of the organization's and users' security attributes in the cyber realm against relevant security dangers. The next generation[19]

The international standard defines information security as the preservation of information's confidentiality, integrity, and availability. Information communication can take numerous forms depending on the situation. For example, it can be printed or written on paper, kept electronically, sent via post or electronic means, viewed on film, spoken about, and so forth.[20]

Information security refers to the safeguarding of data and its vital components, such as the systems and hardware that use, store, and transfer it.[21]

3.3 Impact on Cyber Security, increased threat and vulnerabilities posed by remote working

In February 2019, Microsoft Ireland observed at how poor employee security habits within the large public and private organizations across Ireland threatened data loss and cyber breaches. It was found that 44% of employees have encountered problems with hacking, phishing, and cyber fraud. This was a compound of poor security practices amongst employees and a lack of consistent security training. Nevertheless, the issues highlighted are not only the single responsibility of the employee. As cyber threat risks grow and grow more sophisticated, a more comprehensive view of the security landscape in Irish organizations is demanded[22].

Cybersecurity is a problem of resilience. No system can be entirely secure at all times, but the experts must think of ways it recovers in case of an attack. Organizations must formulate appropriate teams to deal with unfavorable conditions. The concept

[13]https://www.securitymagazine.com/articles/95177-study-reveals-growing-cybersecurity-risks-driven-by-remote-work

of "flexibility" is fascinating and helpful, but employees need to ensure that this does not "compromise" the organization's security. With proper strategic planning, secure pervasive technology infrastructure can be built to strike an efficient balance between flexibility and safety. Success in cybersecurity is not eradicating cyber threats or the coronavirus. Still, it is about making sure that life can go on despite the challenges posed by cyber threats or the virus. Thus, employees and employers must cooperate to safeguard flexible work arrangements. In the future, a ubiquitous secure technological system model needs to be developed that protects the company's network infrastructure and access to confidential data. The model must consider complex networking devices used by Internet Service Providers and those personal devices used by employees. It must protect the devices from the predominant cybersecurity attacks and the known threats. Also, new security-related protocols and standards must be developed to provide end-to-end security from the user's device to the company's network. This will help organizations to provide secure flexible work arrangements in the true sense[6].

The acceleration of digital transformation has strengthened the importance of cybersecurity and brought the need to control and secure against remote devices and threats. Businesses need to ensure they have total control and clarity of all company data while supporting employee productivity. Contrarily, we start to see innovation come at the expense of data protection[23].

According to a poll done by Netwrix Research Lab and published in Cyber Threats Report 2020, the remote work culture has resulted in new trends in the threat landscape, requiring enterprises to rethink their priorities to adjust to the new work-from-anywhere model. Unfortunately, the adjectives "difficult" and "frantic" don't come close to explaining the rapid transition to remote work[24].

3.4 IT infrastructure and Secure applications for remote working

Working from home is now a measure that has the potential to save lives. However, it's important to know what kind of software and hardware are being used to do the task. Simple checks and program installations can make an employee's performance at home almost as safe as it is at work, where a digital security department exists. If necessary precautions are not followed, the choice to relocate the employee to work from home can be harmful. Since working from home employee is transporting sensitive company information outside of a secure setting, it is critical to have a robust infrastructure in place.

A few recommended measures:

- Connectivity: Network capacity is essential for remote workers. Many companies have discovered what network and security specialists have known for a long time. Once an endpoint leaves the company perimeter, security suffers. According to Matias Katz's secure connectivity for remote workforce post, the average home wifi network has ten or more unmanaged devices connected to it, including personal laptops, cellphones, gaming consoles, and home IoT devices. The vulnerability in today's cybersecurity posture is a layer of separation from remote work and home network attacks. In his, work Katz suggests a new way by separating wireless networks for personal and untrusted devices and trusted devices through network segmentation[25].

Endpoint micro-segmentation is the suggested design for remote workers. Each endpoint is unique and manages its own dedicated and managed network security stack, isolating the entry from other devices on the same network. This architecture provides a high level of connection, manageability, and governance that can be proven. Additionally, the remote worker device is physically isolated from their home network. To meet the emerging needs regarding remote working, strict data and network security are essential.

- Availability: Remote workers must have adequate equipment and accessories, which the company must provide, such as a monitor, keyboard, and mouse etc. reduces their need to use unknown-source external equipment.

- Flexibility: Access to the necessary tools and extension limited to what is relevant to the business.

- Integrity: Data from the virtual space should not be replicated to the physical desktop.

- Reliability: To ensure that remote working solutions deliver a basic level of reliability, they must be validated against a set of functional requirements through service testing.

- Assistance: Remote workers require immediate assistance, as well as clear information about who/when/where to contact in the event of an incident.

- VPN: In terms of technology, VPN (Virtual Private Network) solutions, for instance, store encrypted access to an organization's server, allowing users to locate files and systems kept there. The technology builds a secure tunnel between the user's home and the company's administration criteria for data transmission and application access. The employee receives an IP address from the internal network and can then start using the allowed resources.

- VPNaaS: VPN as a service (VPNaaS) offers are already available on the market and are a great alternative for companies that do not have remote work infrastructure. In this model, access to data and systems is made via a portal with SSL security protocol and double-check, without the need to install an agent on each user's machine.

- MFA (multi-factor authentication): MFA, or multi-factor authentication, is an expansion of two-factor authentication. As the name implies, multi-factor authentication is an authentication method that uses two or more authentication elements. It is now broadly accepted as the de facto standard for any system requiring high security[26].

- Access controls:As an example, the role-based access control (RBAC) can be used to configure baseline and default access for the remote worker on internal and web applications with Cloud Access Controller (CAC). It is possible to know what activities they can perform, such as which buttons they can click, which text they can read, which form they can fill out, and so on. For today's companies, the zero-trust concept is the only approach to provide total data protection and to know who has access to data, when data has been accessed, and from which end-point.

> Insider risks are difficult to spot. We must ask who we commit our data to for enterprises to regain control of data fully. Only digital solutions built by companies fully aware of the need to protect their data can successfully standardize remote working.

As a result, remote workers should be encouraged to take the required precautions, such as utilizing only business email on the device they use for work, not clicking on suspicious links or emails from unfamiliar sources, not sharing passwords, and accurately using company resources. In the event of an incident, the industry's ability to respond quickly to threats is critical. A quick response and recovery function are critical for decreasing the risks of a prospective cybersecurity event, as well as the loss and reputation of the firm.

3.5 Internet of Things (IoT)

The internet of things (IoT) is recognized as the infrastructure of the information society. All these "things" connect to the Internet via Wi-Fi and then "talk" to each other. It is the current world network of home appliances, vehicles, and other physical devices. All these devices are interconnected across the grid provided. They are embedded with the required software, actuators, sensors, and network connectivity. Each of these devices are identified over the network and exchange data. IoT is exceptional automation and analytic system which uses networking, sensing, big data, and artificial intelligence technology to deliver complete systems for a product or service. These systems allow more comprehensive transparency, control, and performance when applied to any industry or method. IoT systems have applicability across industries through their unique flexibility and capability to fit in any environment. They improve data collection, automation, operations, and much more through smart devices and robust enabling technology[27].

The Internet of things is a world where physical objects are integrated into the information network and where the physical objects can become effective participants in the business process.[28].

The Internet of Things (IoT) is a fast evolving model in which a wide range of things are instrumented in such a way that they may be questioned and controlled through the Internet, either directly by users or through programs that encapsulate their behavior and intentions. [29, 30].

The Internet of Things will transform individuals and organizations' interactions with the physical world and among themselves. Interactions with home devices, autos, customer things, industrial plants, and weaponry, for example, will be drastically transformed. In addition, many services, including health, education, and resource management, will be delivered in unique, better-organized, and customer-specific ways. [31].

The rise of Internet-connected appliances, which are part of a growing breed of Internet-of-Things (IoT) gadgets, is making the home more "smart." Consumers can now monitor and regulate their home environment from afar. Lighting systems, for example, may be controlled remotely, smoke alarms can alert us if a fire is suspected, we can monitor our children from afar, and our health/fitness data can be sent directly from the home to the cloud for analysis. Personal or family safety, property protection, lighting/energy control, and pet monitoring are among the top incentives for using such devices, according to surveys in the United States, with 51% of those polled preferring to pay a premium for them.[32].

3.5.1 Cyber Security x IoT Security

IoT security is not traditional cybersecurity but a blending of cybersecurity with other engineering disciplines. It addresses much more than data, servers, network infrastructure, and information security. Instead, it involves the direct or distributed monitoring, control, and administration of the state of physical systems connected over the internet. Cybersecurity often does not discuss the physical and security aspects of the hardware device or the physical world interactions.[33]

3.5.2 IOT devices security and the impact on remote working

Working from home is already a reality in many companies. However, with the Coronavirus (COVID-19) pandemic, the security of devices used remotely has become an issue in many organizations. The main concern is that the employee usually works in a network that their company does not control.

That's why companies need to set up processes to allow staff to connect to the company's network securely remotely. The security of IoT devices must be a priority for companies, and it must be planned from the beginning of the projects.

IoT devices are present in our homes and offices and to improve security a proactive approach needs to be followed to secure and control the organization's assets.

It is not just the absolute number of people now expecting remote authentication and digital capabilities that pressure IT infrastructure. There are significant security challenges that face people working from home. Unsecured Internet connections, personal devices entering business systems, and the presence of intelligent home appliances put new stresses on business cybersecurity. In addition, Internet of Things (IoT) devices are volatile in the frontline of cybersecurity, with recurring stories about coffee makers being used as network points of entry and speaker systems used to record conversations.[4].

A majority of the IT security professionals express their concern, ranking the altering of a device's function as the most critical threat to IoT security, closely followed by the unauthorized control of devices. The evident security concerns are intensified by the surge in ownership of smart appliances and connected devices, with almost 25% of UK homes owning at least one IoT-enabled device and projected ownership rising to nearly 50% by 2025[4].

IoT solutions manage and have access to a unique set of sensitive data that, if exposed, might jeopardize users' privacy. At any tier of the IoT system, privacy issues can arise. In some cases, infected devices may use backdoors or malicious kernel code to send sensitive data to unauthorized third parties.[34].

3.5.3 IoT Attack Surface

These factors expose businesses to a more attractive attack surface than ever before. And with enterprise data transmitted at an ever-greater rate, existing systems are, in some cases, unable to guarantee adequate security. This could lead to data being stolen and sold on the dark web that, according to IBM, costs a business on average over $3.8m. In addition, a breach of any size can also lead to the disclosure of intellectual property and damage to public trust with a permanent impact on business reputation. [35]

Well-placed security controls are vital to reducing either the likelihood or severity of an attack's exploitation of a vulnerability.[36] The following diagram shows the ecosystem of attacks, vulnerabilities, and controls:

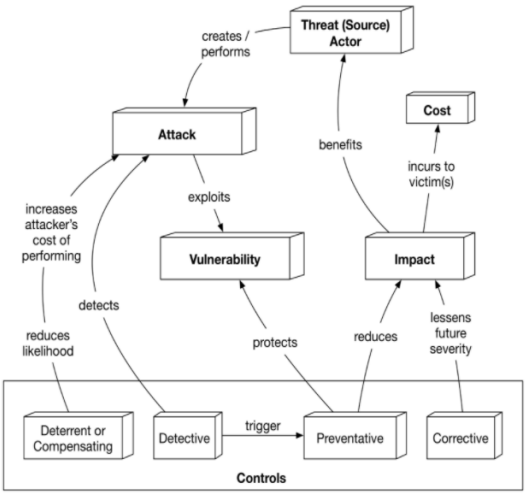

Figure 4: IoT Attack Surface

3.6 Cyber Security Training and Awareness Program specific for the remote work environment

Although a variety of cybersecurity and awareness courses or games have been developed to ensure cyberspace safety, most of these applications have not been adapted to the remote work environment. According to Angela Sasse there are three-step framework capable for changing people's behavior[37].

- Awareness: captivating the attention and interest of the user
- Education: thorough awareness of the user base's expertise level
- Training: by supplying the necessary skill set.

Security awareness campaigns aim to pique people's interest in security and draw their attention to it. Awareness and education lay the framework, but for changing people's behavior needs training and new mental models or internal representations of how something works in the real world.

3.7 Security Assessment in the "Home-office"

Relevant factors are taken into account and followed when assessing the security of a home office: The authentication solution evaluation in relation to the enterprise network (SSO, MFA, etc.). Secure access to the company network via VPN as an example and any cloud-based resources. Firewall rules verification in order to secure the company's network against intruders. Revision of the procedure for delivering client systems (staging, provisioning, etc.) Security-relevant configurations and hardening measures on remote worker systems are examined (e.g. hard disk encryption and rights management) An investigation of user management techniques (patch management, protection against malware, etc.) Employees' security awareness when dealing with sensitive data in private and/or public places (privacy filter, screen lock, etc.)

4 Methodology

This part will go over all of the research's characteristics, environment, data, and components. The topic of methodology will be separated into two parts. The first is concerned with the survey, while the second is concerned with the Cyber-Security Training and Awareness Application.

4.1 Study Area

Following an examination of the scientific research papers in the literature review section, it was determined that none of the studies could provide a quick solution for protecting remote workers from easily accessible IoT devices that pose as a threat to business assets.

4.2 Data Sources

A questionnaire in Survey format was used to create the qualitative dataset. It was emailed to participants in Google document format, and it was also shared on Facebook and LinkedIn to get a sense of what remote employees thought about the topic.

The goal was to reach 100 people in Ireland, and we only got 59 or 59 percent of the way there. The information was gathered from remote workers in Ireland between April and July 2021. We designed the survey questions to provide a better understanding of how remote working is changing the cybersecurity landscape in Ireland.

Only remote employees in Ireland were considered for this survey. Therefore there was no need to analyze geographic inequalities or inequities. The results of this poll and the literature research will combine to help us conceptualize with the goal of developing a cybersecurity training and awareness app.

Validity and Reliability: Google Survey. Target population: Dublin Area. Data collection Method: Quantitative.

4.3 Survey Development

The survey questions were divided into three sections: remote working, cyber security, and IoT devices.

1. Before COVID-19 did you ever work remotely?
2. On a scale of 1 - 5 with 1 being the least positive and 5 being the most positive, how much of an impact has remote working had for you?
3. On a scale of 1 -5 with 1 being the least positive and 5 being the most positive, how much of an impact has working remotely had for you in terms of productivity?
4. Would you consider working from home permanently or on a blended approach?
5. Have you seen more phishing emails, spam emails and fraudulent emails lately?
6. Are you concerned about cyber and data security while working from home?
7. Did you participate in a cyber security training and awareness program specific for remote working environment?

8. On a scale of 1 -5 with 1 being the least positive and 5 being the most positive, how would you rate your company and IT department's response in relation to the technology infrastructure and security measures?

9. Do you own any smart devices in your home / home office? i.e: Alexa, Amazon Echo Family, Google Nest, smart plugs, security cameras, smart locks, smart heating and cooling, Nest thermostat, smart lighting, smart kitchen appliances, robot vacuums cleaners and mops, smart health and fitness devices or any other IoT (internet of things) devices? If yes, please specify what device.

10. Has smart devices easily accessed from your home office?

11. For your personal use, do you own one or more of the following devices or any other?

12. Did your employer provided the equipment for working from home or you are using your own equipment?

13. Has your employer conducted a security assessment in your work environment?

14. On a scale of 1 -5 with 1 being the least positive and 5 being the most positive, do you consider smart devices can help reduce distractions whilst making a positive impact on your work environment at home?

15. Do you use a VPN?

16. When security updates become available, do you often update your laptop and IoT devices?

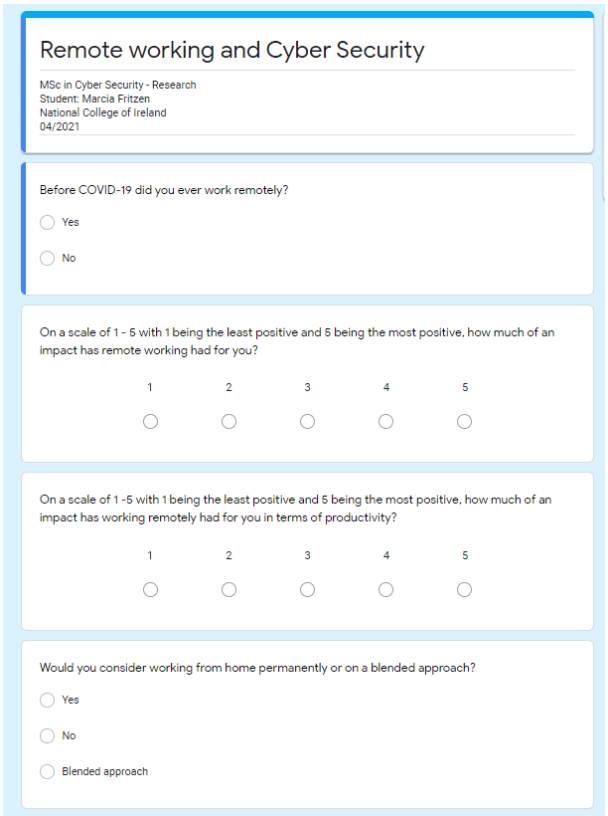

Table 5: Remote working questions

4.4 Research Analysis

After collecting the survey responses through Google forms, the file was downloaded from Google Forms platform and converted into a .csv file to analyse it in R.

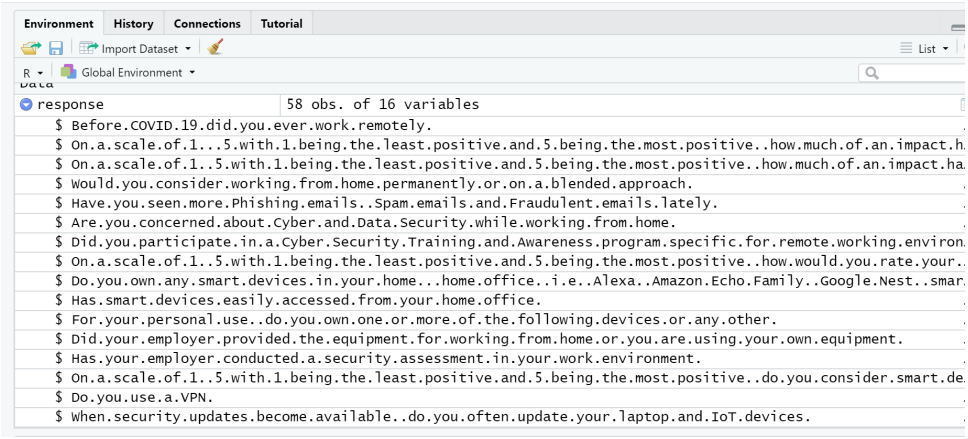

Table 6: Data analysis overview

The frequency of values of a variable bucketed into ranges is represented by the histogram.

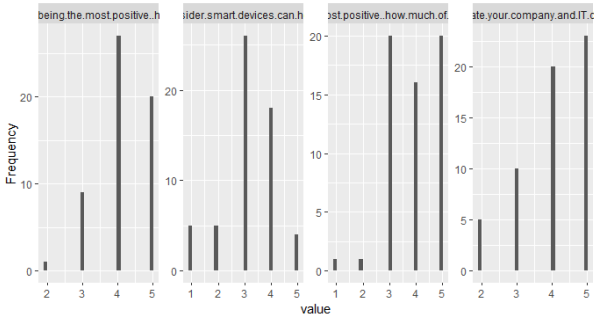

Table 7: plot_histogram(response[,-1])

Plot density function that created the density curve in the R window.

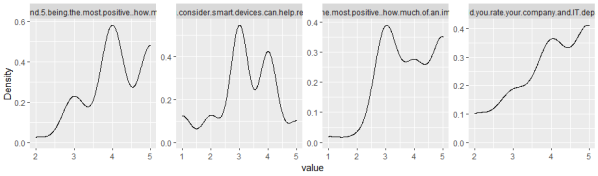

Table 8: plot_density(response[, -1])

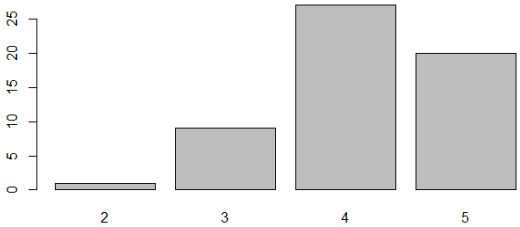

Table 9: Before COVID 19 did you ever work remotely?

The second part of the research is to develop a cyber security training and awareness application specific for remote workers.

4.5 Cyber Security Training and Awareness Application for remote workers with IoT devices Security.

The second part of the research is developing a cybersecurity training application, including IoT devices security training, proposed to solve the gap in this area. The application aims to help Remote Workers create something meaningful to learn how to protect themselves and their organization from cyber attacks.

- To assist remote workers in learning and practicing cyber security through online videos on a variety of topics.
- All users should be able to access a secure application;
- To create a reliable and secure online application that protects against unauthorized access and other dangers.
- Store all the information shared in a secure manner in an encrypted database.

4.5.1 Software Development Methodology

The methodology used for the proposed application is the Waterfall Model. It is clear to understand, and all the specifications were detailed before the project started. This model is properly defined and documented, which helped to organize and visualize the information for this research. Even though the Agile Model was also considered during the decision on what methodology to use, it did not succeed due to the lack of documentation.

4.5.2 Agile Model

Agile is a philosophy that uses organizational rules based on people, collaboration, and shared values. Agile provides a framework to adapt to the changing needs of the customer and surfacing risks beforehand in the project lifecycle and consequently improving the chances of a project's success[38].

4.5.3 Waterfall Model.

The Waterfall software development methodology is a logical and sequential one. Basicaly, each stage of the life cycle has to be completed in its entirety before moving on to the next stage. Some benefits of this model cover the following: The model is manageable and simple to understand. Stakeholders will know what to foresee in terms of timeline, functionality, and cost. Due to the artifacts required to be produced out of each phase, different sorts of documentation about the system will be available. The documentation is helpful for those who will be maintaining the software in the future. It can also facilitate bringing new employees on board and lessen the impact of any employee turnover.[39].

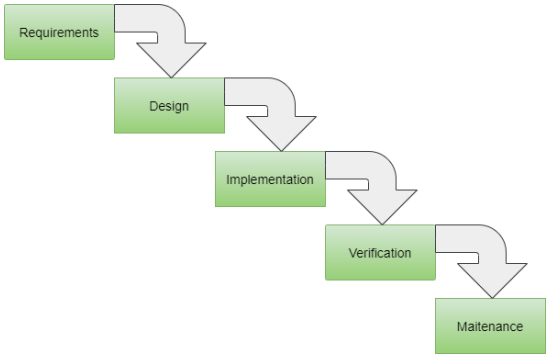

Figure 9: Waterfall Model

Requirements -All of the limitations and constraints to effectively complete the application were outlined in the first portion of the project. During this step, the programming language and all of the technology involved were determined. Design - A comprehensive list of hardware and software requirements, as well as programming languages, networks, user interfaces, and system architecture. To help conceptualize the project, an ER diagram was required. All of the risks that could compromise the result analyzed, as well as the logical design. A three-tier architecture was used, with PHP for the backend and HTML, JavaScript, and CSS for the web browser and front end client. Implementation - In this part the source code was written. Verification - The code was test to ensure it was working as expected. Maintenance - This stage will occur after the deployment. The intention is to deploy the application on Heroku.

5 Design Specification

This section discusses the techniques, architecture, frameworks that underlie the implementation and the associated requirements are identified and presented here.

5.1 Survey

The survey was designed, and the link to access the online survey was shared with Remote workers located in Ireland. The survey submission was open between April and July 2021. The online poll had sixteen questions related to remote working, cyber threats, cybersecurity, and home office structure.

The respondents were from Facebook, LinkedIn connections, and team members of the author of this research paper. Before sharing the survey online, it was informed that no personal data would be collected. Ethical consideration was taken across all areas of the present research.

The participants demonstrated a great interest in the topic, and they answered the questions rapidly. Most of the participants were from the Information Technology industry working remotely due to the COVID-19.

All the responses were downloaded from the Google form survey in a . .CSV format and analyzed in R studio.

5.2 R

R is a statistical computing and graphics language and environment. R is very extendable and provides a wide range of statistical (linear and nonlinear modeling, classical statistical

tests, time-series analysis, classification, and clustering) and graphical procedures. R is accessible in source code form as Free Software under the provisions of the Free Software Foundation's GNU General Public License.[14].

5.3 Algorithms

After the research analysis and discussions, the importance of developing a novel application where remote workers could access a cyber security training and awareness platform with video classes, movies, quizzes to educate efficiently. It was identified that there is a gap related to the Internet of Things devices security which poses a threat to organizations.

5.4 3-Tier Architecture

A 3-Tier architecture technique was employed to construct the cyber security training and awareness application.

The underlying structures of a software system, as well as the discipline of building such structures and systems, are referred to as software architecture. Each structure is made up of software elements, their relationships, and the qualities of both the elements and the relationships. It serves as a blueprint for the system and the ongoing project, detailing out the tasks that the design teams must complete[40].

Architecture decisions define the rules for how a system should be built. For example, in a tiered design, an architect can decide that only the business and services levels can access the database, preventing the presentation layer from making direct database calls. Thus, architecture decisions define the system's limits and direct development teams on what is and isn't permitted[41].

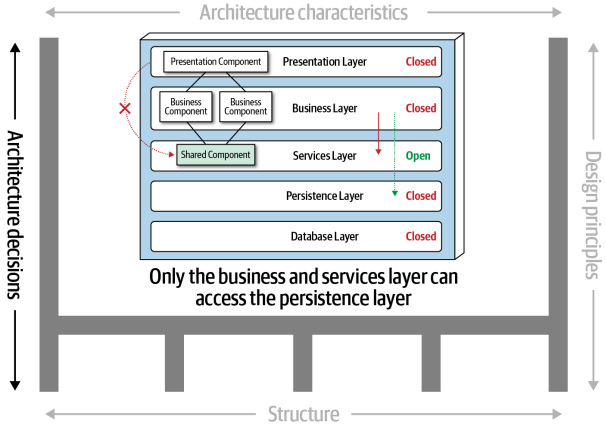

Figure 10: 3-Tier Architecture.

We provide a modular architecture for managing the Cyber Security Training and Awareness application in this study. The 3-tier approach architecture was chosen because it combines an effective combination of techniques with development flexibility.

A 3-tier architecture is a form of software architecture that consists of three logical computing "tiers" or "layers." They are a form of client-server system that is frequently utilized in applications. By modularizing the user interface, business logic, and data

[14]https://www.r-project.org/about.html

storage levels, 3-tier architectures offer numerous advantages for production and development settings. This allows development teams more freedom by allowing them to update a specific section of an application independently of the rest[15].

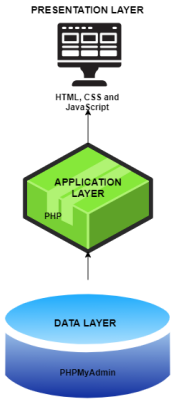

Figure 11: Project Architecture.

5.4.1 Presentation Tier

The user interface is contained in the presentation layer, which is the application's front end layer. HTML, CSS, JavaScript, React, and Ajax were the web technologies employed in the application.

HTML (HyperText Markup Language) is the most fundamental component of the Internet. It establishes the structure and meaning of web content. The term "hypertext" are reference to links that connect online pages inside a single website or between websites. HTML annotates text, graphics, and other content for display in a Web browser using "markup."[16]

CSS (Cascading Style Sheets) is an easy approach to customize a website's style and identity, fonts, colors, and spacing.

Every time a web page does more than just sit there and display static information for you to look at displaying timely content updates, interactive maps, animated 2D/3D graphics, scrolling video jukeboxes, and so on — JavaScript is a scripting or programming language that allows you to implement complex features on web pages. [17]

React.js is a famous and widely used JavaScript library for creating online application graphical interfaces. Jordan Walke, a Facebook developer, created it after being inspired by the XHP HTML component library for PHP. [18]

AJAX (Asynchronous JavaScript and XML) is an acronym for Asynchronous JavaScript and XML. AJAX is a new technique for using XML, HTML, CSS, and Java Script to create better, quicker, and more interactive web applications[19].

5.4.2 Application Tier

The application tier is in charge of the application's key capabilities and functional business logic. Because of its versatility and adaptability, PHP was chosen as the program-

[15]https://www.jinfonet.com/resources/bi-defined/3-tier-architecture-complete-overview/
[16]https://developer.mozilla.org/en-US/docs/Web/HTML
[17]https://developer.mozilla.org/en-US/docs/Learn/JavaScript/First_steps/Wha_is_JavaScript
[18]https://binarapps.com/what-is-react-js-used-for-whats-worth-knowing
[19]https://www.tutorialspoint.com/ajax/what_is_ajax.htm

ming language for the back end.

PHP is a programming language that can be used in two ways: PHP, or server-side scripting, was created to create dynamic online content, and it is still the greatest tool for the job. PHP is also used to create dynamic content using database connections, XML documents, images, and PDF files, among other things. The language is incredibly adaptable[42].

5.4.3 Data Tier

The database and data storage system, as well as the data access layer, are included in this tier. Because it is a free and simple to use software program, phpMyAdmin was picked.

phpMyAdmin is a free PHP-based software utility for administering MySQL databases over the Internet. phpMyAdmin can perform a wide range of MySQL and MariaDB tasks. The user interface can be used to manage frequently used activities (such as databases, tables, columns, relations, indexes, users, and permissions), although we can still run any SQL expression directly.[20].

5.4.4 Vulnerability and Security Threat Analysis for IoT Devices

After identifying the lack of security about the Internet of Things devices and posing a threat to remote workers and businesses. A table of the application was designed to help remote workers and training them about this topic. It was used the OWASP Internet of things to analyze the vulnerabilities caused by IoT devices.

This section will examine the sorts of vulnerabilities found in IoT devices as specified by the Open Web Application Security Project (OWASP) and present instances of security risks encountered in IoT devices.

5.4.5 IoT Vulnerability Project

The goal of the OWASP Internet of Things Project is to help manufacturers, developers, and consumers better understand the security issues surrounding the internet of things and to empower users in any context to make better security decisions when developing, deploying, or evaluating IoT technologies.

[20]https://www.phpmyadmin.net/

OWASP IoT Top 10 2018	Description
1. Weak Guessable, or Hardcoded Passwords	Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed system
2. Insecure Network Services	Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.
3. Insecure Ecosystem Interfaces	Insecure web, back end API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
4. Insecure Ecosystem Interfaces	Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (unencrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates
5. Use of Insecure or Outdated Components	Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain
6. Insufficient Privacy Protection	User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
7. Insecure Data Transfer and Storage	Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
8. Lack of Device Management	Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
9. Insecure Default Settings	Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
10. Lack of Physical Hardening	Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

Figure 12: OWASP IoT top 10 2018,

The reason to focus on OWASP project for the IoT vulnerabilities and threats was the nature of the approach and the methodology used to measure the risk. The OWASP project is an important first step in leveraging expertise, testing, and ensuring compliance. The inclusion of OWASP was primarily intended to serve as a starting point for implementing security controls and get to know about the main issues involving IoT devices. In addition, the firmware analysis was an excellent reference for testing the security and guidance for vulnerabilities. Furthermore, the single list that tackles the primary challenges for manufacturers and consumers was the crucial factor in deciding on the OWASP project. There are many other security frameworks that are super detailed and could also be considered for this project ETSI TS 303 645 V2.1, This project also introduces bestpractices for IoT devices and provides high-quality service. In addition, the document aims to provide guidelines to all parties included in the development and manufacture and consumer. It primarily concentrates on technical controls and organizational policies. The ENISA also developed a baseline security for IoT devices, but it is more oriented on critical information infrastructure. ENISA is the European Union's agency for network and information security. It provides guidelines and recommendations on information security best practices to EU member states.The project covers many applications areas such as smart homes, smart cities, smart grids, smart cards, smart airports and ehealth and smart hospitals. Furthermore, the NIST IR 8228 study contains important recommendations for federal agencies and organizations by addressing IoT cybersecurity and privacy concerns linked to IoT devices. All the frameworks available can help to better secure the IoT devices, each one of them with specific characteristics and instructions.

6 Implementation

We'll talk about how to put the proposed solution into action in this part. Then, only the final level of the implementation, the outputs created, and the tools and languages graphic utilized to create the results will be disclosed.

The proposed solution was to create a cybersecurity training and awareness application that would allow remote workers to learn about various topics by watching interactive videos, taking quizzes, watching movies, and being updated on the latest cybersecurity news. The application was created with phpMyadmin for the database, PHP for the backend, and HTML, CSS, and JavaScript for the front end. The end product is a web application with a site that displays all of the films accessible on the platform, as well as links to watch them, classes, movies, quizzes, and a news page.

The application's goal is to be user-friendly and uncomplicated. The videos progress feature will allow users to resume watching their videos from where they left off. A checked status will be shown in the videos once you've finished watching the training.

A security evaluation form will be supplied, allowing each user's remote office setting to be identified.The users will experience a dynamic and enjoyable experience. After watching the classes, users will have the opportunity to solve quizzes about each topic to solidify their understanding.

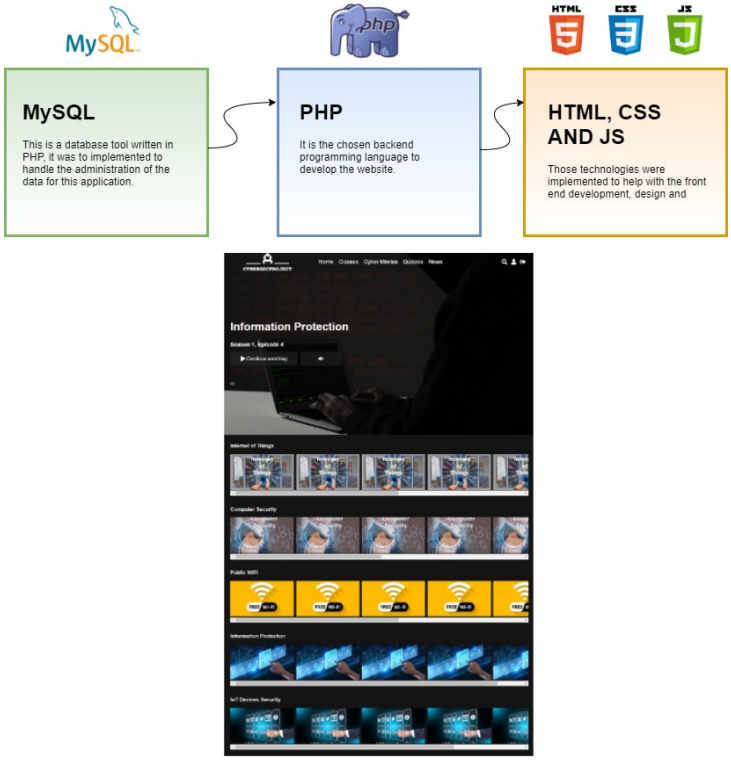

Figure 13: Application ecosystem.

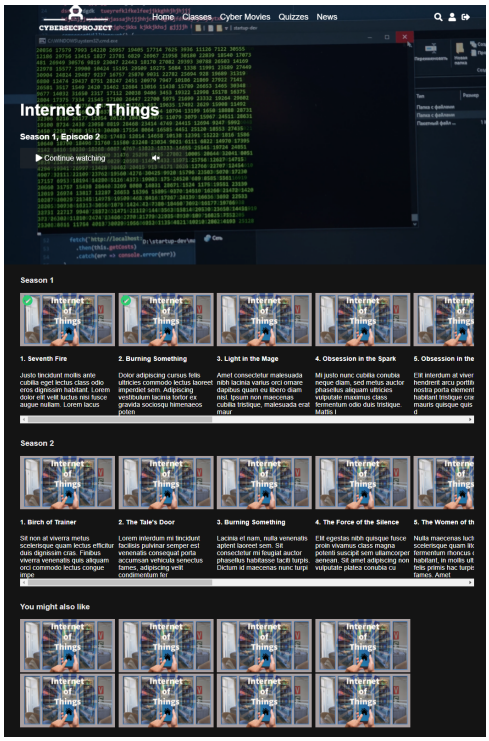

Figure 1: Entity page with all the seasons available.

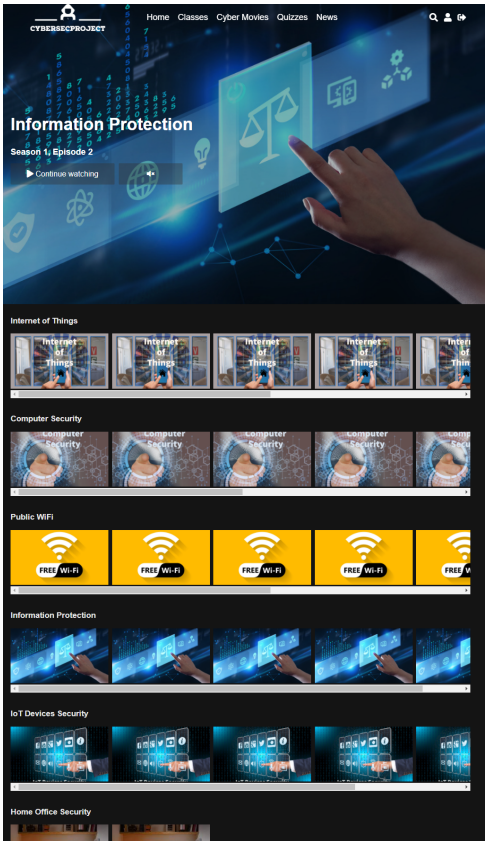

Figure 2: Homepage, topics separated by categories.

7 Evaluation

This section will present a comprehensive analysis of the results and main findings of the study and the implications of these findings both from academic and practitioner perspectives. An evaluation of the remote working scenario and cybersecurity-related questionnaire. For a better understanding, some graphs from a survey filled by remote workers will be presented here.

7.1 Case Study 1: Working Remotely

The first question in the survey is to see if the participants had previously worked remotely before COVID-19. 64,4 percent of those polled stated this was their first time working from home, while 35,6 percent said they had previously worked remotely.

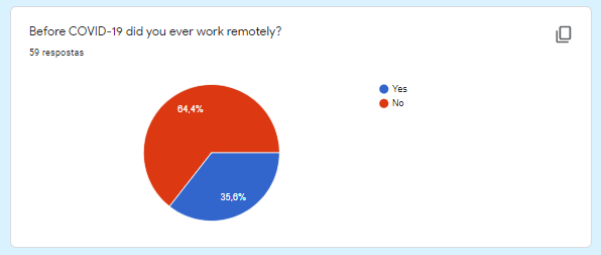

Figure 16: Before COVID-19 did you ever work remotely?

7.2 Case Study 2: Positive or Negative impact caused by working remotely.

The second question sought to determine whether working remotely has a positive or negative influence. Working from home was a new experience for most of the participants, and 0 percent of the surveyors responded on scale one on a scale of one to five. Also, 1,7 percent chose option two, 15,5 percent chose option three, 46,6 percent chose option four, and 36,2 percent chose option five on the scale.

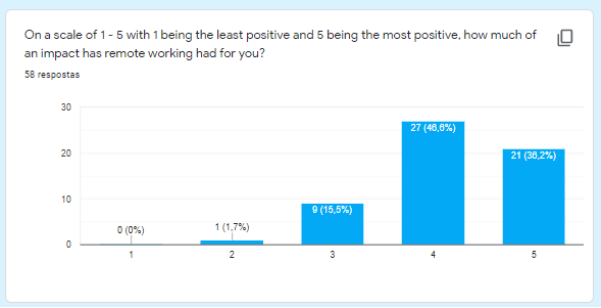

Figure 17: how much of an impact has remote working had for you?

7.3 Case Study 3: Positive or Negative impact caused by working remotely in terms of Productivity.

On a scale of one to five, the influence of working from home on participants' productivity was examined in this case study. In which 1,7 percent agreed on scale one, 1,7 percent

on scale two, 35,6 percent of the top participants chose option three on the scale, 27,1 percent chose option four, and finally 33,9 percent determined that remote working has had a major impact on productivity.

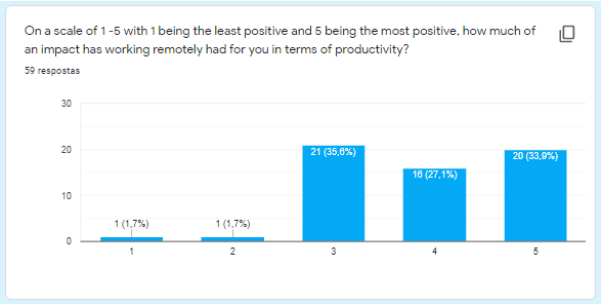

Figure 18: how much of an impact has working remotely had for you in terms of productivity?

7.4 Case Study 4: Study involving the possibility of working from home permanently or on a blended approach.

The major goal of this question was to elicit responses from participants and determine whether they would like to work from home full-time or on a part-time basis. Surprisingly, 59,3 percent of those in the first position said they wanted to work from home full-time, and 39 percent said they preferred a combined/blended approach.

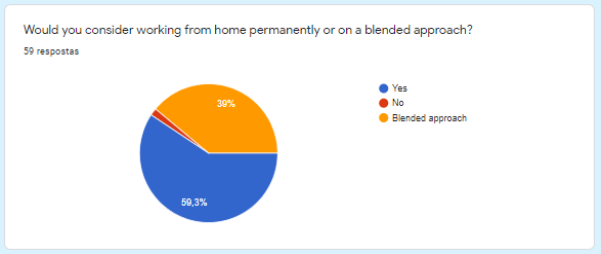

Figure 19: Would you consider working from home permanently or on a blended approach?

7.5 Case Study 5: Study involving the opinion if remote workers have seen more Phishing emails, spam emails and Fraudulent emails lately

The goal of this study was to encircle the participants and see if they've been exposed to more cyber dangers like phishing emails, spam emails, or fraudulent emails since working from home. Surprisingly, 55,9 percent of the participants said no, while 44,1 percent said yes.

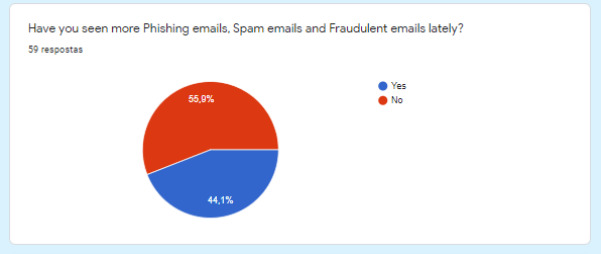

Figure 20: Have you seen more Phishing emails, Spam emails and Fraudulent emails lately?

7.6 Case Study 6: Study involving the opinion of remote workers are more concerned about Cyber and Data Security while working from home.

The goal of this survey was to find out how concerned participants are about cyber and data security while working from home. 54,2 percent of respondents said yes, while 45,8 percent said they are not concerned about cyber and information security while working from home.

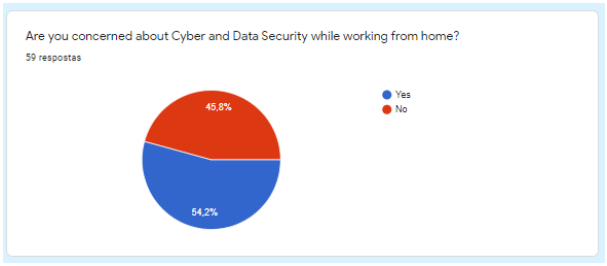

Figure 21: Are you concerned about Cyber and Data Security while working from home?

7.7 Case Study 7: A study involving an analysis if the participants have completed a Cyber Security Training Awareness program specific for the remote work environment

This question had the purpose of analyzing if the participants had completed a Cyber Security training and awareness program specific to the remote work environment. Also, unexpectedly, 59,3 percent of the participants answered that they had not received specific cybersecurity training for the remote work environment, whereas 40,7 said they had.

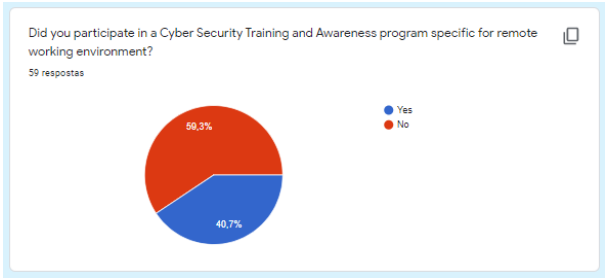

Figure 22: Did you participate in a Cyber Security Training and Awareness program specific for remote working environment?

7.8 Case Study 8: In this case study, participants had an opportunity to rate their IT department's response in relation to the technology infrastructure and security measures.

The majority of respondents, 39 percent, rated their IT departments on a scale of 5 (most favorable) for technology infrastructure and security measures, 35,6 percent liked scale

four, 16,9 percent chose option 3, 8,8 percent chose option 2, and no respondents chose option 1.

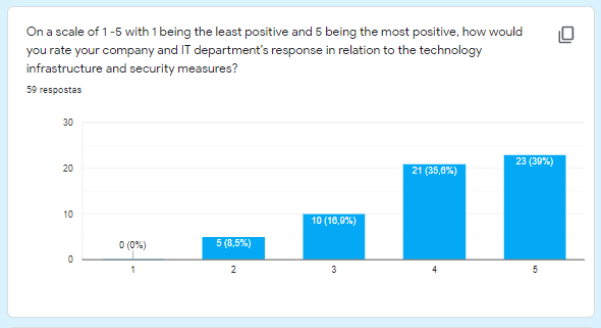

Figure 23: how would you rate your company and IT department's response in relation to the technology infrastructure and security measures?

7.9 Case Study 9: Study involving Smart devices

The goal of this case study was to examine the participants' creative smart technologies in their homes and home offices. It covers their home's use of a number of connected devices and systems. 11,8 percent of respondents own Alexa, 19,6 percent do not own any smart gadgets, and 3.9 percent own only robot vacuum cleaners and mop, among other devices.

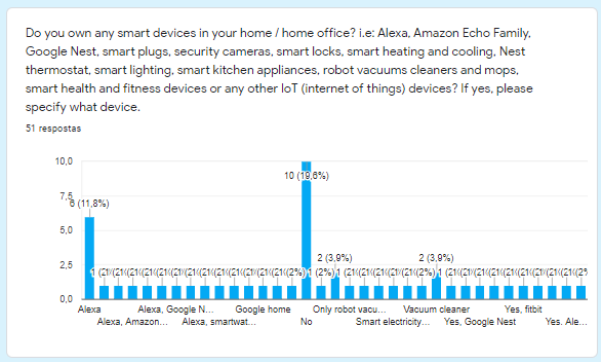

Figure 24: Do you own any smart devices in your home / home office?

7.10 Study 10: Study involving Smart devices and how easy they are accessed from the participant's home office

The goal of this study was to see how easily smart gadgets could be accessible from the participant's home office. Every day, smart devices are connected to the internet. If participants work from home, smart devices pose a threat to the respondents' houses and personal information. The majority of respondents 58,6 percent said that smart gadgets are difficult to access from their home office, while 41,4 percent said yes.

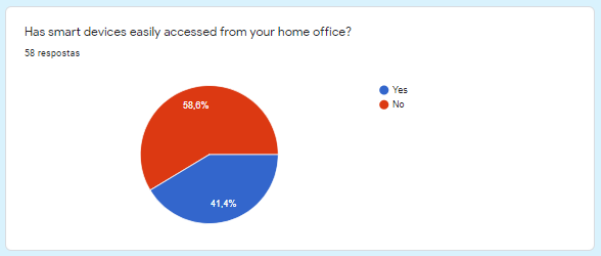

Figure 25: Has smart devices easily accessed from your home office?

7.11 Case Study 11: Study involving the smart devices the participants own for their personal use

This question helped to understand what smart devices the respondents own for their personal use. Most of the participants, 52,7 percent, use a smartwatch, 47,3 percent own a fitness tracker, 40 percent have in their homes a game console, 41.8 own an e-reader, 23,6 use intelligent assistant, etc.

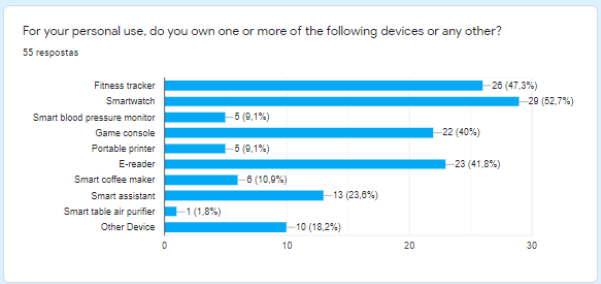

Figure 26: For your personal use, do you own one or more of the following devices or any other?

7.12 Case Study 12: Study related to know if the employers provided the equipment the participants are using or if they are using their own equipment

This study had the intention to identify if the remote workers were working with their equipment or the employer's equipment. A majority of the respondents, 83,1, said they were working with the employer's equipment, and 16,9 were using their equipment.

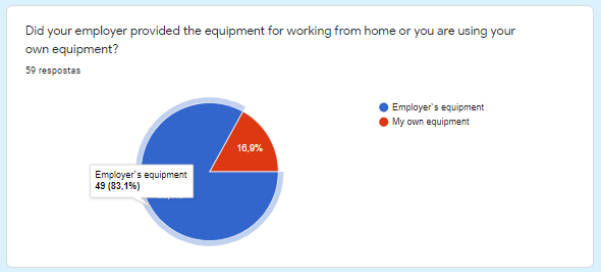

Figure 27: Did your employer provided the equipment for working from home or you are using your own equipment?

7.13 Case Study 13: Security Assessment

In this case, 52,5 percent of the respondents answered their employer did not conduct a security assessment in their work environment, and 45,8 of the participants replied yes, and a small percentage said just briefly.

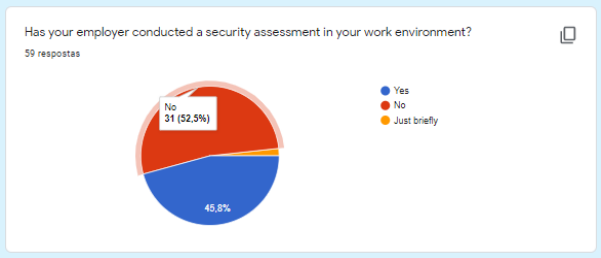

Figure 28: Has your employer conducted a security assessment in your work environment?

7.14 Case Study 14: Study about Smart devices and positive impact in the work environment at home

The goal of this case study was to look at how smart devices may help and have a beneficial impact on the homework environment by reducing distractions. On a scale of one to five, 8,8 percent chose option two on scale one, 45,8 percent chose option three on scale two, 30,5 percent chose option four, and only 7

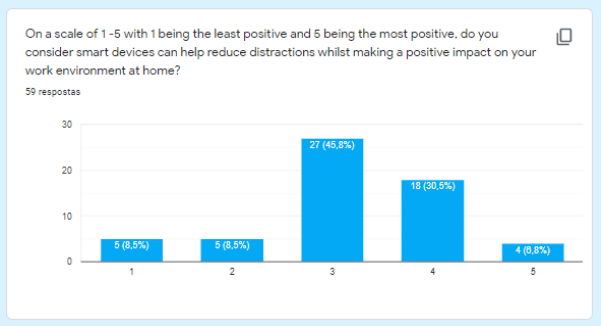

Figure 29: On a scale of 1 -5 with 1 being the least positive and 5 being the most positive, do you consider smart devices can help reduce distractions whilst making a positive impact on your work environment at home?

7.15 Case Study 15: VPN case study

The goal of this inquiry was to see if respondents used a virtual private network, and 69 percent said yes, while 31 percent said no.

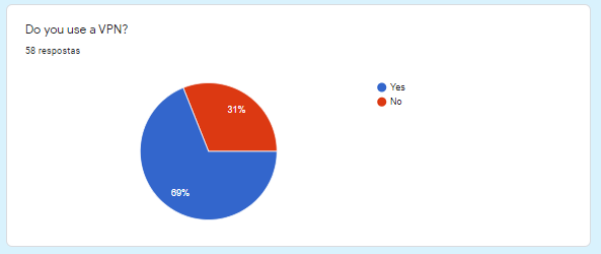

Figure 30: Do you use a VPN?

7.16 Case Study 16: Patching case study

The goal of this case study was to see if participants updated their computers and IoT devices when new security updates became available. The majority of responders 91.5 percent claimed they have upgraded their equipment, while only 8.5 percent said no.

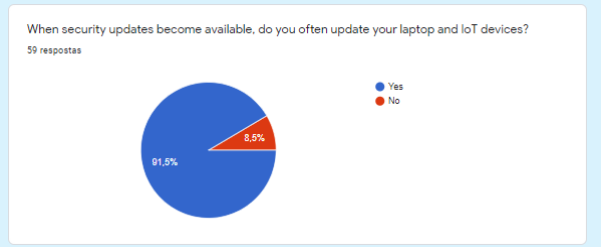

Figure 31: When security updates become available, do you often update your laptop and IoT devices?

7.17 Discussion

Despite the fact that our study included a small number of participants, the results were consistent. As a result, we feel our results are representative.

The COVID-19 had a huge impact on many sectors. Several professionals had to modify their work routine and adopt a working from home regime quickly and compulsory. In addition to literally taking the job home full time, many people had to assume, without outside help, the activities care of their families and their homes, which considerably increased the amount and diversity of demands.

According to the findings, the majority of participants are working from home for the first time. As a result, what was formerly seen as a company-provided benefit has quickly become the norm, and appears to be a permanent part of our working lives. For many of the participants, working from home has positively impacted their lives.

Furthermore, the majority of respondents would consider working from home on a permanent basis. While it is too early to determine the full potential of working from home on a permanent basis, the news suggests that a hybrid strategy will triumph.

On the other hand, this reality did not limit personal and professional life, as homes became our workstations, leading us even more to adopt new behaviors. As a result, the cybersecurity risks of working from home are becoming much more severe than expected. When working from home, companies and their employees must be aware of a series of factors that may pose risks to that company's cyber and information security and its customers.

One of the survey's questions asked if respondents were concerned about cyber and data security, and a sizable percentage of those who responded said they were. Surprisingly, a sizable portion of the respondents stated that they are not. Critical challenges associated with the new security threats resulting from this distributed work setting are a new reality since Working from Home employees face more risks than those in the office. As a result of the survey, most participants replied they see more phishing emails, spam emails, and fraudulent emails lately.

Most respondents answered that they did not participate in any special training specific to remote work environments.

Moreover, 40 percent of participants assessed their company's response to technology infrastructure and security measures as reasonable, which is a fantastic result. It was also

feasible to determine that practically every participant owns an IoT device for personal or household use.

Unexpectedly, nearly half of the respondents indicated their employer did not provide a security assessment specific for the remote work environment.

The majority of those polled indicated they use VPN and upgrade their equipment as soon as new versions are released.

The cyber security training and awareness application is working as expected. The program is user-friendly, engaging, and intuitive. It is an effective methodology that will help remote workers to obtain cyber security information and learning quickly. In addition, it was structured in a system for effective error handling response. The purpose was to develop a unique cyber security training and awareness application-specific for work-from-home employees. The module will discuss security topics that are relevant to remote workers. Although the threats are growing considerably over the years and are real and concerning, the aim is to help mitigate the risks and human error. The application intends to help companies of all sizes and remote workers engagingly increase cyber awareness. Evaluating the application is limited at this time, because the platform is not deployed on a live production environment. Once the application is completed with all the features available, the intention is to deploy on Heroku. In order to verify the application's success was estimated by comparing to previous cyber security training solutions, after examining many applications and papers, it was possible to recognize that they did not provide specific training or guidance for the remote work environment. Consequently, the proposed solution aims to approach relevant topics for work from home employees, such as information protection, public wifi, home office security, reporting incidents, computer security, working best practices remotely, secure file transfers, VPN basics, networking, etc.

8 Conclusion

The primary goal of this research work was to define how remote working has affected workers in Ireland since the start of the pandemic. The research explored the risks of internet of things devices in the work environment. Another goal was to identify if companies in Ireland provide enough support and appropriate cybersecurity training to remote workers in Ireland. We looked at how remote working is changing the landscape of information security in Ireland. A survey was utilized as a tool to learn about the perspectives of remote workers on this topic.

We were able to successfully conclude from the findings that most of the participants are working remotely for the first time and that they have found working remotely to be beneficial in terms of work-life balance and productivity. The majority of the respondents want to work from home full-time.

Our findings related to IoT devices, on the other hand, were worrying: the majority of respondents own some form of IoT device, and 40 percent said these devices are easily accessible for their home office. We determined that most of the participants did not receive a cybersecurity training and awareness program tailored to the remote work environment. The majority of the respondents did not also complete a security assessment to work from home.

The primary purpose is to safeguard users' data, privacy, connections, and home-based systems. Despite lingering doubts about the pandemic's true impact on business,

many organizations recognize the need to safeguard their data. Therefore, companies must invest in telecommunications infrastructures, create security control policies, and implement efficient protection measures capable of extending security to remote workers to maintain operations safe when working from home. Furthermore, technology must be combined with behavioral requirements, tools, procedures, and appropriate security practices.

Finally, we were able to develop a cutting-edge cyber security training and awareness program that can be used by remote workers in Dublin. Unfortunately, there aren't many public-facing applications available today that focus on IoT device security, particularly for people who work from home.

Changes we adopt amid a crisis are not always ephemeral crises that can radically modify our ideas and habits and business and industry in various ways, as history has shown. Our current situation serves as a wake-up call for all businesses to get ready for this new reality, educate their staff, and respond quickly in the event of a cyberattack. After the COVID-19, the world will never be the same, and now is the time to ponder, explore, plan, strategize, and act.

The limitations of the research development was to find articles related to the topic to gather data in the beginning and also the lack of time to complete the quizzes and news pages on the application. The survey could have reached more people in this study, which could have been done better. It was expected to reach a larger number of people, but asking people to take the two-minute survey proved difficult.

The application will be updated in the future to include a live chat help area that employs Artificial Intelligence and Machine Learning. Furthermore, in the future, another concept is to include a system where organizations may do security risk assessments with remote workers using the program.

References

[1] A. A. Shammari, R. R. Maiti, and B. Hammer, "Organizational security policy and management during covid-19," in *SoutheastCon 2021*, 2021, pp. 1–4.

[2] S. Furnell and J. N. Shah, "Home working and cyber security – an outbreak of unpreparedness?" *Computer Fraud and Security*, vol. 2020, no. 8, pp. 6–12, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372320300841

[3] T. B. Pedley, D; Borges, "Cyber security skills in the uk labour market 2020 – findings report," 2020, pp. 660–666.

[4] J. Grimm, "Securing the remote workforce in the new normal," *Computer Fraud & Security*, vol. 2021, no. 2, pp. 8–11, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S136137232100018X

[5] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers and Security*, vol. 105, p. 102248, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821000729

[6] V. Soni, D. Kukreja, and D. K. Sharma, "Security vs. flexibility: Striking a balance in the pandemic era," in *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2020, pp. 1–5.

[7] A. Karale, "The challenges of iot addressing security, ethics, privacy, and laws," *Internet of Things*, vol. 15, p. 100420, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660521000640

[8] E. Clark, "Telecommuting and working from home," in *IPCC 98. Contemporary Renaissance: Changing the Way we Communicate. Proceedings 1998 IEEE International Professional Communication Conference (Cat. No.98CH36332)*, vol. 2, 1998, pp. 21–25 vol.2.

[9] I. Eian, "Cyber attacks in the era of covid-19 and possible solution domains." *Annalen der Physik*, 2020.

[10] Bitdefender, "The indelible impact of covid-19 on cybersecurity," 2020.

[11] T.D.Golden, "The impact of professional isolation on teleworker job performance and turnover intentions: Does time spent teleworking, interacting face-to-face, or having access to communication-enhancing technology matter?" no. 93:6, 2008, pp. 1412–1421.

[12] T.L.Brodt, "Managing mobile work – insights from european practice", new technology, work and employment," vol. 22, 2007, pp. 52–65.

[13] T.L.Elliott, "Digital strategy at display note technologies, posted in meeting room productivity, wireless presentation system," 2015.

[14] D.V.Martino, "working remotely,first edition, publisher: Institute of labor and social security, tehran, iran," vol. 1.

[15] K.Parand, "What is teleworking? why? how?" vol. 4, 2010.

[16] S.Bulut, "Remote working in the period of the covid, journal of psychological research," vol. 1, 2021.

[17] J. Sharit, in *Occupational*, no. 10.1177/001872088202400201, 1982, pp. 129–162.

[18] P. Bleijenbergh, "The telework," vol. 1, 2009.

[19] ITU, "International telecommunications union (itu). itu-tx.1205:series x: data networks, open system communications and security: telecommunication security: overview of cybersecurity 29," vol. x, 2008.

[20] I. . (2005), "Iso/iec 27002: code of practice for information security management," vol. x, 2005, p. 1.

[21] M. H. Whitman ME, *Principles of information security.3rd ed.Thompson Course Technology*, 2009.

[22] D. Ryan, "Secure the future 2020," no. 10.1177/001872088202400201, 2020, pp. 129–162.

[23] R. Ali, "Looking to the future of the cyber security landscape," *Network Security*, vol. 2021, no. 3, pp. 8–10, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1353485821000295

[24] Netwrix, "2020 cyber threat report," 2020.

[25] M. Katz, "Securing connectivity for remote workforces," *Network Security*, vol. 2021, no. 4, pp. 18–19, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1353485821000416

[26] S. Boonkrong, *Authentication and Access Control: Practical Cryptography Methods and Tools*. Apress, 2020.

[27] D. Usha and M. Bobby, "Privacy issues in smart home devices using internet of things – a survey." 2018, pp. 566–568.

[28] S. Haller, "The internet of things in an enterprise context, in future internet,fis 2008 lecture notes in computer science," vol. 5468, 2009, pp. 14–28.

[29] N. Council, "Disruptive civil technologies: Six technologies with potential impacts on us interests out to 2025 in conference report cr," 2008.

[30] L. Atzori, "The internet of things: A survey-computer networks," vol. 54, 2010, p. 2787–2805.

[31] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of iot systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014, pp. 417–423.

[32] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home iot devices," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 163–167.

[33] M. Y. Madhusanka Liyanage, Pardeep Kumar, *IoT Security*. John Wiley and Sons, Inc., 2020.

[34] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on iot platforms: Communication, security, and privacy perspectives," *Computer Networks*, vol. 192, p. 108040, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621001444

[35] "Cost of a data breach report 2020. ibm security," *Computer Fraud and Security*, vol. 2021.

[36] D. V. D. Brian Russell, *Practical Internet of Things Security - Second Edition*. Packt Publishing, 2018.

[37] S. Furman, M. F. Theofanos, Y.-Y. Choong, and B. Stanton, "Basing cybersecurity training on user perceptions," *IEEE Security Privacy*, vol. 10, no. 2, pp. 40–49, 2012.

[38] S. C. Saikat Dutt, *PMI- Agile Certified Practioner, 3ed*. Pearson India, 2016.

[39] J. Ingeno, *Software Architect's Handbook*. Packt Publishing, 2018.

[40] E. W. Murat Erder, Pierre Pureur, *Continuous Architecture in Practice: Software Architecture in the Age of Agility and DevOps*. Addison-Wesley Professional, 2021.

[41] N. F. Mark Richards, *Fundamentals of Software Architecture*. O'Reilly Media, Inc., 2020.

[42] P. M. Kevin Tatroe, *Programming PHP, 4th Edition*. O'Reilly Media, Inc., 2020.