TELECOMMUTING

LAB-UNIVERSITY OF APPLIED SCIENCES
Bachelor of Engineering
Information and Communication Technology
Autumn 2020

Elom Agbodzie

Tiivistelmä

Tekijä Agbodzie, Elom	Julkaisun laji Opinnäytetyö, AMK	Valmistumisaika Syksy 2020
	Sivumäärä 78	

Työn nimi

Telecommuting

Tutkinto

Insinööri Ammattikorkeakoulu, Tieto- ja viestintätekniikka

Tiivistelmä:

Maailma, jonka olemme aina tunteneet lakkasi olemasta COVID-19 pandemian puhkeamisen aattona, mikä pakotti meidät radikaaliin muutokseen sekä yksityis- että työelämässä. Sen suora seuraus on yhden tehokkaimpien teknisten välineiden syntyminen, joka näki valon 70-luvun alussa, mutta vasta nyt aletaan ottaa käyttöön maailmanlaajuisesti: “Etätyö”.

Etätyö mullistaa meidän maailmamme ei vaan turvallisimmalla ja nopeimmalla mutta kirkkaimmalla tavalla kaikilta osin, jopa pienemmiltäkin osin. Meidän elämäntapamme on muuttunut parhaaksi mutta sen mukana tuli ruma, ankara todellisuus: “*virtuaalielämän sivuvaikutukset*” josta tullaan myös puhumaan tässä työssä. Kuten olemme jo tottuneet todellisessa elämässä, jokaisessa yhteyskunnassa on aina hyviä aikomuksia omaavia ihmisiä, jotka noudattavat lakia ja haluavat parantaa maailmaa tekemällä yhteiskunnasta paremman paikan elää. Samasta yhteiskunnasta löydetään myös ns. lainvastaiset, jotka pelkästään, ajavat omaa itsekästä etuaan. Sama tilanne vallitsee myös “digitaalisessa maailmassa”. Tärkein ja merkittävin “vanhan normaalin” ja “uuden normaalin” välinen ero on se, että rikollisten kiinnijäämisen aste (asteikolla: 0–10) on vanhassa normaalissa 5 ja uudessa normaalissa 10. Tämän vuoksi rikollisten jäljittäminen vaatii erittäin päteviä asiantuntijoita: “*kyberturvallisuus tiimit*” sekä lisäksi huomattavan määrän aikaa rikollisten kiinni saamiseen.

Tässä opinnäytetyössä, käydään ensin läpi lyhyt määritelmä etätyöstä, sen eduista ja haitoista, siitä, mitä vaikutuksia COVID-19 oli ja on edelleen aiheuttamassa maailman taloudellisiin rakenteisiin ja mihin meidän uusi normaaliutemme heijastaa meitä lähitulevaisuudessa. Lopuksi keskitytään virtuaalimaailman tuomiin vaaroihin sekä suosituksiin millä keinoilla pystytään lisäämään digitaalisen maailman turvallisuutta kyberturvallisuustiimien avulla.

Asiasanat

COVID-19, Digitaali-, Elämä, Etätyö, Hakkeri, Koronavirus, Kyberturvallisuus, Liikkuva, Maailma, Riskit, Taudin puhkeaminen, Työvoima, Uhat, Yritys.

Abstract

Author Agbodzie, Elom	Type of publication Bachelor’s thesis	Published Autumn 2020
	Number of pages 78	

Title of publication

Telecommuting

Name of Degree

Bachelor of Engineering, Information and Communication Technology

Abstract:

The world as we have always known it ceased to exist on the eve of the outbreak of COVID-19 pandemic, what propelled us into a drastic shift regarding both in our private professional lives. This gave rise to one of the most powerful technological tools which saw the light in the earlier 70s but had not been widely being used up till now: “*Telecommuting*”.

Telecommuting is revolutionizing our world in the safest, quickest, and brightest way in every aspects of our lives. So, not only our way of life has changed for the best, but with it came the ugly harsh reality. As we already accustomed to real life, whereby in every society on one end there are always been those people well intentioned who abide by the law hence try to make the society a better place, and on the other end the outlaws who would not stop at anything to make the world go upside down for solely their own selfish interests, so do we have in the new ultra-modern “*digital world*”. The main difference between the “*old normal*” and the “*new normal*” is that criminals are getting harder to get caught as tracking them required well-qualified teams: “cybersecurity” and an incommensurable amount of time to get them down.

In this thesis, we will first go through a brief definition of telecommuting, its advantages and inconveniences, what effects COVID-19 had and is still having on the financial, economic structures of the world and where our new normalcy is projecting us to in the nearest future. At the end, we will focus on the dangers usually encountered online and how to decrease those attacks intensities with the ever reliable and unfailing support of the cybersecurity teams.

Keywords

Company, Coronavirus, COVID-19, Cybersecurity, Digital, Hacker, Life, Mobile, Outbreak, Risks, Telecommuting, Threats, Workforce, World.

TABLE OF CONTENTS

1 INTRODUCTION

Onsite or on-premises or the oldest and traditional way of conducting business sits firmly deep within us. This is fairly understandable because such an approach has always been deeply rooted in the history of work since the dawn of ages. The object of the work, the tools and the materials required to accomplish professional duties and the use of a common work input have been the most sensible focal point both in time and space. Production control, the required materials as well from the informative flow and interactive point of view is still often the case today. The development occurring within the information and communication technology (ICT) field as well as the constant growth of the data contents work-related are changing the dynamics. In jobs where data processing is the key part – and still is in several cases, it is now possible for an employee to work or perform the required professionals' tasks either fulltime or part-time off company premises.

Even as close as in the late 90's, there had not been a major breakthrough, until 10 years ago we started noticing a rise of telecommuting even though it still was not widely adopted as the new modus operandi.

While in the traditional field of work, the employee has to move to wherever the job is, in telecommuting it is simply a matter of the job being transferred to the employee irrespective of his/her location. In addition to the employees work ethics, the potentials of telecommuting are beyond expectations when the right tools, infrastructures, materials are put in place. Let's do not forget that this idea has not been new: home work in which the employer supplies the materials and the equipment necessary for the work for an employee so the work can be done at home is old, albeit already giving way, existing way of working. With the new telecommuting, physical materials are no longer transferred but the content of the information in the electronic form is transferred. Thus, the work can also be called *e-work* or *decentralized work*.

Even though all jobs cannot pass through the process of telecommuting, it is however advisable to set up a functionable telecommuting model around each company as a preventive measure in regards to any sorts of disaster that would have a financial crisis impact on the business. It sounds easy when we talk about telecommuting solution, however it requires a lot of resources and time as to come up with a flawless model whereby company productivity is on the constant rise, employees maintaining their work ethics, practices and most importantly protecting the company assets as working is totally digitally oriented . So, the early an ideal solution is concocted and tactfully laid down, the better are we prepared to face all sorts of crisis. A perfect example is the recent pandemic: “corona-virus” which was a huge blow for many technically unprepared companies, so the earlier an adequate telecommuting solution is put in place, the better it is. The outbreak of COVID-19 put the whole world onto another stratosphere: work as we have always known it is far away from the new model through which businesses are conducted nowadays. The new norm being totally already integrated into our livelihoods, we therefore need to up our games to make the best of telecommuting wisely and safely.

This thesis consists of articles that describe in a more detailed way, the human resources dimensions of telecommuting, the productivity and the competitiveness potential, shortly presented above, the good practices and the “*rules of the game*”, from both the sole employees and the employers or companies perspective. Moreover, lights will be shed on the impacts of COVID-19 both in our private as well as professional lives as these two latter are closely cohabitating more than ever. Finally, we will elaborate about the immanent dangers in the digital world and recommendations regarding the cybersecurity aspect of telecommuting.

2 WHAT IS TELECOMMUTING?

2.1 A brief definition

Telecommuting also known as “telework”, “remote work”, “future of work”, “working from home (WFH)” came into vigour around year 1970 to ascertain new ways works can be done. Thanks to modern technology, telecommuting enables us humankinds to make a positively drastic shift from a company/organization’s brick-and-mortar location to a completely different location such as residence, or in the neighbourhood like as a co-working space, public library, coffee shop or any other location when one feels comfortable to perform works-related tasks (Figure 1).

Work as we used to get accustomed to, has now taken a new dimensional shape: this is not only the beginning of a new era but a promising future towards a better world where impossible will become possible.

Figure 1. Working within the comfort of your home. (Moonlyte 2020)

2.2 Types of Telecommuting

Due to the exponential evolution of technology, it is no surprise that nowadays many jobs can be done off the organization premises and two most vital elements required in all circumstances are: online connection (access to internet) and a computer. These jobs are classified into three main categories based on how and where occupational duties are performed:

- THE CORPORATE TELECOMMUTER OR REMOTE WORK

  The telecommuter has the best of both worlds in other words, being able to perform occupations "off-site" and still has "on site" presence with co-workers at the office. A remote worker has to occasionally show up at the organization's premises for meetings. For instance, people who travel for the greater part of time for work purposes such as sales representative, are as well considered as telecommuters. Remote work offers flexibility of performing professional duties from the comfort of one's home, the employer being responsible for all the equipment and software. In addition to that, the telecommuter perceives a steady salary, meanwhile the downside of it is that the employer still has all the control of how a telecommuter's working days goes by.

- VIRTUAL JOB

  Unlike the remote work, this position offers 100% location freedom, reason why it is also called: "*The independent contractor*". The telecommuter has the most control, especially if the telecommuter is a parent who wants to care for children during daytime. As such, the telecommuter is not attached to any kind working conditions stipulated by law from the employer, nor this latter can insist on the telecommuters working hours. The main control which the employer has over the telecommuters is the deadline and the end-product stipulated in the contract signed by both parties. In this category the telecommuter is not forcibly limited to one employer: "the sky is a limit as to how much income can be made". On the downside the income is not steady as it is for the telecommuter corporate: no benefits coming from the employer, and the telecommuter is in charge of own equipment and software, making sure working tools are updated and on point. The teleworker takes care of own his/her self-employment taxes and other issues that is usually less of a concern of an employee.

- WORK-FROM-HOME-JOB

  Work-from-home also known as the *Self-employ teleworker* is where the absolute wealth and freedom lay. The teleworker may or may not have a home office and this field of work allows for naming one's own price for work done, choose the type of people one wants to work with, and grow as quickly or slowly based on talents, determination and zeal. So clearly, all opportunities start and end with the teleworker. The success of the telecommuter relies solely on him/her.

  However, this type of telecommuting holds the most risk between the two other type of telecommuting we discussed earlier, as the teleworker has his/her own business, constantly in search of potential clients while working strictly via

> phone, fax and Internet. It might also require of you to be available even beyond standard business hours as one's income depends a great deal on how much customers one can bring in and as such availability plays a big role in an employer-customer relationship dynamics. This route offers no benefits (unless the telecommuter's company pays for them), no helping-hand from an employer, nor co-workers(unless the telecommuter has a partner), no "corporate platform" for an assistance, but immense opportunities for all the brave individuals who choose this path.

(*Mays 2019*).

So, as we can see, this option allows for growths in the most peaceful set of minds but once again all lays in the teleworker's hands.

2.3 Kinds of Telecommuting Jobs

Telecommuting is predominant in almost every industry- thanks to modern technology. It is no surprise that many jobs can be done from home, but the surprising fact is the type of jobs that are most suitable for telecommuting ranges: from brokering stocks to writing to engineering without forgetting that experience and seniority are "a-must-to-have" since many positions require some minimal years of experience for best productivity. But not all jobs can be performed remotely.
In the coming sub-chapters, we will elaborate on these two types of work feasibility.

2.3.1 Jobs that does fall under telecommuting field

These are type jobs that requires a physical contact or presence. Some of these positions are:

- Counselling, some sales (Wholesale, retail trade)
- Health department (medical assessment)
- Leisure and hospitality industry
- Agriculture, fish and hunting, forestry
- Manufacturing, construction
- Public administration
- Transport and utilities

2.3.2 Telecommuting jobs

All jobs falling under this category are location independent, thus can be done within the comfort of one ‘s desired places. Below are some of the telecommuting positions which are offered by several industries all around the world:

- SALES AND MARKETING:

  Account Executive, Community Manager, Marketing Associate, Social Media Manager, Sales Representative, Affiliate Marketer, Telemarketing, Direct Salesperson, Brand Ambassador, Paid Search Strategist, Marketing Designer, SEO Manager, Client Success Manager, Sales Engineer, Account Manager, Growth Marketing Manager, Fulltime Marketing Writer, Marketing Director. (*wwr 2020*)

- CUSTOMER SERVICE:

  Customer Success Manager, Call Centre Agent, Customer Support Advocate, Maintenance, Customer Success Manager, Customer Support, Director Customer Success, Customer Success Lead, Customer Success Manager, Client Success Manager, Customer Experience Specialist, Customer Growth Specialist, Customer Service Representative. (*remote.co 2020*)

- INFORMATION TECHNOLOGY AND COMPUTING:
- Platform Engineer, Programmer, IT Analyst, Incident Response Forensic Examiner, Software Designer Engineer, Client Services, Engineering Architect, Program Manager, IT Support Specialist, Consulting Engineering Manager, Data Engineer, Help Desk Technician, Software/Hardware Assessment Manager, Senior Security Researcher, Business Intelligence Analyst, Database Administrator, Cloud Compliance Program Manager, Senior Incident Response Consultant. (*flexjobs 2020*).
- EDUCATION, TRAINING AND COACHING:
- Training Specialist, Tutor, Product Designer -UX, UI, Administrative Associate, Adjunct Professor, Program Assistant, Organizational Effectiveness and Learning Senior Consultant, English-as-a-second-language, Learning Lab-Instructor, High School Special Education, Speech Language Pathologist, Personal trainer, Research Operation Manager, Curriculum writer. (*flexjobs 2020*).
- HEALTH CARE:

Clinical Content Creator, Director, Appeals and Grievances Reporting, Healthcare Consultant, Coding Consultant Inpatient 3, Client Billing Analyst, Medical Transcriptionist, Director of Therapy, Coding Auditor, Tele-doctor, Nurse Practitioner, Clinical Instructor- Psychiatric Mental Health Nurse Practitioner, Medical Coding Specialist, Military Treatment Facilities. (*remote.co 2020*).

- ADMINISTRATION:

  Virtual Appointment Setter, Assistant, Telecom Project Coordinator, Account, Admin Clerical Assistant, Sales Support Assistant, Site Manager, HR Assistant, Marketing Administrator, Account, Production Assistant, Administrative Assistant. (*Working Nomads 2020*).

2.4 Key factors to take into notice when applying for teleworking positions

Telecommuting appears to be the ideal work situation, as it fits into every type of lifestyle known to Human Being. We have certainly noticed, telecommuting comes in different shape and forms, hence vital to take few factors into consideration before going "*Telecommute"* or applying for telework-related position.

- DISCIPLINE

  Working from the comfort of one's residence gives a lot of flexibility, but if care not taken you will wander off and having nothing to account for at the end of the day. So clearly "distraction" is not an option. Successful telecommuters abide by a set of self-definite rule: "daily schedule and routine" to stay on track and be the best productive as they can be.

- LOCATION

  - What options are available in terms of "workspace"? : many people start their work-from-home day in a bed or on a kitchen table, which is not the ideal situation since work productivity is at its best in a quiet designated environment where you can really be in your element and avoid distractions of any sort.
  - What are the geographical limitations: will the organization allow you to work outside a specific town, state or country or region?
  - Are you legally covered by the organization's insurance while working at an off-site location?

- QUALIFICATIONS
    - Is a prior working telecommuting experience required?
    - Who will you be working with or who will guide you through your working schedule?
- HANDLING OF DISTURBANCES

    A concise schedule should be laid down for work and anyone such as pets, children or for the plumber coming in for a repair that may disrupt while you are at work, they should be aware of your schedule, and so should not get into your way. There must be a frame time when to attend to various interruptions that might occur, and this comes through planning by anticipating potentials disruptions or interruptions. Also, a brilliant idea is to add a browser apps averting you from surfing and wasting time online.
- SECURITY AND EQUIPMENT
    - What supplies do you already have at your own disposal?
    - What supplies will the recruiting firm provide you with? (Items may or may not include a phone, modem, printer, computer, and cybersecurity)
    - Do you have access to the required materials and tools?
    - Are you allowed to use WI-FI?
- FLEXIBILITY
    - Is it partial telecommuting or 100 % (fulltime)?
    - Is it required of you to be available during standard working hours?
    - Is time-tracking used to check your work-input or must you log into the company portal during working hours?
- COMMUNICATION
    - How familiar are you with the technology the company uses?
    - Does the telecommuter’s position require frequent meetings?
    - What type of tools are needed to communicate with the rest of the organization?

3 TELECOMMUTING BENEFITS & DRAWBACKS FOR EMPLOYEES AND EMPLOYERS/COMPANIES AS WELL AS IMPACTS WITHIN OUR COMMUNITIES

3.1 Telecommuting Benefits & Drawbacks for Employees

Technological progress since the late 20th century has made it possible for workers to decide about their working structure or environment. This freedom of choice means a total break away from the traditional working structure, hence the birth of "*remote works*" and its exponential growth as confirmed by a report named "The State of Remote Work 2018" (*Griffis 2018; 2020*) revealed that:

- 90% of telecommuters are willing to continue with working remotely for the rest of their lives.
- 43% agreed that the biggest advantage to telecommuting was the ability to have a flexible working schedule.
- 15% came forward on the basis that telecommuting enables them to spend considerable amount of extra time with their families.

So, while telecommuting benefits both employers and employees, it also holds its challenges, all of which will be discussed in the coming chapters.

3.1.1 Benefits

Telecommuting incorporates tons of advantages for employees which we will break into 9 major areas:

- FLEXIBILITY

  A greater flexibility is achieved through telecommuting, this gives a teleworker a great freedom over the working hours and work location. In addition to that, flexibility enables the employee to create the perfect balance between work and personal obligations. Through flexibility can be achieved: a tremendous improvement of work morale and physical stress through the reduction of stress, diminishing "*negative plethora*" which is a procedure whereby attitudes in addition to behaviours carry over from one role to another. Studies have even shown that workers in healthcare institutions employed by supervisors with low family ties and creativity were highly subjective to CVD (Cardiovascular diseases) threats based on both biological marker evaluations and reports of doctor prognoses *(Kratz 2016; 2019*).

- CUTTING DOWN OF EXPENSES AND MORE FREE TIME

  Zero commuting: "*a survey revealed that 45% of employees related to commuting as the worst part of their mundane*" (*Gaetano 2020*). Working from home cuts automatically all costs associated to all types of means used to get to work and back home. No transportation cost, no dressing codes at home, meaning no expenses on clothes, or dry cleaning or buying lunches and coffee out of the office and any other working garments that are part of your daily routine are out of the way. In addition to these benefits, there are no childcare expenses.

  So, on a large scale you end up saving a considerable amount of money over the year. However basic things such as a computer, a software, reliable phone service, and a fast internet connection may cut slightly off your savings. Nevertheless, you will still be the winner in this situation as a study revealed that *permanent teleworkers put aside well atop $4,000 yearly and gain the equivalent of 11 days per work per year*. (*Shepherd 2020*)

- EMPLOYEE SATISFACTION

  Studies showed that full-time telecommuters acknowledge their happiness towards their job 22% more than non-remote workers. For companies(employers), this is a synonym of higher retention rates. In other words, happier an employee is, less likely he/she would want to quit his/her job. (*Owllabs, 2020*).

- HEALTH-WISE

  No employee is at a risk of any type of contamination or exposed to their ill coworkers who should have stayed home under the brick-and-mortar system. Moreover, even when a telecommuter gets sick, work still goes on, which once again increases the productivity of a company. Adding to this, a telecommuter works at his/her own pace without pressure, thus eliminating any stresses or frustrations as a survey reflected that 82% of telecommuters report having a higher morale (*Shepherd 2020*).

  A typical telecommuter is exempt from the harsh chemical of office cleaners since at home one would always use environment-friendly cleaners.

- INCREASED REVENUE

  By telecommuting, not only do your expenses cut down considerably, but you are also still eligible to workers compensation coverage meaning should a work-related accident occur to an employee, he/she is covered by the mandated insurance. Studies have even shown that on average remote workers make more money than their counterparts who do not engage into telecommuting at all, nevertheless they would accept less payment for a telecommuting schedule swap. *In consonance with one survey 34% of United States workforce would be willing to accept a normal salary being cut up to 5% to work remotely*. (*Shepherd 2020*).

- POSITIONS ALONG WITH EDUCATION

  Out of the high proportion of telecommuters that hold management positions at their organizations, 16% of them are managers and approximatively 53% of them hold no less than a bachelor's degree, compare to 37% of their counterparts on-site workers. (*Shepherd 2020*).

- NO DISCRIMINATION

  Hiring offsite or sight unseen reduces greatly any sort of discrimination since an employee is no longer judged through his/her social aspects such as the way one looks, dresses, walks, talks, even the skin colour becomes a minor aspect in the recruiting process since you are solely hired based on your professional qualifications.

- HIGHER EMPLOYEE EMPOWERMENT

  Telecommuting in a positive way, obligates people to be more independent and self-directed.

- EXTENSION OF CAREER

  With all the benefits that telecommuting provides, it also allows people over the age of 64 to keep working as long as they are mentally fit to accomplish their tasks. So, to all those who have inadequate savings or would like to keep an active lifestyle within the working industry, telecommuting opens the perfect door to delay retirement. Additionally, this is not only beneficial to the older generation, but it boots the productivity of companies in particular and economy of a nation as a whole.

3.1.2 Drawbacks

Despite providing a substantial amount of advantages, *telecommuting* also has its downside.

- DISRUPTIONS

  People working companies off-premises may easily ends having nothing done at the end of the day due to a wide range of variety of distractions such as pets, roommates, spouses, children and working in a coffee shop or any similar location can easily infringe in your work performance if you do not set your priorities right.

- TOUGH TO UNPLUG

  Working in the comfort of your own place or any similar place makes one not putting a clear distinction between working hours and personal time, hence becoming difficult to stop working, what in return ends up jeopardizing one's private life.

- LACK OF COMMUNICATION

  Working off companies' premises creates less personal contact between the employee and the co-workers as well as managers, which leads to poor productivity especially when the new teleworker is a novice in his/her field of work (Figure 2). This subsequently leads to stress and frustrations and so impact on the employee's health.

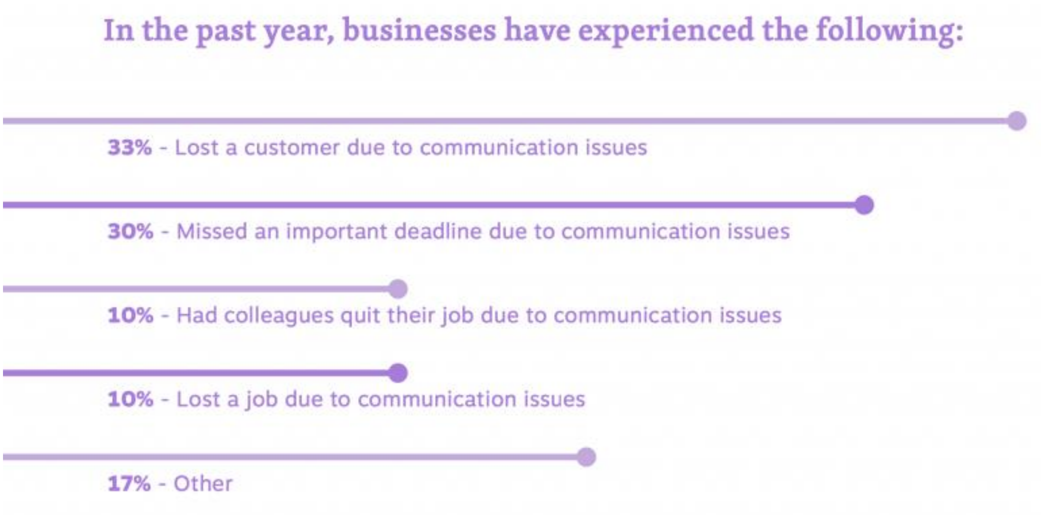


Figure 2. Loss due to communication issues due to not possessing the right tools (Gaetano Dinardi 2020)

- ISOLATION

  People living alone might find it hard to cope with telecommuting as they are completely cut-off the world, having to spend most of their days indoors and easily overworked, what easily leads to health issues.

- LACK OF DRIVE AND DISCIPLINE

  Due to less structure, no supervision whatsoever and the loss of office camaraderie, a telecommuter is let to himself/herself, what creates lack of motivation especially if the employee is the outgoing, social type, so it becomes hard to get any work done.

- LIMITATION FOR THE UNEDUCATED

  Due to the fact that telecommuting required some basics technological knowledge or technical background, young employees and those without university degrees are highly subjective to be cut off the telecommute employment marvellous opportunities.

3.2 Telecommuting Benefits and Drawbacks for employers/companies

In this new digitalized era where every business aspires to success, it becomes obvious that all legal means are to be exploited for financial gain. In the light of this remarkable evolution, telecommuting appears to be one of the major tools that companies seems to run for.

What do we have instore in terms of benefits and advantages at companies' levels?

3.2.1 Benefits

Employers are no doubt benefiting a lot when they set a well-designed telecommuting plan for their employees.

- INCREASED PRODUCTIVITY

    - Fewer interruptions from either supervisors or co-workers, hence the teleworker has more time to focus on his/her tasks and get them done much quicker than it would have been in the work office. As such the productivity is 13 percent higher as compare to their colleagues working in the office as Stanford study showed it. The University of Texas conducted a similar study which showed that telecommuters engaged in their professional activities averagely 5-7 hours longer than their in-office colleagues. (*Villanova University 2020*)

    - Based on scientific research and anecdotal evidence, people who are allowed to work in a flexible working structure see boosts in productivity. A perfect example was JD Edwards teleworkers who had 20-25 percent more productivity as compare to their fellow colleagues working in the office. Adding to that American Express workers who performed their duties via their residence happened to be 43% more productive. (*Digneo 2019; 2020*)

    - The increase in productivity is partially due to our human natural ability to be happier and healthier when we have some control over our work lives. A study based on work from home statistics revealed that 82% of telecommuters have a low level of stress and are happier than the non-telecommuters (*Pinchen 2019*): the lesser the stress, happier and more engaged hence more productive the employees are.

    - Another report "The State of Workplace Productivity Report" revealed that of the 2009 employees that were interviewed, 65% were positive about the fact that remote and flexible work options made them more productive. (*Cornerstone 2014*; *Moonlyte, 2020*).

- Most telecommuters tend to work overtime for free without realizing it. AT&T reported that their remote workers worked on average 5 hours more per week than their counterparts office workers (*Nevogt 2020*). A motivated, responsible worker once up on his/her feet in the morning, no matter what the time can easily get to work immediately, so do not until he/she commutes to the office before starting the day. And once the tasks achieved, a new task can be assigned, hence an increase in the productivity.

- Telecommuting increases work presence: for instance, the employee is required to fulfil multiple tasks at different locations, the virtual approach solves it all. Such inputs are highly valuable as it puts the typical employee ahead of the game by fulfilling the required tasks and even having a lot done despite being home.

Moreover, studies have shown that two-third of managers disclosed that telecommute have a productivity increase. *Furthermore, 86% of the workforce say they are at their productivity peaks while working solely.* So, distractions such as unorthodox meetings, co-workers gossips, interruptions by colleague are totally out of the way. (*Shepherd 2020*).

- ROOMS FOR NO ABSENTEES OR LATENESS OR SICK LEAVE

  Your office being right next to you, in the comfort of your home, this cuts off any lateness which might be due to traffic or broken car. Within the same context, telecommute does not give room to absentees nor sick leave since you can still get work done during certain stages of your illness, and unless under critical health conditions, should you refrain yourself from working. As such during natural disasters such as flood or on extremely snowy days, work goes on. A study found that 69% of telecommuters lower their absenteeism. All these lead to the increase of productivity (*Shepherd 2020*).

- TURNOVER REDUCIBILITY

  The recruiting and training process of new employees always being expensive, telecommuting provides the ideal platform to save money as companies need no more offices or cubicles or any other type of equipment to get the trainees ready for work. Additionally, studies have shown that employers offering work telecommuting positions end up losing lesser employees.

In a Stanford University study, *a turnover rate of 50% was achieved by workers who were offered telecommute positions*. (*Maddie, Shepherd 2020*).

Another survey turned out *80% of responders would be more loyal to their employers if they had any type of telecommuting positions,* while in that same survey *30% of employees quit their jobs because they did offer no flexible work possibilities*. (*Tamara, E. Holmes 2019*).

- FINANCIAL BENEFITS

With the flexibility teleworking offers, companies end up gaining a lot by saving on expenses such as:

- Energy: electricity, light, water: “less lighting, few electrical devices such as printers, scanners and laptops, lower cooling and heating, smaller offices.”
- Real estate: office facilities :“smaller offices(office spaces does cost money)”; other related utilities costs “ cost of equipment, property, parking facilities”; and taking care of those assessment through cleaning, canteens security, as well as their maintenance ceased to be subjects of concerns for companies.
- Expansion of geographical realm: recruiting a new employee becomes most effective and less costly than ever since no expenditures, for instance when it comes to potential employees relocations with their families as the employee can work from wherever location he/she is.

Through telecommuting, employers can easily end up saving over *$11,000 per time and a half per employer yearly (Digneo 2019)*. In 2015 another study showed, employers who offered at least telecommuting part-time positions were able to save $44 billion a year (*Dragomir 2019*).

Even a study found out that office desks are unfilled 50-60% of the time (*Twinstate 2020*), yet companies keep furnishing either permanently or temporarily via rental options office spaces for their staffs. Through the same survey was being revealed that almost 60% of on-premises workers spend enormous amount of time looking for a conference room! *Is not that crazy?* Adding to this an astonishing number of 25% of workers would take a 10% pay cut per half-time telecommuter per year (*Marinova 2020*). So, telecommuting does not solely come with a huge cut of expenses but it also paves a way for a more efficient way of boosting companies profit.

- MORALE VALUE

  The Pennsylvania State University studies revealed telecommuters lifestyle to be more stress-free and happier than their fellow non-telecommuters. Due to their flexible working schedule, it gives them ability to exercise freely without negatively affecting productivity. A physically healthy individual is a synonym of a healthy mind which signifies more enthusiasm and devotions towards daily activities. This has an immediate positive impact not only on the increased of the productivity but on the reduced turnover as well.

- EMPLOYEE RETENTION

  Due to the flexibility telecommuting offers breaking away from the traditional way of working, telecommuting aspires to a high employee retention. Say, for the employees who lives from afar the office, or single parents or parents with children, or workers who are too sick to make it to the office, but can still work from their home, or an employee who has to move domicile to another location, this latter no matter how further away from the office would not flinch an inch his/her output towards his/her work.

- COLLABORATION INCREASES

  The moment telecommuting technologies are efficiently put in place, employees, employers, contractors, companies can work together regardless of logistics and creates a perfect symbiosis for work collaborations. This builds a strong network in a sense that if you are in a dire need to get a task solved, or in need of someone from a datacentre, or HR(human resources) or any responsible in any field, getting in touch with the right ,skilful person only requires you to reach out via email, or instant messaging, or even better via phone call and this without any deep personal relationship. And as time goes on, so will your network grow, and you will then know whom to call on to get the required information or the needed help.

- PROFICIENCY TO HIRE THE BEST SKILFUL EMPLOYEE WORLDWIDE

  Having the best, required personnel is a-must for any business that thrives to succeed, and it is no secret to no one that lesser people are willing to leave their families and friends behind for a new job across the country or worst case scenarios move to another continent. Telecommuting provides the perfect solution to this through the implementation of flexible work policy that enables companies to get hold of the skilful talent regardless of the location.

This is confirmed by a pool: "*over 70% of employee consider the ability to work remotely is somewhat to extremely important to their selection of employer*". (*Moore 2018*; *Digneo 2019*).

- WORKFORCE EXTENSION

  As telecommuting reduces a considerable amount of stress by providing a more flexible schedule, this is a perfect opportunity for a senior employee (at a retiring age) who is mentally fit to still stay in the working force while being productive.

- BUSINESS CONTINUITY

  With telecommuting as a new platform for businesses, this enables companies to successfully set business continuity plans (BCP) in case of natural disasters such as flood, bad weather, pandemic as the one we are having going on now "COVID19" or any other events that might prevent working on office premises.

  As Figure 3 depicts it, even as far back as in 2012, the affluence of telecommuting is fairly noticeable in the marketplace worldwide.

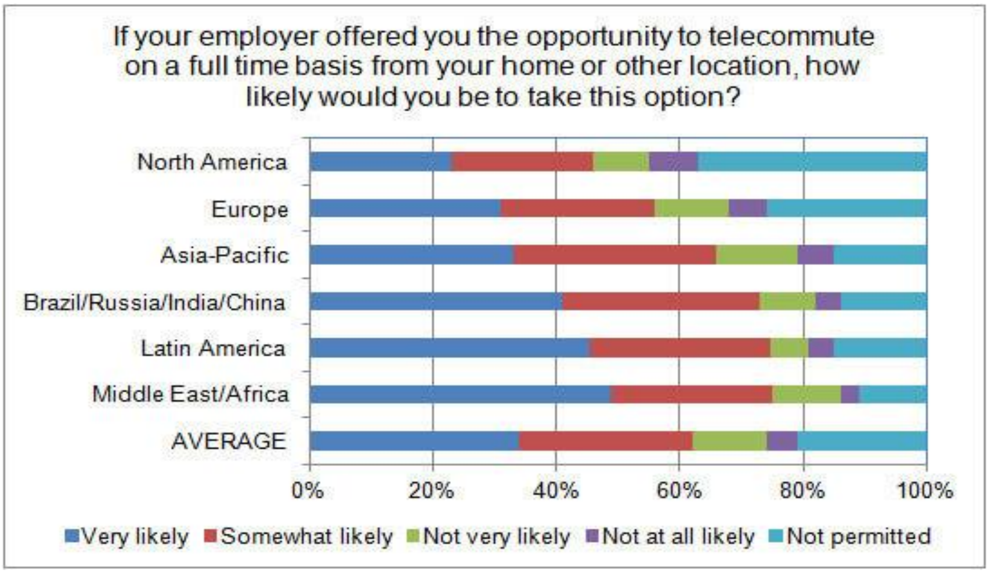


Figure 3. Telecommuting impacts on employments (singularityhub 2012)

3.2.2 Drawbacks

Telecommuting works best for humankind interest. Nevertheless, it comes with challenges.

- LACK OF COMMUNICATION

  Like already mentioned in chapter 2.1.2, both the employee and the employer being out of physical reach clearly limits the ability of the managers or the employers to have a closer look at the employee's productivity. There is no doubt that trust stands as the most valuable weapon in telecommuting and despite the fact that majority of telecommuters productivity is high, there is also a small proportion of employees that use teleworking as an opportunity to slack off. This ends up keeping the employees totally disconnected from the organization's culture. (Refer to Figure 3)

- LACK OF SELF-DISCIPLINE

  Productivity in this field of work comes solely if the employee is self-disciplined hence committed to achieve his/her mundane goal.

- THE REQUIRED EQUIPMENT

  Not all companies provide their employees the right tools to work with. In some cases, employees are expected to use their own electronical devices (laptops, mobile phones and technology) which results in the employee being forced to be on-premises.

- SECURITY ISSUE: NETWORK PROTECTION

  A critical issue that many companies fail to notice is the security aspect of telecommuting. Whenever a telecommuter accesses a company's portal, there is a higher probability of breach due to the security measures the employee may be using. All it takes is a single breach for the company to suffer a data loss that could be costly, that is the reason why owned company equipment should be a standard requirement when it comes to telecommuting. It is also important to point out that in no circumstances, administrator rights should be given to telecommuters.

- INSURANCE POLICY EXPENSES

  One vital strategy for companies to be to be at the top of their games is to purchase a first-party and a third-party insurance policy in a way that:

- First-party insurance policy would protect all the company's assets such as *tangible assets* and intangible assets.
    - Tangible assets are physical assets (office equipment, building, inventory, stocks, cash and bonds)
    - Intangible assets are abstracts assets which are divided into two categories: *Intellectual Property* (copyrights, patents, trademarks, franchises, licensing agreements) and *Goodwill* (the reputation of the company, strategies, workers relations, customer base).
- Third-part insurance policy which would cover any settlements or defence expenses should a data loss occurs.

Such investments while protecting the company also means less revenue for any business with weak foundations or newly built.

- INDIVIDUAL CREATIVITY AT STAKE

  Working within the comfort of your home provides the adequate conditions for better productivity but yet those little moments of distractions at office whereby casual conversations between colleagues may lead to individual creativity taking a co-worker project to another level resulting in promotions, raises and any other benefices attached to individual performances when it comes to creativity are missing.

3.3 Telecommuting impacts on the community

Did it ever occur to you that telecommuting even though has some negative effect in our societies, has also tremendous beneficial effects in our environments but then the positive side of it takes over the negatives ones?

We well expatiate about those impacts in the coming subchapters.

3.3.1 Advantages

Three main factors which helps in the advancement of environmental effort are: the undeniable consistent progress of technology, the tighter legislations cutbacks, and more social consciousness. For the purpose of this thesis we will focus on 8 majors positive effects of telecommuting in our community. Daily transportation being out of the way, meaning removing of cars from the way results in:

- LESS FUEL CONSUMPTION:

  It easily saves a significant quota gallon of gas daily.

- CARBON EMISSIONS REDUCTION:

  Just by not driving to and from work daily undoubtedly diminishes communities contributions to overall carbon emissions.

- LESS ENERGY CONSUMPTION:

  Whether the employee is working at home or in an office, energy consumption is inevitable. However, since our human natural attitudes prone us to take better care of what belongs to us than what is not yours, well the same scenario takes place while working at home and working on-premises hence office-based work consumes more energy.

- AIR POLLUTION REDUCTION

  Driving not only produce carbon, but nitrous oxides (NOx: NO2 may cause respiratory issue such as infection and asthma), particulate matter (PM) as well as volatile organic compounds (VCOs), all of which are destructive to environment and human beings. NOx in contact with VOCs, ammonia and other compounds results in alteration of soil and water acidity, ecosystem diversity and ozone concentration.

- FEWER FOSSIL FUELS IN USE

  Fossil fuels (coil, oil, natural gas, or heavy oils) produce huge quantity of carbon dioxide (CO2) when set to fire. Carbon discharges retain heat in the atmosphere which leads to climate change and global warming crisis. Sadly, all we human have been doing for almost two centuries now is burning fossil fuels purposefully for heat, electricity, transportation and 90% of transportation fuel originates from petroleum products. Hence by working from home, telecommuters diminish the overall energy consumption, so in the process reduce fossil fuel demand.

- REDUCTION OF PAPER USAGE

  An average office worker can barely consume about 100,00 sheets of paper yearly, by coming in with email, software programs, cloud-based applications in other words digitalized-jobs eradicate the disposal or recycling of paper of enormous quantity of paper per year.

- LESS PLASTIC USAGE

  Considering how many workers buy breakfast (food packaging, beverage bottles, utensils), coffee (coffee cups lids) and lunch (plastic bags) daily, it came as no surprise that the world plastic production is approximatively 9 billion to date (*Schad 2020*). By working home, telecommuters have this comfort of eating right out of the bowl, refilling coffee pot, using the same dishware over and over.

- ENVIRONMENTALLY FRIENDLY

  Working off-premises or from any other locations that differs from work premises gives an employee the convenience to set his/her own routine towards work as well as his/her own privacy. While making sure that the productivity regarding his/her work is efficient, motivation builds up to engage into things that matters the most. As such, a telecommuter has enough time for instance to be involved into spending time in nature, gardening in the backyard, taking part in community tasks such as clean-ups, enrolling into environmental organization, support a cause, animals care, ecosystem rehabilitation and spread the word about environmental friendly conscious lifestyles.

3.3.2 Disadvantages

Remember the old saying: “all that glitters is not gold”? Well, it also applies to telecommuting. Below are some few concerns.

- INTERPERSONAL RELATIONSHIP AT STAKE

  Through remote work, the basis on which society lays interpersonal relationship is considerably decreasing. Interpersonal relationship has always been one of the oldest and most fundamentals tools on which our societies have been built for centuries and in humankind history there has never been a single period whereby interpersonal relationship has been not existing but yet a nation saw progress. The urging question is: on what basis are we going to build the future which is our legation for the next generation?

- SOCIAL DIFFERENCES ON THE RISE

  By being away from the offices, workers end up living in their own world hence socializing less which is a huge issue of concern because as stated by Aristotle the great Greek philosopher said: “*Man by nature a social animal; an individual*

> *who is unsocially naturally and not accidentally is either beneath our notice or more than human. Society is something that precedes the individual. Anyone who either cannot lead the common life or so self-sufficient as not to need to, and therefore does not partake of society, is either a beast or a god*." (*Aristotle The Stagirite 350 B.C.E*). We humans cannot therefore live alone. We ought to satisfy natural basics needs to survive! Social life is totally embedded in us. So, as to what the future holds for us is still uncertain, but the undeniable fact is that we must find a way to bring back our normalcy.

All along this chapter 2, a clear distinction as to how telecommuting impacts every little aspect of our lives has been lit. Despite the disadvantages that come up with it, telecommuting brings to the table a whole lot of ingredients (Figure 4) which are good recipes for success both as career-related and in personal life.

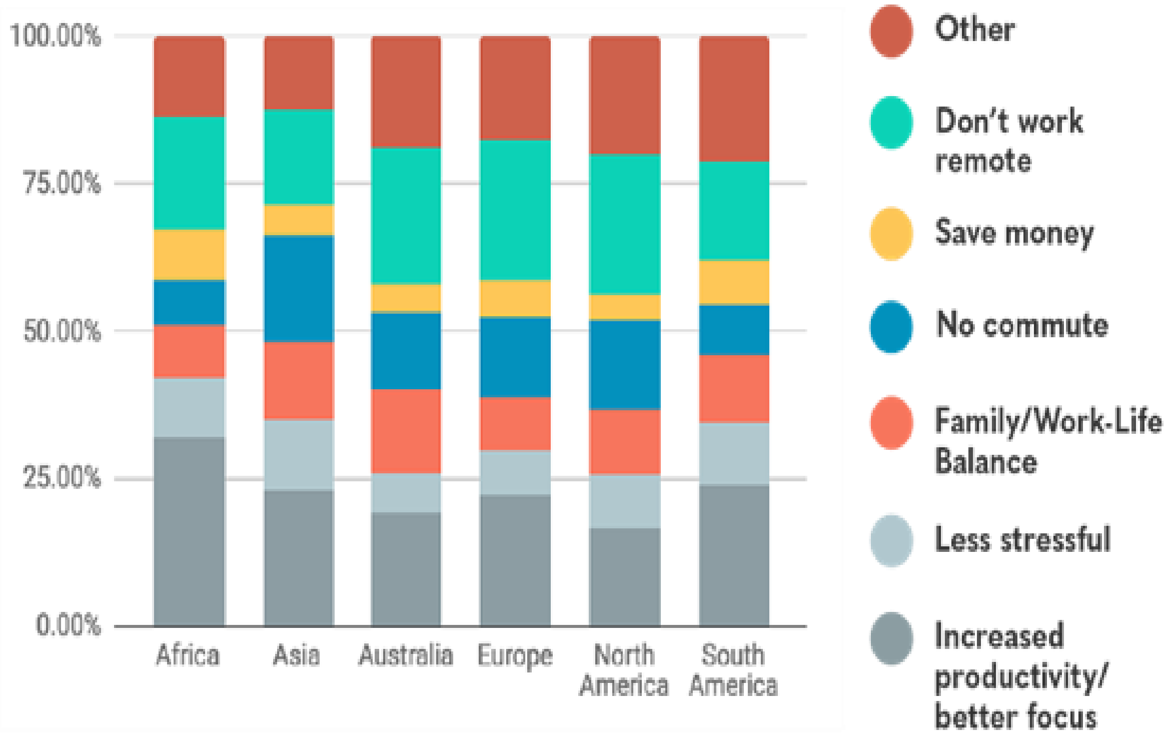


Figure 4. Overview of telecommuting impact in some part of the world (Remoters 2020)

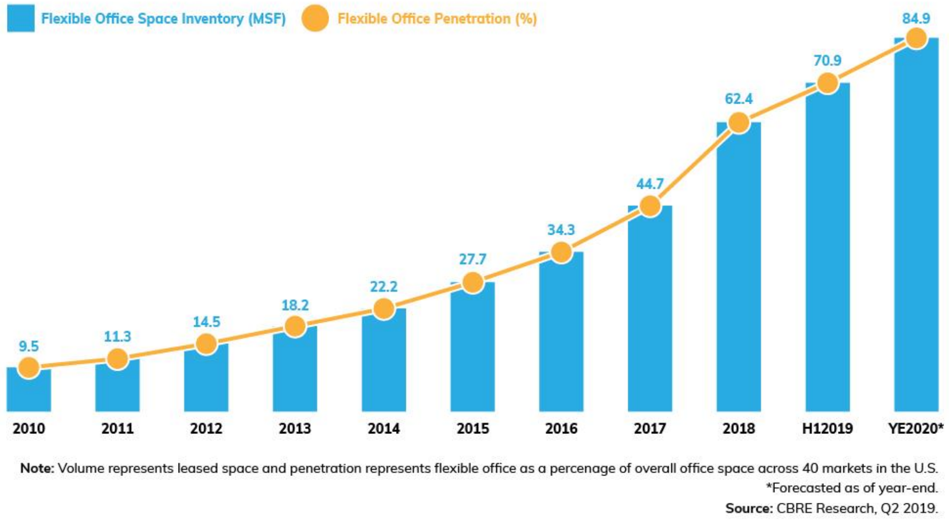
4 TELECOMMUTING TREND IN 2020

4.1 Overview of telecommuting worldwide

Remote work has been around us at least for the past 50 years but has never been visible since not a lot of companies, organization, employers, employees had the obligation to design their whole working infrastructure around this new technology “*telecommuting*”, as workplaces have always been well equipped and furnished, available to employees so why “*go telecommute*”?

Telecommuting has been moving at a small pace for the past 10 years before the outbreak of COVID-19 pandemic hit the whole world by surprise in December 2019. As a matter of fact, as of 2019, only a tiny percentage of 9% of the taskforce in the EU-27 worked at least sometimes remotely as compare to 5,2% in 2009, while the self-employed over the same period of time was respectively 36% and 30% (*Milasi* etc *2020, 1*).

Productivity being the goal of all enterprises, a revolutionising way of doing business was needed to be put in place hence “telecommuting”. As such we see the evolution of telecommuting in some of part the world (Figure 5 & Figure 6) where some nations had an early awakening.



Note: Volume represents leased space and penetration represents flexible office as a percenage of overall office space across 40 markets in the U.S.
*Forecasted as of year-end.
Source: CBRE Research, Q2 2019.

Figure 5. Telecommuting evolution in the United States (Elena Carstoiu 2020)

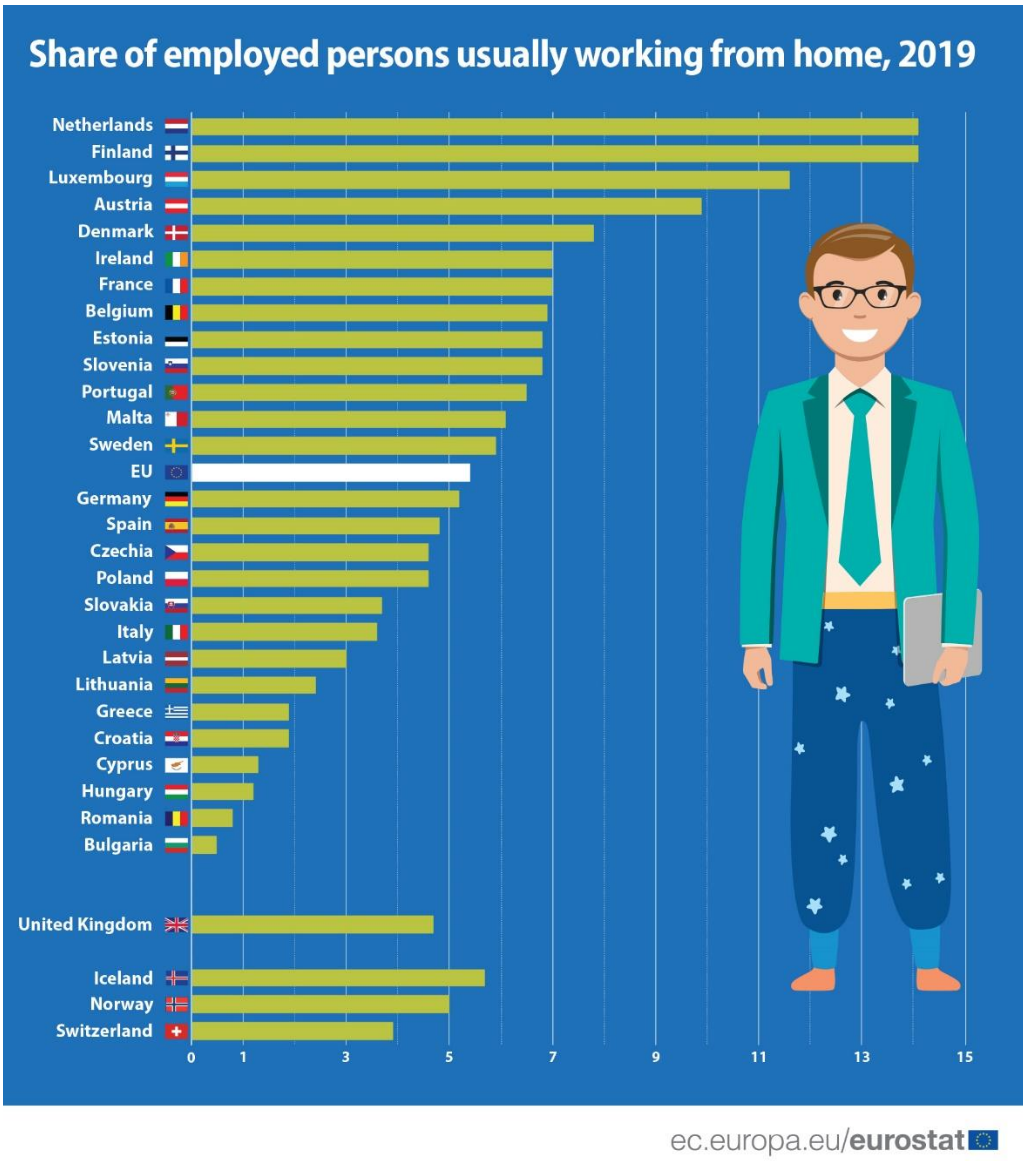


Figure 6. Telecommuting evolution in Europe (European Commission 2020)

4.2 Status of telecommuting

Telecommuting is taking shape across many sectors “ web development, accounting and finance, customer and technical support, teaching, sales, digital marketing, writing, IT, HR and many more”(refer to 2.3), as well as in many countries whereby location of employees is irrelevant but their knowledges and experiences are predominant. Before we jump into the future of telecommuting, let us have a glimpse at where the industry stands as of today.

As technology evolves so does every little component of it: old technologies giving way to the new ones, resulting in remote work being more technically grounded today as compare to the first newly flexible telecommuting companies half a century ago. Thanks to all the development that has been occurring on a slow but ground-breaking steps, we were able to shift from our traditional way of working to a newly modern sophisticated way which has been enforced on us by COVID- 19 pandemic.

Let’s see what the statistics are revealing to us in the rise of telecommuting

Eurofound corroborates this as close to 40% of workers in EU are currently telecommuting fulltime while JRC study provides an estimation of 25% employment rate. (*Daphne etc.* 2020).

In another study “Buffer.com” states that 99% of the participants confirmed that they would rather opt for remote work in their career (Figure 8) and are likely to recommend telework to their siblings, friends, entourage. An astonishing figure which shows that telecommuting has not only become the new normalcy but it is here to stay.

A report by “Zapier.com” revealed that about 74% of the taskforce are willing to change workplaces in exchange of the ones that offers telecommuting positions. As a matter of fact, 96% of workers in U.S. opted with no hesitation as to having flexible positions in regard to their current jobs and 99% of telecommuters want to stick to it from home at least on part-time basis. (*Zapier Editorial Team 2019*).

Embracing telecommuting technology as *a new normal and professional platform* of conducting businesses has seen a rise among consulting companies, and freelancers providing services to customers.

How fast is telecommuting evolving?

According to FlexJobs analysis (*Hering 2020*), remote work saw a considerable rise of 91% within the past 10 years in US. Similar analysis from TechRepublic ended up with the same result (*Bayern 2019*).

Another analysis from *GlobalWorkAnalytics* revealed that among the non-self-employed community, regular remote work has seen a rise of 173% since 2005, meaning 11% faster than the rest of the taskforce. To be more specific, telecommuting has seen a noticeable growth of 115% within the last 10 years in the US (*Remoters 2020*).

Across Europe, telecommuting was a normalcy in some countries long ago before the advent of COVID-19. That is why some EU countries have seen a tiny rise in teleworking industry since the beginning of the pandemic, in contrary to others who have seen a significant increase in telecommuting. This results in a large diversity as to the pace at which telework is evolving in EU member states. A clear idea of it is depicted in figure 7.

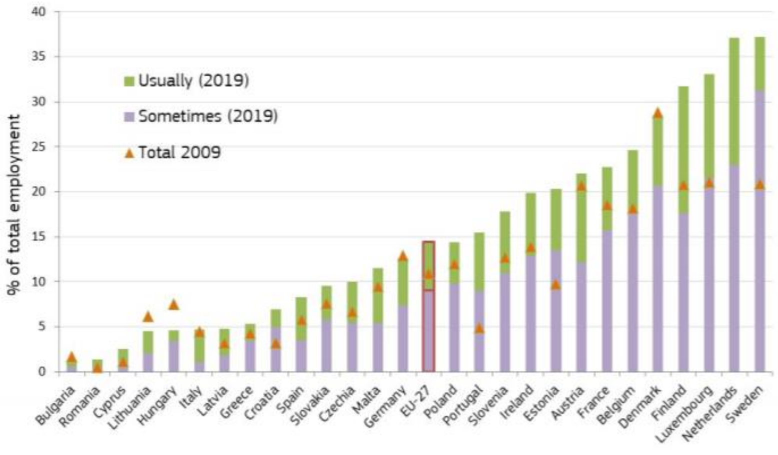


Figure 4. *Prevalence of telework across EU Member States.*

Source: Eurostat, LFS. Variable code: lfsa_ehomp.

Figure 7. Evolution of telecommuting (Eurostat LFS. Variable code: Ifsa ehomp. 2020, 4)

As figure 7 shows it, in 2019 the share of regular telecommuters was higher than 30% in nations such as Netherlands, Finland, Sweden, ranged from 15-24% for Belgium, France and Portugal whereas below 10% in half of EU Member States *(Eurostat LFS. Variable code: Ifsa ehomp. 2020, 4)*. Nordics countries clearly showed the largest growth.

Recent studies by IWG revealed that telecommuting is already effective as 70%of the global workforce community remotely work not less than a day weekly. (*PRNewswire 2018*).

Where do freelancers stand?

In this new era whereby work can be done irrespectively of locations, freelancers have this opportunity to enlarge their already built networks, though it can be harder for start-up freelancers based on their environment, equipment as they clearly are in disadvantage in contrast to bigger organizations in term of support and benefits-like insurance. Despite this downside, currently freelancers constitute between 33%-45% of the workforce, meaning out of 3 telecommuters more than 1 is a freelancer. A number which will undoubtedly growth in the future as according to “Peerism” by 2030, freelancers could constitute 80% of the global workforce (*Christo, Petrov 2020*).

Most preferable location to telecommute

It seems obvious that telecommuters prefer working within the comfort of their home. *Who would not?* Well the statistics confirmed it as 84% of the interviewees during a survey conducted by Buffer “State of Remote Work”. In this this survey, based on employees performances at domicile, it came out that: 8% work at coworking residence while 4% at coffee shop (cafes) (*Buffer etc. 2019*).

4.3 Hiring statistics from enterprises

Telecommuting has taken the world globally more precisely since the outbreak of COVID-19 pandemic. Stats about companies diverting to this new normalcy take a huge proportion in the marketplace, but to have a better grasp at how telecommuting is affecting businesses, we will emphasize on the few key ones.

- TELECOMMUTE LABOUR FORCE
    - In the United States 4,7 million workers (3,4% of the labour force) telecommute at least half time on weekly basis. The same report stated that more than 40% US companies offer remote works positions compare to 5 years ago.
    - 44% of employees confirmed that part of their team has shifted to fulltime telecommuting. (*Buffer*)
    - 44% of companies around the world do not allow telecommuting at all. (*Owl Labs*)
    - Approximately 62% of the workforce between the age of 22-65 remotely work at least occasionally.
    - While 30% of employees telecommute fulltime,18% telecommute one to three times weekly. (*Owl Labs*).
    - Telecommuting has seen 115% in rise for the past decade.
    - Globally at least 52% of the workforce telecommute via homes once weekly.
    - 18% of the workforce telecommute fulltime: other figures conveyed 34% of the workforce as being engaged a day or two weekly, 16% just once monthly, meanwhile 32% of interviewees has no whatsoever experience telecommuting-wise. Stats revealed however a slight gap between the sexes: women being 8% less likely to telecommute than men.
    - Small companies are twice likely to recruit permanent telecommuters and 16% of companies exclusively recruit telecommuters.

(*Bump 2020*).

- WORKFORCE ENGAGED IN TELECOMMUTING
    - 18% of executives telecommute more than being on companies premises.
    - 30% of respondents work for a fully remote company.
    - 35% of telecommuters are individuals contributors.
    - At least 46% of C-suite members work remotely.
    - 55% of VPs switch to part-time remotely.
    - Approximately 75% on-premises employees have fulfilled their positions in less than a year.

(*Bump 2020*).

- TELECOMMUTING GROWTH
    - The amount of workforce who telecommute at least once weekly has risen to 400% since 2010.
    - 42% of workers with telecommuting option under their sleeves plan to continue the same lane for the next five years to come.
    - Between 2017-2018, remote work has increased by 22%.
    - If possible, 98% of office workers would opt for telecommuting at least partly for the rest of their professional lives while a tiny proportion of 2% would not (Figure 8).

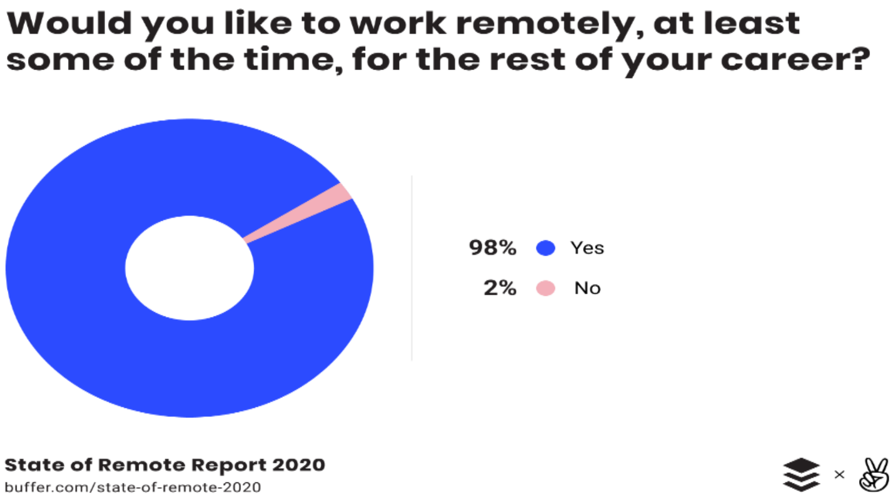


Figure 8. Remote work (Buffer & AngelList 2020)

- ➢ More than half of fulltime office-based workers long to telecommute.
- ➢ 95% of people would willingly advise their entourage into telecommuting.

(*Bump 2020*).

- Enrolment and Job Retention
  - ➢ 40% of the population agreed that a versatile working schedule would revive telecommuting.
  - ➢ The flexibility of telecommuting lays before our eyes and one cannot deny the tremendous advantages telecommuting incorporates. (Figure 9).

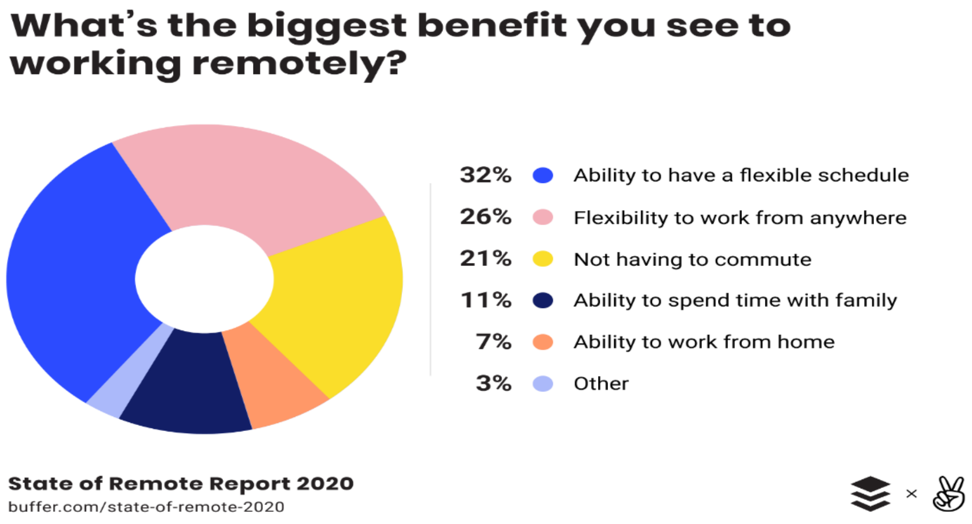


Figure 9. Benefits of remote work (Buffer & AngelList 2020)

- 72% of talents professionals concurred to the fact that work flexibility (work options included) would be a stout foundation for the future of Human Resources as well as recruiting.
- 74% of the workforce confirmed that telecommuting option would less likely made them quit their current positions.
- 81% of workers would recommend their companies to job candidates and prospect in case telecommuting is included in the working guidelines or contracts.
- 83% of employees, either remote or on-premises stated that telecommuting option would brighten up their relationship towards their occupations.

(*Bump 2020*).

- Telecommuting Productivity and Behaviours
  - 23% of telecommuters work longer hours than they would on-premises.
  - 43% of telecommuters take three weeks or less paid vacation yearly.
  - 53% of telecommuters take less time-off than they would on business premises.
  - 76% would likely avoid office premises completely when there is need to be focussed on a project.

- 77% of telecommuters affirmed that they are more productive while working within the comfort of their homes.
- Employees with high complex positions that require almost no interaction with the stakeholders happened to be more productive remotely than on-premises.
- The three main communication channels for telecommuters in priority order are email being the primary, then instant messaging and video chat.
- Even though telecommuting allows employees to decide on working locations, 84% still feels more comfortable with home working.

(*Bump 2020*).

- INCOMES AND BENEFITS FOR TELECOMMUTERS
  - 30% of telecommuters voiced out that they save at least $5,000 annually with no on-premises expenses and work-related trips.
  - Despite the improvement of telecommuting, less than 34% would accept a check cut of 5% to sign up for fulltime remote working while just 24% would go in for 10% under similar condition.
  - 69% of millennials would give away some other benefits in exchange for telecommuting.
  - 71% of organizations do not renumerate for the colleague spaces, as it sometimes happens that an employee might need a colleague resources or help to accomplish his/her tasks, hence a need to be physically present with this latter on the same premise.
  - 74% of telecommuters earn less than $100,000 yearly.
  - 75% of employees affirmed that their organizations would not renumerate for the internet while they are telecommuting.
  - Companies would save a substantial amount of $11,000 annually averagely annually per half-time remote worker.

(*Bump 2020*).

4.4 Telecommuting challenges

Despite being one of the most revolutionary digitalized modern tools that renders the workforce more dedicated, telecommuting comes with challenges as well, as already explained in previous subchapters (2.1.2, 2.2.2 and 2.3.2). Do please refer to them if needed.

Additionally, a report from Buffer State of Remote (2019, 2020) elucidates it better (Figure 10).

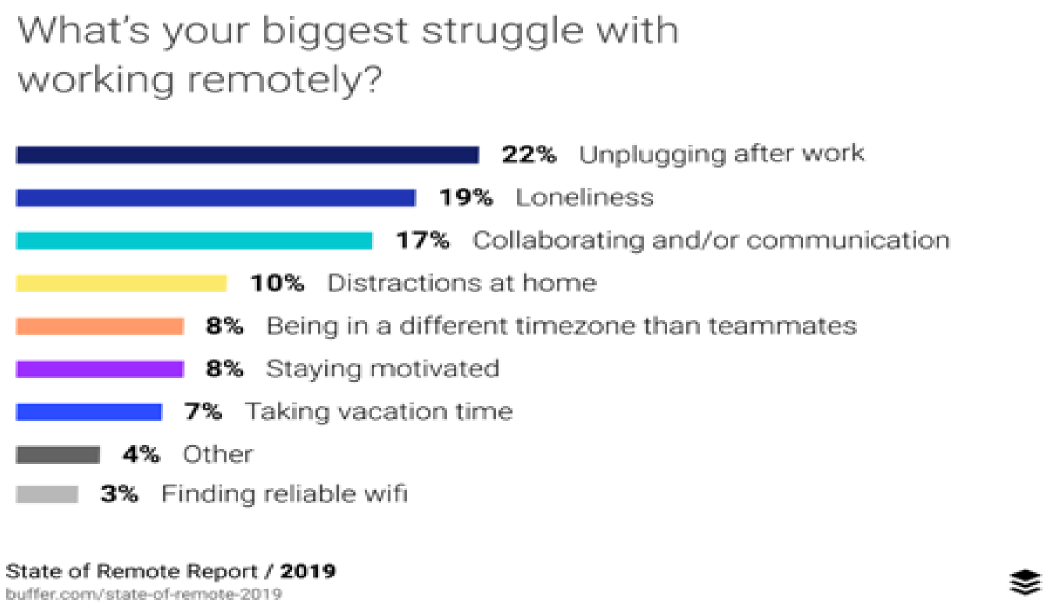


Figure 10. Telecommuting challenges (*Buffer State of Remote 2019, 2020*)

5 CORONAVIRUS (COVID-19) AND TELECOMMUTING

5.1 Impact of Covid-19: Work during lockdown

There is no denial about the fact that, the outbreak of coronavirus (COVID-19) pandemic has major impacts on every existing worldwide and the mostly affected are those either entirely new to telecommuting or not having a telecommuting solution in place or worst case scenario, do not have the satisfactory financial means to be virtually present in the marketplace.

Telecommuting being a whole integrated part of every industry, in the coming lines, we will substantiate on the impacts thrown at us by COVID-19 pandemic, as well as the new disposal that companies should put in place to run businesses safely.

5.1.1 Infrastructure

Lockdown due to its limitations, has urged on-premises organizations whether small, medium large, or gigantic to a swift forceful shift from the traditional way of working into adopting cloud services such as: Software-as-a-Service (SaaS), Cloud Computing (CC), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) IT models. It therefore becomes the responsibility of IT departments(directors) to make sure companies infrastructures such as hardware, software, applications, desktops, and datacentres are sustainable during this current crisis as well as any other that might occur in the future.

But why do we need to have such IT models in places?

- Lockdown has restricted accesses to on-premises IT infrastructure, so this would be a determining factor in case IT department needs accesses to datacentres or any type of cloud infrastructure.
- Working from home requires an increase in connectivity for workers.
- With home working being the new normal, it is required to improve the quality and securities of companies' desktop infrastructure because for a better rentability, productivity, an employee working from home should have the same feeling in terms of speed and reliability when accessing company's cloud infrastructure, applications and communication network.

Failing to adhere to all the three points listed above will result in companies financial losses as we have seen during the outbreak of Coronavirus (COVID-19).

So, giant techs companies already equipped saw a tremendous rise in their net profit. As of June 19th, 2020, the 6 major ones are:

- Amazon: $401.1 billion as world leaders ordered their populations indoors, Amazon stepped in to become the emergency for vital household goods.
- Microsoft: $269.9 billion by shifting to the cloud, enables a huge proportion of people to telecommute via *Microsoft Teams* app: a powerful communication tool with high reliability used worldwide and at the same time, *Azure Cloud* computing platform has been gaining the same notoriety as Microsoft Teams. Adding to that a record 90m players turned to Xbox Live gaming service in April.
- Apple: $219.1 billion: through resiliency online sales made possible by a dedicated network by allowing employees to being on duties as usual even remotely.
- Tesla $108.4 billion: clear technology leader for battery-powered cars.
- Tencent $93 billion: through online gaming.
- Facebook 85.7 billion via advertising business.

(*Raj 2020*).

On the other hand, some of the big companies which rely on steady flow of traffic subsequently suffered devastating losses:

- Airbus the European plane manufacturer suffered a pre-tax forfeiture of 1.2 billion euros.
- Oil and gas companies: E&P industry went $1.47 trillion down as compare to 2.47 trillion last year.
- Deutsche Bahn: 3.7billion euros losses.
- 1.4 billion euros loss was reported by the German carmaker Volkswagen during the first six months of 2020.
- French carmaker Renault: massive loss of 7.4 trillion euros.

(*Deutsche Welle 2020*).

5.1.2 Privacy and Security Risks

Once the infrastructure is set up, the next logical step is to secure this latter which consists of valuable assets (discussed earlier in subchapter 2.2.2). These assets are highly valuable data, type of information that require the highest protection within every company.

Before we move on, one thing worth noticing is: information security on-premises IT differs a huge deal from cloud IT. One major advantage on being in cloud is that your business inherits the rigid cyber security of your cloud provider. This requires an investment from companies, as such start-ups, small, medium-size companies, freelancers lacking the adequate resources end up being at the mercy of attacks since they cannot afford such expenses and not all businesses have the required personnel to achieve that level of ingenuity. For bigger companies with sophisticated IT, shifting to the cloud can usually take between half a year and a year. So, the earlier you start, the better it is while making sure the infrastructure put in place is sustainable now and, in the future as well. However, it is regrettable that many companies are not fully onboard as confirmed by IT professionals: only 41% are using the best security practices, meanwhile other 50% group of respondents admitted that there is a way for improvement (*Security magazine 2020*).

But even when your infrastructure is in the cloud, this does not mean you are away from preying eyes, it only makes it difficult for you to be a victim of any form of attacks. Securing ones data is always vital, worst case scenario is in times of crises whereby attackers hit the most companies as it has been the case during the outbreak of CoVid-19. Below are some alarming facts:

- It has been reported 4,000 cyber-attacks daily, representing 400% increase from all previous years attacks as of August 11th, 2020.
- The *entrepreneur.com* revealed in May 2020 that FBI disclosed an 800% rise in cybercrimes.
- As of May 6th, 2020, almost half (46%) of global businesses have faced at least one cyber threat. (*Techrepublic).*
- *Computerweekly* published on May 18th,2020: coronavirus may be the largest-ever global security threat.
- On 6th, May 2020 *Baracuda* stated that the upcoming month would see 49% of enterprises likely facing a breach incident due to telecommuting.

- *ZDNET* reported an increase of 238 %in cyber-attacks against bank and this directly link to CoVid-19.
- As of March 28th,2020 *thenextweb.com* cyber-attacks saw an increase of 5,000 in one day.
- April 21st, 2020, COVID-19 related scams clocked up atop 2,000 in the United Kingdom within a month, which were luckily taken down. - *BBC*
- On August 11th, 2020 MonsterCloud.com reported the ever rising and devastating ransomware attacks.
- 71% of security professionals saw a noticeable increase in cyber security attacks since the outbreak of COVID-19.

(*MonsterCloud 2020*).

5.1.3 Policy framework

The uncertainty of COVID-19's end is turning out in favour of telecommuting which is asserting its place as the number contender in terms of businesses productivity worldwide. It is therefore of a higher priority to have a business policy in place to strengthen remote work by the way of designing policies, incentives, and mechanisms. Economic and workforce should shift to support telework since teleworkers bring talent and income pay taxes hence contribute to their communities (Erard 2016*; Gallardo 2016,1*).

Factors to be considered when designing a policy framework:

- Telecommuting eligibility: lay out who "individual, teams or staffs" are eligible since not all work can be fulfilled remotely.
- Set up an approval process: once the eligibility process is established, employees should be educated on how to behest work from home entitlements, the approver, and the time of approval.
- Establish steady working schedule: telecommuting policy should clearly state the working hours of an employee.
- Provide recommendations on time management for hourly workers: ensure that hourly telecommuters should record accurately their time to their managers.
- Design attendance, availability principles and communication: since remote work does not create the old perfect atmosphere whereby workers are all onsite except under special conditions; and the use of tools such as: " Teams,

Slack, Trello, Quip, Loomio, Zoom, Skype, Tinypulse, G-chat, email " to keep an eye on whatever goes on within companies. To keep the companies in perfect symbiosis it should always be a common agreement by team members as to which tools to stick to, to lower inefficiency.

- Provide IT support at all time: technology being the basis of telecommuting, employees rely solely on it, hence it is primordial that technical teams and a defined communication channel should available at all time for employees to reach out for IT support at any given time.
- Preserve security standards: having even the best secure system is useless if employees have no ideas of the “dos” and “don’ts” when it comes to using companies resources remotely. It is thus, required of all employees to be educated about the basic functionalities of the security structure put in place.
- Preserve the working atmosphere: continuing cheering up and amenities as much as you can, will provide a sense of normalcy and continuity with workers even though professionals tasks are remotely done.
- Document acknowledgment of receipts: digital e-signature solution in the lights of PandaDoc, eSign Genie, Contractbook, Skribble, eversign, Easysend, Visma Sign or DocuSign to document workers receipts.
- Convene feedbacks and recapitulate: create ways for anonymized feedbacks from both the managers and individual contributors similarly.

5.1.4 Telecommuter’s well-being

It is vital for managers to be aware of the well-being of employees. This was easily done before COVID-19 stroke us and now with the restrictions being set in many other parts of the world, resulting in extreme isolations, loneliness, it is tougher than ever before to be abreast with your employees. So, how best an employee can be remotely managed?

Through individualized coaching, managers of telecommuting companies (especially the new employees) would have to ramp up their communication skills and get up front of the loneliness. Find appropriate, dedicated time to each employee on a regular basis.

This not only limited to employees because managers are also humans, therefore susceptible of the same issues as an employee, so the main key is for managers to be able to voice their issues which will in return encourage the employees to willingly come forward on any other issue whether work related or not.

Adding to these, companies should promote, and prioritize the wellbeing of remote workers through:

1. Set up a virtual water cooler: A virtual water cooler is way of opening the lines of communication for workers to interact with each other, by switching off completely out of the zone of loneliness, enabling them to fully connect. This can be set via tool like Slack, or Loomio.
2. The Unsick Day: An idea piloted by Buffer (*Seiter 2016*) whereby every employee is allowed, encouraged to be off duty at least a day in a year to get him/herself for check-up or preventative treatment.
3. Compensate employees for their endeavour into fitness exercises: set up a physical activity (Fitbits, gym, dance classes) for the staff but make sure to motivate them through ways like reimbursement partly or in full.

5.2 Increased in Privacy and Security risks

Telecommuting on its own poses security and privacy threats already but now with the coronavirus pandemic implications (the restrictions established by either employers or governments on employees) on our societies, the workforce is digitalized more than ever, so to maintain profit margin on the high, a complete transition to the cloud needs to be done as the attacks keep increasing day by day (numbers speak from themselves: "*refer to 4.1.2*"). Reasons for these happenings can be classified as follows:

- Easy Accessibility to previously Restricted Systems

  A huge proportion of companies always have been built up based on on-premises accessibility, eventually the shift to the cloud aka "telecommuting" is not going to be an easy task to establish, as offsite networking principles differs a great deal from the on-site structure. This is due to the lack of adequate configuration of those systems that require remote access and additional authentication (specifics passwords requirements, two or multifactor authentication) requirements that are left out of the remote work environments accessibility principles.

- LACK OF IT RESOURCES

  As we all know many companies has been set on the mortar-and-brick system, subsequently are facing difficulties as to equip the huge proportion of the workforce who had to fully transpose to the cloud in a so short amount of time. This is a serious issue since productivity is the main reason why businesses run. Consequently, in case it happens to be a delay in the acquisition of devices, the companies would have no other choice than:

  - Deployment of older generation electronical gadgets or set aside laptops or other devices to be put in use, automatically creating a huge risk of breach as these devices do not surely hold up-to-date security software as well as software security patches lacking totally the right definition files.

  - Allowing employees to use personal devices for accessing company systems and resources to get the work done. Companies most at times fail to realize that they have a restricted or to say a tiny control over the security of privately own devices of their employees, unless those gadgets have been subject of congruence (example via security applications) prior to being utilized.

- PHISHING AND MALWARE ATTACKS

  Regardless of how well prepared or security strong-wise a company is, there have always been malicious actors who leverage fake opportunities (emergency emails, health updates, software update, promotion on electronical gadgets) to create an opportunity to attack organizations. As such, unless the remote workforce environment offers more than decent security solution (firewall configurations and restricted systems access), the company ends up by paying the high price: “ransomware”.

- A RISE IN TELECOMMUTING

  COVID-19 forced the whole world into a digital world whereby we cannot fulfil our goals without digital tools, hence an unprecedent increased of remote connections. The risk of these connections is undeniably higher every second employees are accessing companies resources via an unsecure connections (e.g. working from a restaurant, a coffee shop, train station, airport, or a public opened place near your house). Those public places obviously lacking the appropriate security measures as they are being set up for public consumptions easily turn out to be the focal point for black hats.

- DATA PRIVACY THREATS

  Using personally owned gadgets offsite should always be thoughtful in addressing eventual privacy issues that may rise at any given time. Great care should be taken to ensure that:

  - The organization has accordingly issued a privacy notice or/and acquire agreement/approval.
  - Data Protection Impact Assessment (DPIA) is put in place.
  - A cross-border transfer solution available at all time.
  - The adequate terms between any vendors or third parties that might access the data.

6 TELECOMMUTING SECURITY CONCERNS OVERVIEW

6.1 Protection of Internal Systems

It is about making sure that the transition from work on-premises to offsite is safe as much as it should, while ensuring constant productivity growth.

In setting up a security plan, six key points strike the mind:

- The type of access needed
- Systems and data needed by the workers
- How sensitive are the needed systems and data?
- Are administrator privileges required?
- How about file sharing?
- What is the level of confidentiality of the data?

From a security angle, the determination factors are:

- What are the consequences in case a trespasser gains the access allocated to the telecommuter?
- What would occur if a trespasser successfully gained a hold of the employee's credentials and went above the restricted zone of that employee?

These are critical questions that need absolutely solutions for any other companies out there looking forward to an-almost unbreakable fortress.

6.1.1 Secure Gateways / Firewalls

A secure gateway or blocks or generally known as firewall monitors controls the traffic flow (incoming and outgoing network traffic) connecting two networks, usually between a private secure network and a broader unsecure network namely internet or PSNT (public switched telephone network). The danger is extreme and real on the public network as disclosed by iPass who reported that of all security incidents, 62% were directly linked to Wi-Fi and they occurred over public networks as shops, coffee shop (*Braelow 2019*). So, the crucial key implementations in telecommuting ought to be:

- ➢ Make decisions on what type of tools (software and hardware) to be available at the disposal of telecommuters using a public networks.

- ➢ To what extent the only authorized teams/staffs can have access to their corporate network.
- ➢ Ensure as well that firewall rules function efficiently as they should.

It is also possible to transfer the required resources needed by the telecommuters via a dedicated (public) database out of the secure gateway, but it is only going to work if employees need no access to organization (corporate) database.

However, the truth is that a typical telecommuter will likely require more access to provide satisfactory results. Internal resources access can be achieved through a diversity of tools as Local Area Networks applications, TCP/IP services, run the installer executable of the client software, mainframe applications. Employees to whom travelling is a priority might be restricted to emails through firewalls implementations that use email proxies to enable access to files on a well shielded system without connecting directly to that system.

Based on the need of the employees, a series of gateways can be utilized to split internals resources. For example, a router can be used to separate devices (laptop, computers, electronical gadgets) with high-risk organizational data from lowest risk systems. Furthermore, to restrict access to systems which have high-risk level statuses, a series of routers is the best solution.

In certain cases, current firewall technology (CFT) is set up to allow virtual access with proxies. Additionally, the same technology (CFT) can use IP filtering to allow access to a specific type of assets or materials.

Nevertheless, for a multitude of organizations, the number one security priority of the secure gateway is to set up a robust authentication of users.

It is worth mentioning that secure gateways also bring additional auditing and session monitoring, beholds intrusion and detections functionalities.

6.1.2 Robust Authentication

Robust authentication is a-must if internal systems and emails are to be accessed. Nonetheless, most companies undermine the strong authentication when it comes emails forgetting these latter can contain crucial businesses data.

Robust authentication increases security through:

- A token-based authentication in addition to a password or PIN
- A one-time passwords

Almost all commercialized robust authentication systems utilize smart tokens. The smart token (looks like an ATM card, a PC Card, a 3.5” diskette, a credit card, or pocket calculator) is an easy portable gadget into which a user inserts a PIN which unlocks the token to generate a one-time password. Nonetheless, there are token such as ATM cards that do not provide the one-time password, and these later are less involved into telecommuting since a hardware at the remote site is needed, and with no physical security, they are highly endangered via electronic monitoring.

The fusion of robust authentication and routing strengthen tremendously security and cost effective as it reduces the cost associated robust authentication by restricting it to workers. Telecommuters having direct access to internal systems should be required of to be authenticated through the robust authentication system and then routed via specifics computer mechanisms.

6.1.3 Port Protection Appliances (PPA)

A PPA is fitted to a communication port of a host gadget (such as computer, laptop) and allows access to the port itself usually based on a separate authentication regardless of the gadget’s own access control functionalities. A PPA may be a detached device in a communication flow or might be integrated into a communication device (example: modem). PPAs often require a distinct authenticator as password to enable the utilisation of the communication ports.

Dial-black modem, one of the well-known and most used PPAs functions on the principle by allowing the user to call it first before entering a password. The modulator-demodulator(modem) hangs up on the user and carries out a thorough search via a table to match up the given password. In case there is a pair, the modem calls back the user (to a number given prior to the beginning of the process) to commence the session. Despite it is not always the case, the return call itself is important because it protects against the use of lost or hacked accounts. The advanced functions as “*call forwarding*” may be used by malicious hackers to redirect calls.

6.2 Security Apprehensions regarding Data Transmissions

In the line of duties, the telecommuter one way or the other will be sharing a confidential data with either a co-worker or a feedback to a customer. Thoughtful process is required as to what channel to use to avoid any praying eyes that would eavesdrop on the entire session. Eavesdropping is technically easy to do if there is an access to wire or a physical cable to communicate or logical access for apparatus switching. In such process as eavesdropping the best solution is encryption. Another example of eavesdropping may be a telecommuter taking part of a macroscale conference or any other environment whereby an eavesdropper easily set up appliances with the hopes of sneaking crucial data. Some conferences provide appliances to participants for emails check-up, data transfer. This being helpful to participants as they need to provide no form of electronical devices (example laptop), nevertheless, this might easily end up being a target for an electronic eavesdropping.

So, how to combat eavesdropping?

Electronic eavesdropping can be avoided through software- or hardware-based encryption. Even though software- or hardware-based encryptions are in no way shape or form cheap (in initial and running costs) than robust authentications, they are extremely recommended when it comes to protecting confidential data that will be transferred in a high-level threat environment. However, due to the lack of training, employees fail to distinguish a high threat area from a low one.

6.3 Security concerns for Telecommuting from Home

As it has been noticed, the themes in this chapter 6, have so far evolved around safeguarding corporates internal systems and data transfer. However, as telecommuters perform their professional duties at home, it raises additional concerns.

Some of these issues have to do with telecommuters using their own electronical gadgets or the ones supplied to them by their employers/companies.

6.3.1 Integrity and Confidentiality for Home Data Storage

Working from home easily brings about a lot of mess, meaning a telecommuter working tool (computer, laptop) might be used for instance by family members who might want to buy, or do an important search on it. As such, the employee entourage through their doings on the laptop may inadvertently corrupt files, download malwares (just to name few: viruses, hybrid and exotic forms, trojans, fileless malware, worms, adware, malvertising, ransomware, spyware) or snoop. It is therefore recommended that companies take the following approaches:

- TELECOMMUTER ACCOUNTABILITY

  Some companies may decide not to set a rule that forbid employees' entourage to have access to the PCs but will still hold the worker accountable for data integrity and confidentiality, which is clearly a wrong way of dealing with such issues.

- REMOVABLE HARD DRIVE

  In case an organization data is saved onto a removable hard drive disk (HDD) or solid-state drive (SDD), the menace is considerably downsized.

- DATA ENCRYPTION

  Organizations information should be maintained encrypted on hard disk (HDD, SSD) since It shields the confidentiality of the data and exposed any modifications to any types of folder or files.

- DEDICATED USE

  This can be the perfect solution for companies to preserve their data, but we must admit that it is hard to enforce.

6.3.2 Residence Systems Accessibility

Adding to the fact that a private residence electronical gadget may be broken or looted, or worst-case scenario not compatible with organization equipment configurations. As an example, the domicile computer might not be using the same operating system as the office computer. This results in complication setup, software support, investigating or restoration, so companies ought to guarantee that their policies cover such areas as well for their own best.

As we clearly heed it, even at this stage, a lot of thoughts are put into insuring a sustainable, reliable transition.

7 CORONAVIRUS (COVID-19), TELECOMMUTING AND COMPUTER SECURITY

7.1 Covid-19, telecommuting and cybersecurity interdependency

With the increase of coronavirus patients as day goes by, it is starting to sink in more than ever that telecommuting is the “way-to-go”. This led to most organizations infrastructures being shifted to homes, public places (coffee shops, library, airport), which implies that more organizations are subjects to attacks from malicious actors in their increasing number, especially now that a huge number of less technical employees are now available online. They become easy targets for the malicious attackers, resulting in devastating consequences for organizations when sophisticated measures are not put in place to deter them from wrong doings, in other words: IT professionals have a lot on their plates.

What are then, the best, idealistic approaches can we armour ourselves with to duly conduct business, maintain productivity but at the same time avoid getting entangled into malicious actors’ web?

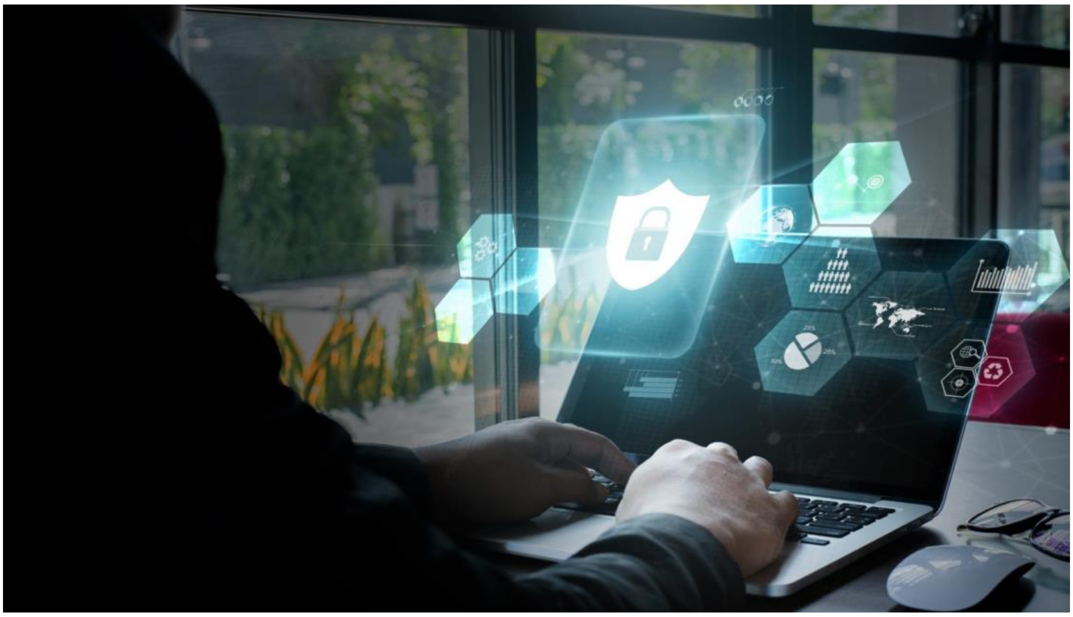


Figure 11. The threat is real (Nicky Daly 2020)

7.2 Visibility and Threat Detection in a telecommuting world

Lockdown at its summit obliged the workforce to convert their usual, traditional operating mode into a digital way, creating a class of abundant less technical people online who are at risks in every actions they take while performing duly their duties. New loops and holes unconsciously created by the non-technical employees become a duty of the security teams who with centralized security information event management (SIEM) solution will regain, increase visibility, and monitor controls. Below are four keys on which we will focus.

- EMAIL

  Email is one of the easiest way to infiltrate a corporate as 94% of malware that get to a company is delivered through phishing (*Sobers 2020*). With the expansion of non-technical employees online, attackers are getting better at crafting compelling phishing emails, malspams and ransomware, all of which have skyrocketed: a serious threats for an organization! So, to keep tabs on all incidents after a phishing electronic mail is unwrapped, security teams require a centralized view of the occurrences throughout the company.

  Accomplishing this, requires from security operations centre (SOC) teams to convey an amalgam of related electronic mail happenings and network flows to a centralized SIEM solution for scrutiny. Security analysts can, thus obtain a more adequate, effective, comprehensive view of email-based threats by absorbing and analysing electronic mail occurrences or electronic mail security occurrences via the use of tools like the ones from Cisco IronPort or Proofpoint.

  Network analytics can also be used to pull out additional characteristics such as file hash and URL, attachment name, sender email and then match up the gotten characteristics versus threat intelligence at the exact moment of occurrences to get deeper insights of the threats. Subsequently, the network-level insight can produce early visuality and alert about known threats and dubious characteristics synonyms of a phishing attack.

- ENDPOINT

  There were two types of companies before COVID-19 hit us by storms:

  - The almost entirely office-based companies (brick-and-mortar)
  - The remotely-based companies (full telecommuting)

  In the lights of the transition, office-based workforce with no prior experiences had to first figure out within the shortest amount of time how to make functional core services and application, then put those infrastructures at the disposal of the remote employees, and in some situations deploy a virtual private network (VPN) on the ever first instance. Remotely-based companies witnessed tremendous and sharp rises in virtual private network utilization, submerging networks and dramatically turned down speed, particularly obligating employees to perform their duties off VPN to keep up with prolificacy. From a security point of view, both cases set in motion an enormous blind loop (spot) for endpoint and employee activity.

Reclaiming visibility calls on for the security teams as regarding the possibility to synchronize altogether the VPN, the endpoint operating systems (OS), the endpoint detection and response (EDR) events to assist with threat detection. The fact is that Windows, MacOS and Linux logging allow security teams to have deep insights of all the events at the endpoint level. With Sysmon (windows system monitor), security teams have the possibility to even reach profound threat-relevant apprehensions like domain name system (DNS) requests and process activity.

Companies utilising EDR solution like Carbon Black or CrowdStrike, endpoint security events have the probability to be conveyed to a centralized SIEM (security information and event management) solution and matched up against other firms data for end-to-end threat visibility. Endpoint detection and response tightly integrated with a SIEM results in response action which can be initiated straight from the SIEM interface.

Additionally, whenever an employee signs in through risk-based authentication or onto VPN to access applications, not only a clear insight about the endpoint's location is provided, but the MAC address, as well as the user agent and other vital information, which can provide insights into the real identity of the user.

Upon collection of the valuable data (vital information), sequences of both machine-learning (MA) and correlation-based analysis (CBA) are applied by the security teams to detect unknown and known threats. Let' s bear in mind that it is quite helpful for a security operation team (SOT) to check out for SIEM vendors, suppliers of pre-built security use cases and analytics, thus companies do not have to devote their time and financial resources in researching and developing these from the scratch.

- APPLICATION

The main priority for security teams should be applications monitoring because unlike endpoints, companies are still in charge even while being off network and this as well helps to unmask the malicious actors who are already embedded into the network.

Application monitoring can be enforced at different levels in the network:

- At sign-on through identity as a service (IDaaS) solution such as Okta.
- From sign-on through to sign-off straight through application such as Office365 or SalesForce.com.
- Through cloud access security broker (CASB) solution, such as Zscaler, use in monitoring the user accessing or trying to access a specific type of application.
- Directly within the application stack, incorporating OS container orchestration platforms (Kubernetes) being containers themselves and application program interfaces (API) calls within these domains.

(*Horaist 2020*).

Additionally, when performing monitoring and analysing events activities at each of these levels, network monitoring can reveal a thorough insight into how the application data is going through the network, the "*who*" and "*what*" is connecting to these systems and in case an abnormality has been watched and noticed down. Through this added layer of insight, existing visibility and insight are augmented helping to expose several dubious activities faster such as compromised accounts. Furthermore, network monitoring may be especially helpful in case malicious users have gained the desired control to successfully utilise detections evasion techniques (DET) such as disabling logging. The network being a highly reliable source of truth have this ability to show when systems and applications are online even though they may be sending no logs at all and keep providing visibility into what the systems and applications are doing.

- CLOUD

With telecommuting becoming the new norm, many physical datacentres shut down temporarily, companies are faced with the eminent task to shift to the cloud to support their workloads and applications for business productivity continuity.

Security teams within these environments can monitor a range of events: user activity, application activity, resource and configuration changes. Luckily, the four giants in the cloud world: “IBM, AWS, Google Cloud and Azure” come along with a rich set of logs, events and network flows data which can be transferred into a centralized SIEM solution to obtain visibility and detection across on-sites and multicloud environments.

By incorporating this data and applying security use cases to it, analysts have the ability to gain insights into a multitude of dubious activities such as:

- Suspicious resource alterations: for instance, non-standard virtual private cloud (VPC) or Amazon Elastic Compute Cloud (EC2) instances or a swift increase in the number or size of EC2 instances highly pointing to cryptocurrency mining.
- Anomalous user and account activity: multiple logins from different geographical areas or suspicious root user’s activities, abnormal authentications.
- High-risk configuration modifications, including security policy group modifications, alterations to S3 bucket policies (resources-based Amazon Identity and Access Management (IAM) which is the only object storage that allows blocking public access to all objects) or newly or altered certifications.
- Anomalous workload activity: which comprises suspicious container activity or non-standard activities accessing resources, abnormal API calls.

As of the writing of this thesis, many cloud providers own native security capabilities, but with no centralized outlook into security data across environments. As such analysists are literally stuck as they are obliged to work within complex data silos. Here are hybrid and multi-cloud numbers broken down during *CloudHealth Connect 18’*s week in Boston last year:

- 62% of public cloud adopters utilize 2 or more public clouds platforms.
- 74% of companies portray their MO (modus operandi) as hybrid/multi-cloud.

However only:

- 37% impose expirations or capacity limits.

- 41% keep a satisfactory service catalogue.
- 42% on regular basis enhance cloud expenses.

(*Chapel 2019).*

And on average, corporate utilises a total of 4.8 separate public and private cloud environments to run applications (*Chapel 2019)*. For an analyst, this means having a hard time to keep up with the consistently growing workload, having centralized cloud visibility joined with the ability to automatically analyse, detect and track threats as they evolve through several environments is extremely critical. A centralized SIEM solution has the potential of incorporating and analysing events and data flows across cloud and on-site environments, which subsequently enable analysists to be quick and more efficient in detecting threats before they become more intense and cause serious damages.

7.3 Cybersecurity during COVID-19: Managing cybersecurity

As business proprietors, partners, chief information officers (CIOs), chief information security officers (CISOs) tussle to come to terms with the ever increasing restrictions instituted either by governments or by businesses, the challenges never cease to arise as to the risks, threats in the type of environments where companies are shifting to.

The world in which we live nowadays is no longer run by weapons, or money or energy: zero – little bits of date commonly known as electrons run our lives. The war that started with this pandemic COVID-19 is no longer about who has the most guns, or bullets or nuclear weapons, it is all about information. The one that holds the data runs the world.

As such, in the coming subchapters we talk about some of the challenges we face and how to manage to our best ability remotely-based corporates.

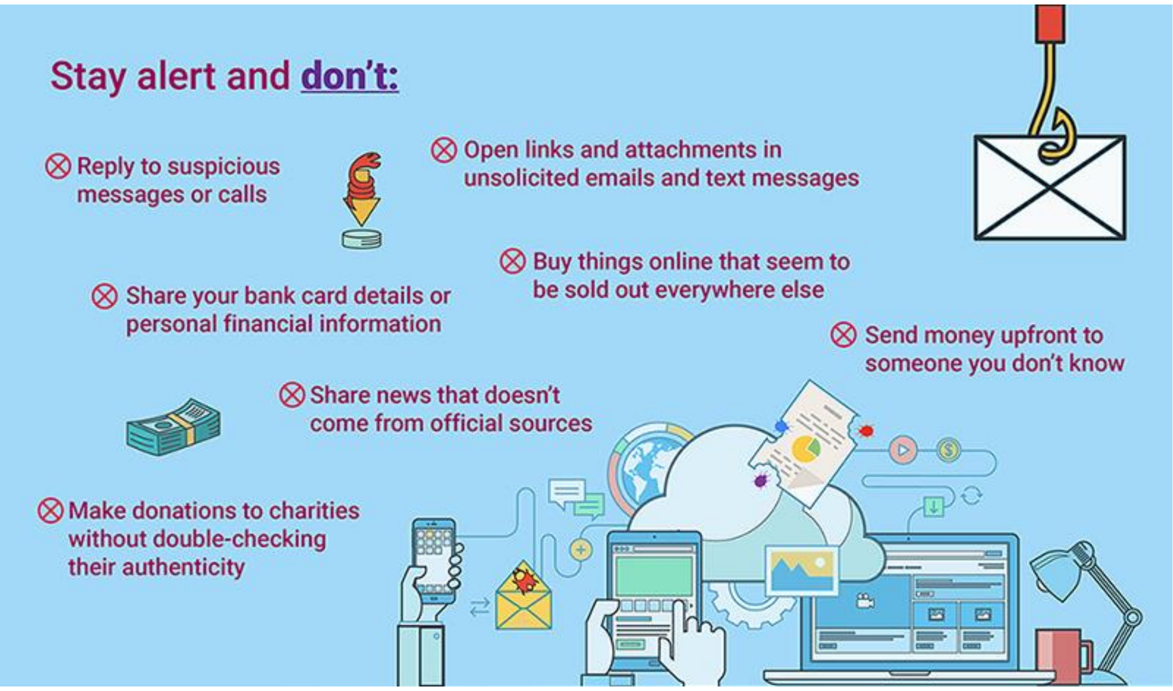
7.3.1 A challenge

With the outbreak of COVID-19 pandemic, we individuals as well as companies have become more vulnerable to malicious actors (cybercriminals) that operate in the digital realm since all electronical devices (computers, laptops, mobile devices) and internet are the new norms.

Below are some alarming facts from the Council of Europe’s cybercrime Division published on 27th March 2020:

- Phishing and malware distribution across websites which seem to be authentic or files laying out facts, documentations or guidances about COVID-19 are utilized to contaminate electronical devices and extricate users credentials.
- Disinformation is laid out in the open by trolls and worst-case fake media accounts to produce a state of fear, panic, social instability, and complete lack of trust in the leadership (government) or preventive procedures put in place by health authorities.
- Attacks against international organizations as the World Health Organization (WHO) or striking critical infrastructures.
- Ransomwares closing down scientific, medical, or any other health-related department where vaccines are being developed or where people are being tested for COVID-19 to extort ransoms.
- Ransomwares launched at electronical devices such as cell phones of people utilizing applications that pretend to bring forth bona fide information about COVID-19 conducive to extracting payments.
- Fraud schemes designed at deceived people into buying products such as hand sanitizers, masks, as well as fake drugs under the pretence that they prevent or cure SARS-Cov2.
- Black hats pushing through the organization systems and targeting remote workers.

Extreme cautious should be taken and security measures strengthened. (Figure 12)

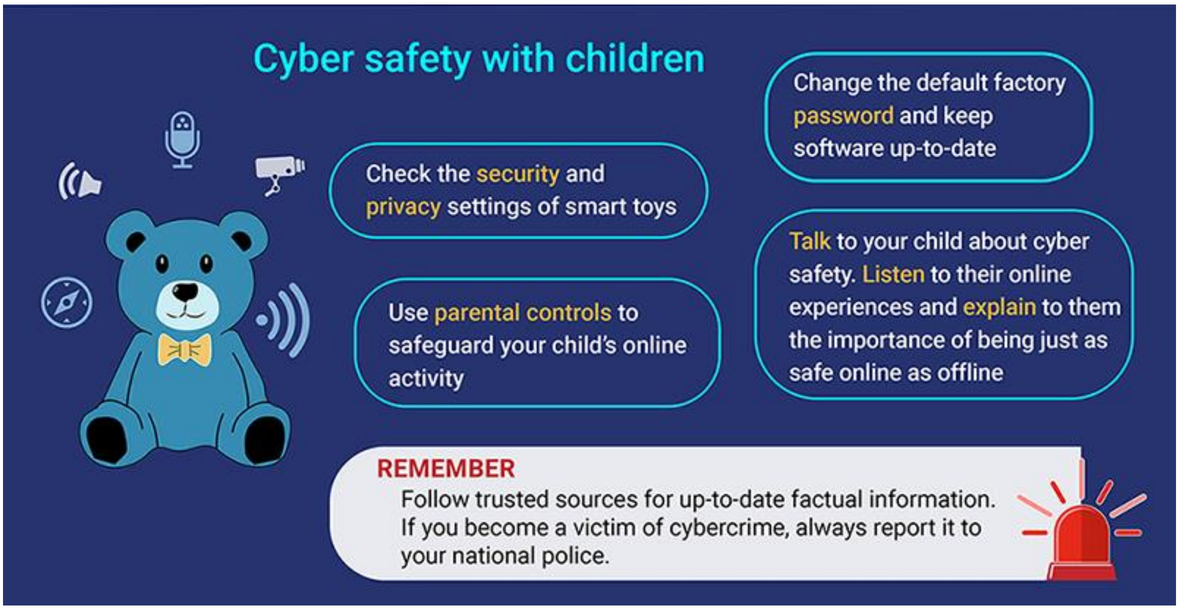


Stay alert and don't:

- Reply to suspicious messages or calls
- Open links and attachments in unsolicited emails and text messages
- Buy things online that seem to be sold out everywhere else
- Share your bank card details or personal financial information
- Send money upfront to someone you don't know
- Share news that doesn't come from official sources
- Make donations to charities without double-checking their authenticity

Figure 12. Few key precautions to put into practice (Europol 2020)

As WFH involves indirectly family members who might one way or the other come in contact with the remote worker tools (exemple: laptop), it is important to inculcate basics knowledges of online dangers to the entourage especially those who have no clue about them to raise awareness. A perfect exemple are children (figure 13) and it is vital since kid in every household in developped countries already owns a celullar phone. This will help them further as they grow up especially as entitled to live through the virtual age for the rest of their earthly lives.



Cyber safety with children

Check the security and privacy settings of smart toys

Use parental controls to safeguard your child's online activity

Change the default factory password and keep software up-to-date

Talk to your child about cyber safety. Listen to their online experiences and explain to them the importance of being just as safe online as offline

REMEMBER
Follow trusted sources for up-to-date factual information.
If you become a victim of cybercrime, always report it to your national police.

Figure 13. Cyber safety with children (Europol 2020)

7.3.2 Managing cybersecurity

In this subchapter, we will focus on six areas of high risks and security threats that are recommended to be aware of to any enterprises out there involved in telecommuting.

1. CHIEF EXECUTIVE OFFICER (CEO) FRAUD EXPLOITING SOCIAL DISTANCING

   As long as human beings have dwelt on this earth, trust has always been an issue when it comes to social interacting. Now, with the social distance in vigour, one has to be more than careful as to whoever he/she is dealing with as social engineering fraud has shifted into more emails and phone calls.

   In this type of scam, the requestor portraying him/herself as a CEO or other senior company s figure lures the receiver to transfer organization funds to other bank accounts under the assumption that an important payment has to go through. Fortunately, this can be detected since receivers probe with their colleagues to the credibility of the communications. So, it is vital to educate staffs into strictly following the company's money transfer protocols, as well as invigorating them to keep up with the incident management process and be ahead of any irregular communications.

2. INSECURE REMOTE CONNECTION TO THE OFFICE

   In crucial times as the one COVID-19 imposed on us, companies need to make sure the remote connectivity is always not just functional but secure as well. Adding to what we elaborated on in subchapter 6.1, it is always highly recommended to enforce the multi-factor authentication (MFA) process.

3. INCREASED PERSONAL USE OF ORGANIZATION DEVICES:

   Performing professional duties from home with organization devices came with new temptations to utilise organizations equipment for personal use. As discussed in subchapters 4.1 & 6.1, this creates the possibility and inflate the malware infections risk for these devices. Be cautious by updating browsers and any other related third-party software such as Flash players, PDF readers and Java.

4. FINANCIAL STRESS OF EMPLOYEES OR INSIDER THREATS THAT MAY BE DUE TO EMPLOYMENT UNCERTAINTY

   The anxiety of the uncertainty during COVID-19 pandemic can create financial concern as well as loss of current job leading employees to be exploited by competitors aware of their situation, hence persuading them into giving away company data. One efficient way to prevent this is to be transparent towards employees in every possible way and often reach out to them to keep the lines of communication opened.

5. CONFIDENTIALITY ISSUE OFF-SITE

   Your household or public place turning out to be your office means that you are no longer the sole responsible as to whatever goes on in your professional career. Being based at home is for sure better than other public whereby you have zero control of your entourage. So, while working from home, great care should be taken not to mix your professional life with your private one. (refer to subchapter 6.1 for more information).

6. PHISHING ATTEMPTS PARTICULARLY COVID-19 RELATED:

   From mid-February, the number of attacks never cease to increase daily and mostly using COVID-19 as themed spear-phishing attacks (refer to subchapter 4.1.2). These malicious actors set baits on fake websites and collect for instance Office 365 credentials.

   Some recent cases of phishing attacks have been directed towards CDC (Center for Disease Control), WHO (World Health Organization), The Gates Foundation, World Bank, NIH (National Health Institute) where 25,000 users credentials and passwords were stolen and thrown away on the dark web by unknown black hats (*Panda, 2020*), or the ransomware attacks that hit the German Hospital leading to a death of a patient on a way to hospital. (*Goodin & Technica 2020*).

   As security teams coordinate responses across all three lines of defence such as: “ risk oversight, operational management, and internal audit”, care needs to be taken to enforce the following steps which help in reducing threats, thus lowering the risks levels to both your corporate and telecommuters:

   - Educate and raise awareness about the highly existing risk of COVID-19 themed fraud and phishing attacks. Enforce the protocols already in place and motivate workers to voice out their concerns, remarks should anything looks even the slightest fishy.

- Rely on the Internal Audit function to guide you through any alterations needed to be done to adapt to changes in decision making or risk tolerance.
- Constant communication with staffs, employees and company regular updates briefing as to how the organization is dealing with the COVID-19 pandemic.
- Encryption of data-at-rest on electronical devices and an additional data loss prevention software to expose data breaches and leaks.
- Make sure that all electronical equipment provided by the company and at the disposal and usage of employees should have up to date firewall software and anti-virus.
- Provide employees with an alternative way to transfer data through secure collaboration and disable universal serial bus (USB) driver.
- Add a dedicated hotline, a portal, or a service desk menu to account for any security issues (potential fishing included).

These few strides are the steppingstones but we all must remember that technology can go so far in protecting companies vital assets. However, these changes can only become effective if only the weakest link “human” is educated enough to follow up and adapt as these changes evolve. It goes this way: *no matter how secure locks or alarms systems you set on your house, if you have an unreliable security guard or your door is most at times unlock, your security system is useless*.

7.4 Cybersecurity Takeaways

With COVID-19 hitting us at the end of year 2019, it announced year 2020 as the new era in so many ways but particularly defining ways businesses would be conducted in the future.

Remote work became the new norm, which gave a sudden and sharp rise to black hats.

7.4.1 Threats and Trends in 2020

- SOCIAL ENGINEERING

  Higher the number of employees, or people, or organizations on internet (the unsecure public web), less technical people are found since remote work is just on the verge of being used by the vast majority of people. As such, technical skills are not yet mastered hence, this is the perfect playground for hackers who would exploit the weakest link in every organization: “human psychology” to achieve their goals through phone conversations and social media outlets, tricking the mass into giving them free passes to sensitive data.

- PHISHING GETTING MORE SOPHISTICATED

  Digital messages carefully targeted to induce the populace into clicking hyperlinks which then, installed unknown to them malware or disclose sensitive data are increasingly turning out to be more advanced.

  Ironically, while the workforce at the majority of corporates are increasingly becoming conscious of the dangers of phishing attacks, malicious actors are upping the ante. For instance, hackers utilizing ML (Machine Learning) to swiftly craft and spread bogus information hoping receivers on the other end will inadvertently compromise their companies’ network and systems. These type of attacks allow non-ethical hackers to steal users credentials, logins, credit cards, and similar sorts of personal data, furthermore, ingressing straight into corporate hearts.

- RANSOMWARE APPROACHES TRANSCENDS IMAGINATION

  Ransomware attacks are approximatively cost-effective billions of dollars yearly, since malicious actors exploit technologies allowing them literally to hijack the populace or companies’ databases then cease all critical, valuable data for extortions. The ascendance of cryptocurrencies such as Bitcoin is believed in helping to propel ransomware attacks by enabling the payment incognito.

  While organizations keep focusing on strengthening their defences against ransomwares breaches, some experts have the beliefs that non-ethical hackers will more and more aim at any other potentially enriching ransomware targets like high net-worth individuals.

- CRYPTOJACKING

  Cryptojacking is an ultra-modern form of hacking whereby cyberattacks abduct a third-party residence or office electronical gadgets such as computers, laptops to "mine" for cryptocurrency. Since mining for cryptocurrency such as Bitcoin needs a massive quantity of computer processing power, malicious actors strategy for financial gain is by covertly piggybacking on another's individual systems. Which causes a serious nuisance for businesses since it leads up to performance concerns and cost downtime as security teams have to pinpoint and find a solution to the nuisance.

- CYBER-PHYSICAL ATTACK

  This modern technology which tremendously changes our lives positively, presents its risks as well. The constant threats of hackers aiming at electrical grids, water treatment departments, transportation systems, represent a crucial vulnerability moving onwards. The New York Times reported two years ago: even *America's multibillion-dollar military systems are at risk* of high-tech foul play (*Navarro 2018*).

- STATE-SPONSORED ATTACK

  Gone are the days whereby hackers focus was only personal or organization data for ransom, it has now levelled up to nations utilizing their high-tech prowesses into infiltrating governments and carry out coups against governments critical infrastructures. As we can see, cybercrime nowadays is no longer just a threat directed at an individual or the companies, but it has risen to governments, states, and nations' level. It came to no surprise as we are witnessing the sudden and sharp rise of cyber criminality during this year of 2020 (refer to subchapter 4.1.2). This is further confirmed by Thomson Reuters Labs: "*State-sponsored cyberattacks are emerging and significant risk to private enterprise that will increasingly challenge those sectors of the business world that provide convenient targets for settling geopolitical grievances*" *(Ulicny 2019*).

- INTERNET OF THINGS (IOT) ATTACK

  Based on Statista's report: *the number of devices : "laptops, tablets, webcams, home security systems, routers, manufacturing equipment, household appliances, smart watches, medical devices, automobile" connected to the Internet of Things is on the verge to hit 75 billion by 2025*, (*Ana, Bera*) which shows how ubiquitous IoT is becoming.

All these devices play essentials roles in private sectors, as well as individual homes who use them to gather huge amount of data, critical for businesses success. However, these same devices are source of huge risks since once hackers get ahold of them, these devices are easily controlled, hence may be utilized to bring about havoc, shut off vital equipment or overload networks for monetary benefits.

- Smart Medical Appliances and Electronic Medical Record Software (emrs)

As technology evolves, so does healthcare industry making huge steps to adapt to digital world, meaning a lot of equipment are digitalized. Good in a sense that it enhances efficiency in performing medical tasks but on the other hand, should one of these devices happened to fall into the wrong hands, the consequence can be disastrous. Already the medical records are almost completely online, and as such those data turn out to be the major target for evils doers due to highly sensitive contents they incorporate. Another example is a device directly connected to a patient to be handled remotely, an attacker could concretely decrease or increase dosages, disable a vital monitoring signal, or send electrical shocks to the patient.

A recent example that happened in September 2020, is an attack of a German Woman who died from delayed treatment at the University Hospital Düsseldorf after malicious actors proceeded on 30 servers with a ransomware attack (7.3.2). This attack has been successful via a hole in Citrix Software which was patched non long ago but has not been updated.

- Third Parties (Vendors, Contractors, Partners)

Vendors and Contractors are sources of huge concerns to organizations because most of them do not provide secure systems, neither dedicated teams on the spot to supervise third-party workers.

RiskManagementMonitor published a report on “Security Risks of Third-Party Vendor Relationships” which comprises a graphic information estimation of 60% of data breaches that includes a third-party while just 52% includes corporates set of security standards related to third-party contractors as well as vendors. (*Sobers 2020*).

- Connected Cars and Semi-Autonomous Vehicles

While the driverless automobile is yet to hit the market, the connected car has made it long ago. Through embedded, tethered, or smart phone integration, a connected automobile uses onboard sensors to enrich its own operation and easement for passengers. As we speak now, approximatively 90% of new cars are going to be connected to the internet (*Moore 2016; 2020*), which undoubtedly will open a wide window for hackers to exploit weaknesses in secure systems (Figure 14), then rob them of sensitive data or harm drivers. So, this not only causes safety concerns but privacy as well.

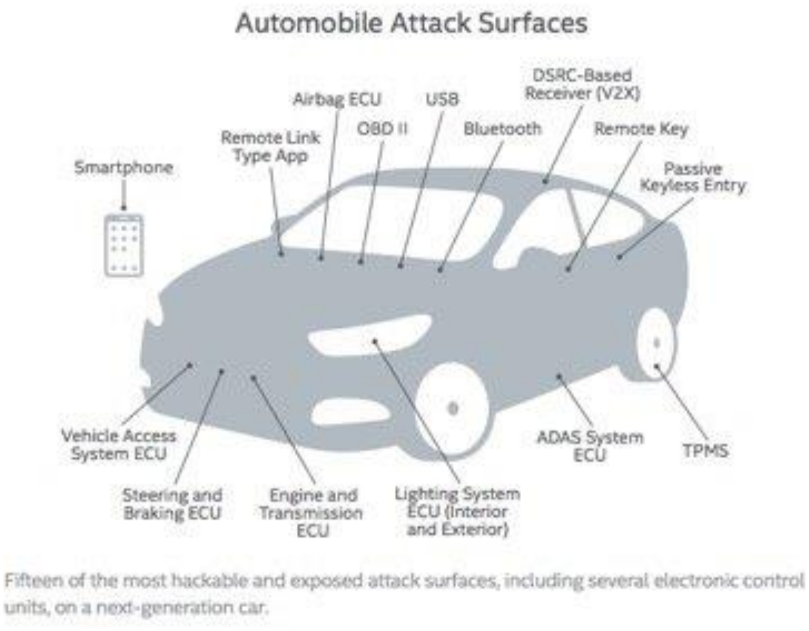

Automobile Attack Surfaces
Smartphone
Remote Link Type App
Airbag ECU
OBD II
USB
Bluetooth
DSRC-Based Receiver (V2X)
Remote Key
Passive Keyless Entry
Vehicle Access System ECU
Steering and Braking ECU
Engine and Transmission ECU
Lighting System ECU (Interior and Exterior)
ADAS System ECU
TPMS
Fifteen of the most hackable and exposed attack surfaces, including several electronic control units, on a next-generation car.

Figure 14. Vulnerable access points of automobile (Michelle Moore 2016; 2020)

- AN EXTREME SHORTAGE OF CYBERSECURITY PROFESSIONALS

The alarming figures in the subchapter 4.1.2 speak volume as to how cybercrime has quickly evolved during the outbreak of COVID-19. A lot of amateurs who are used to the brick-and-mortar business way of life, all sudden burst out online and this, on a regular basis, becoming targets for hackers. Meanwhile, there has always been a serious shortage of cybersecurity, even before COVID-19, so with this pandemic only aggravates the scarcity that was already resonating.

Luckily, the University of San Diego is now offering two master’s degree programs to particularly focus on the vital, critical, sensitive issues faced by cybersecurity professionals nowadays (*Moore 2016; 2020*). Hopefully, others will soon follow the footsteps together, so we have enough tech savvies to combat the dark forces online.

Figure 15. Scarcity of cybersecurity professionals (Haeny 2018)

7.4.2 Cybersecurity Stats for 2020

The threats, attacks come in millions and even if we dedicate our whole lives to them, we would not be done talking about them for the next 30 to 40 years to come, or even be any closer to solve them all. The worldwide damages caused by cybercrime will be hitting by 2021 the $6 trillion annually based on Cybersecurity Ventures' studies (*Freedman 2020*). So, for us to be concise and still come up with the major stats, we will focus on the few keys ones which are data violations, industry-specifics stats, hacking as well as expenditure and expenses related. We will, however put links in case anyone is interested to go deeper into it. Below are the "must-be-aware-of" when it comes to cybersecurity stats.

- THE BIG FIVE (*Cyber Observer 2019*).

  1. Spent budget worldwide on cybercrimes is heading towards $133.7 billion by 2020 (*Moore & Keen 2020*).
  2. Data breaches uncover 4.1billion records in the first half of 2019. (*RiskBased Security 2019)*)
  3. Out of 52% of data breaches hacking-related: 28% are malwares, 32-33% involved phishing or social engineering correspondingly. (*Verizon 2020*).
  4. 68% business executives feel their cybersecurity defences are not strong enough.
  5. 71% of breaches were financially related and 25% were related to espionage (*Verizon 2020).*

- LARGEST DATA BREACHES STATISTICS

Some companies had data breaches during year 2019, which impacted negatively on their credibility, reputations being at stake, thus putting at risk their partners and customers relationship. It is therefore important that we fully understand the common causes related to data violations.

7 Most Frequent Sources of Data Breaches: (*Cyber Observer 2019)*

- Social Engineering
- Insider Threats
- Back Doors, Application Vulnerabilities
- Improper Configuration
- Malware
- Weak and Stolen login, credentials
- Too many permissions

Data breaches break in the open hypersensitive information that usually put users, customers, partners vulnerable to identity thefts, destroy organizations notorieties and leave the corporate subject to compliance breaches.

6. Hackers attack every 39 seconds, meaning an average of 2,244 times daily. (*Cukier 2020*)
7. In 2019, data breach costs averagely $3.92 million. (*Ponemon 2019*). The year 2020 cybersecurity reports are going to be well over that amount.
8. Security breaches have 11% in rise since 2018 and 67% since 2014. (*Ponemon Institue*). Wait yet to see what 2020 has in store for us.
9. As of 2019, it took on average 7 months to identify a security breach, a long period of time in which attackers have enough time to infiltrate companies and do as they please.
10. In 2016, Uber reported being hacked, subsequently the information of 57 million customers were at risks, forcing drivers and customers to pay them $100,000. (*Newcomer 2017*).
11. Averagely the lifecycle of a security violations extends up to 11 months (from the breach to isolation) (*International Business Machines*).

12. Equifax being hacked since 2017 is still paying off the $4 billion of ransom. *(Cyber Observer 2019).*

Diminishing a company's Cyber Risk implies developing a holistic strategy:

- ➢ Having a deep knowledge of your corporate's Status Tools.
- ➢ Having a deep knowledge of the Status of Critical Security Controls.
- ➢ Being familiar with the corporate coverage status.
- ➢ Being alert whenever there is deviation from the standard behaviour.

- CYBER CRIME BY ATTACKS

It is crucial to have a general view of the quantitative assessment surrounding cybersecurity issues as to their types as well as sources since there are lot of them and they greatly differ from one another. Most common cyberattacks are:

- ➢ Phishing
- ➢ XSS
- ➢ MiTM
- ➢ Spear-Phishing
- ➢ Drive by attacks
- ➢ Dos and DDoS
- ➢ Password attacks
- ➢ SQL Injection
- ➢ Malware attack

(*Cyber Observer 2019).*

- CYBER CRIME BY ATTACKS TYPE STATISTICS

13. 34% of data breaches were internal. (*Verizon 2020*)

14. A ransomware attack on businesses averagely costs $133,000. (*Ana Bera*)

15. Countries with the higher number of internet connected people are subject to ransomware attacks. On top of all the ransomware attacks sit United States with 18,2%. (*Symantec 2020*)

16. 69% of enterprises do not believe that the threats which are folding before their eyes can be blocked by antivirus software. (*Pomenon Institute*)
17. 92% of malware are email-related. (*Fruhlinger 2020*).

- INDUSTRY-SPECIFICS CYBERCRIME FIGURES

  Finance and Healthcare are hands down the most popular targets among black hats. Unfortunately, no one is longer safe. In addition to that, SMBs (small and midsize business) had been widely aimed at in 2019 based on the fact that they neglected to put strong security measures in place.

18. 15% of data breaches are Healthcare companies related, while 10% goes to Financial industry and 16% linked to the Public Sector. (*Verizon 2020*).
19. 43% of breaches involved small and medium businesses.
20. In 2019, Supply Chain Attack reached as close to 78%. (*Symantec 2020*)
21. The Healthcare industry had loss $25 Billion in 2019. (*Bera*)
22. In 2018, the banking industry suffered the most loss as the cost is being estimated at $18.3 million. (*Ponemon Institute*)

(*Cyber Observer 2019)*.

- SECURITY EXPENDITURES AND EXPENSES

  Cybersecurity budgets has been constantly increasing due to the awareness of companies who saw the value and importance of investing in cybersecurity. Cyber Security mid-year snapshot’19 report) reported that cybersecurity budgets have hit 60% (Cyber Observer & Rajagopal 2019) and will increase more in the year to come, year 2020 being a determining factor.

23. Heading towards the ending of year 2020, security services are looking forward to going as high as 50% of cybersecurity budgets. (*Gartner 2018*)
24. Expenses data breach related is as high as $3.9 million. (*International Business Machines*).
25. $5.9 million is the cost of the most expensive component of a cyber-attack. (Bissel 2020).
26. A malware attack costs an average of $2.6 million on an organization. (*Bissel* & *Lasalle 2019*).

27. 50 days is the average cost in time for a malware attack. (*Bissel 2020*).
28. 50% of big organizations (with at least 10.000 employees) are spending $1 million or more per year on security related issues, with 43% spending $250,00. (*Cyber Observer 2019*).
29. The cost of business globally involves turnover of customers, their increased acquisition activities, loss of reputation and reduced goodwill, was at its pick for US corporates averagely $413 million per corporate. (*Ponemon Institute*).

Even though it is really challenging to build a strong security defence for business continuity, since the future is still uncertain as threats with coronavirus pandemic on the rise while malicious actors become more and more sophisticated, it is still worth to put an effort into building a strong foundation for your company to avoid being an easy target.

8 TELECOMMUTING BEST PRACTICES

Throughout this report, we have never ceased to emphasize that COVID-19 pushed us into a new era of efficiency through the use of varieties of technical tools we have at our disposal. The rebirth of telecommuting made us see life through new horizons, but for us to perfectly adapt to this new way of life and make the best out of it as individual as well as companies, enterprises; there are some vitals indispensable organs that need to be laid down as foundations for every telecommuting structures aspiring to success and most essentially in the worst possible situation, meaning no matter what type of crisis or economic hardship might resurface in the future.

Perpetuating the team's dynamics and superintending the team experience is iffy. In the coming lines, we will elaborate on Robert Bolton (2020), one of Klynveld Peat Marwick Goerdeler's (KPMG) expert key points meticulously to make sure motivation, productivity, and security during telecommuting remain stout as they should be.

- PERSONNEL INFORMATION
    - Utilizing a stipulatory cooperation site to gather data such as:
        - Customer identification information (cellular phones and email addresses if relevant and germane).
        - Details of time off, holidays and any other important happenings on an internal team calendar.
    - Being active in communicating with teams/supervisors in case there is a change in the schedule.
    - Updating of email signature to incorporate cellular phones numbers and photos.
- LOGISTICS AND TECHNOLOGY
    - Always get the adequate hardware to sustain remote work and ensure its acceptance from the leader/supervisor.
    - Make sure there is access and comprehension of the tools used to maintain team symbiosis (Instant messages, conference bridge).
    - Engage into modifications of any non-virtual training items since all training have to shift into virtual mode at least for some period.

    - ➢ Regular update of meeting invites along with the collaboration software tools for remote teams ensuring proper functionalities prior to start of meetings.
    - ➢ Time-zone differences and businesses hours should be respected at all time.
    - ➢ Ensure the at-home internet connection works perfectly, but in case there is a flaw, look for a substitute (ratified public environment with secure wireless network, hotspot).

- Email
    - ➢ Be extra driven, concise, and meticulous in your emails.
    - ➢ Emails acknowledgement upon reception, stipulate an approach relative to resolution time, and be on point as it should be.
    - ➢ Have a discerning ability as to how productive an email will be or not (complicated, delicate subjects).
    - ➢ If you are short of ideas regarding a specific issue, do refer to individuals or the appropriate team members with their particularities (contact details).
- Phone
    - ➢ Be rapid in answering to clients calls, and text messages.
    - ➢ Whenever required, update voicemail message.
    - ➢ Supervise and superintend background tumults.
    - ➢ Cellular should always be charged, an extra charger along wherever you are during working hours.
    - ➢ Agreed on a mode of communication with teams and clients whether it should via calls or text.
- Instant Message
    - ➢ Messages acknowledgment upon receptions.
    - ➢ Always be available on IM (Instant Messaging).
    - ➢ Remember always to accustom your status in accordance to your activity at any given time. As examples:

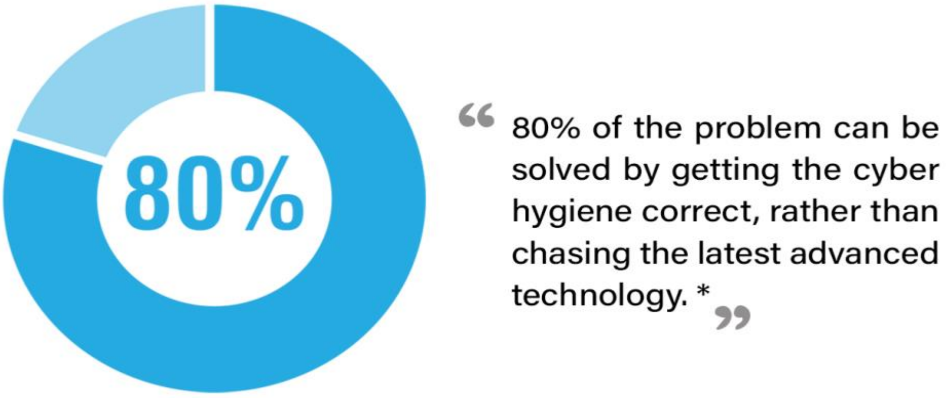
        - Set status to “Busy” while engaged with a customer
        - Set status to “Do not disturb” while in meeting
        - Set status to “Be right back” during a coffee break or a quick errand
        - Set status to “Away” while on lunch break
        - Set status to “Available” when you have nothing going

- Clientele Interactions
    - Always be on time to meetings, best is to be there at least 10 minutes before the meetings. This shows a lot of professionalism.
    - Utilise techniques like round-robin to prevent rattling over one another.
    - Set a buffer of 5-10 minutes in-between meetings to prevent participators of the upcoming meetings from getting started before the current one is done.
    - The purpose of the meeting must be clear to all participants, each ones should be aware of their respective roles, and their contributions to the success of the meeting.
    - Care should be taken to roll-call and ascertain the identities of all attendees.
    - Every little details regarding the meeting should be planned in advanced to avoid any disruptions such as a file not loading, or screen not being able to be shared.
- Internal Team Interactions
    - As in every enterprises, communication is one the major keys that ascertain productivity, such it is in telecommuting as well, but telecommuting takes it another whole level by emphasizing it more than the traditional brick-and-mortar infrastructure since physical contact is almost non-existent.
    - With teams, evaluate the approval process and governance to alleviate all potentials threats.
    - Keep tabs on daily activities for accountabilities purposes.

  - Enforce video conferencing facility to have an eye on team members doings, however the format should be unanimously acceptable.
  - Empathy is also a determinator in this equation as colleagues physical as well as mental wellbeing play a huge role in a corporate productivity. As such there should a regular one-on-one touch with each of the employees.

- Efficacity
  - Make sure to dress decently and bear in minds your environments while receiving videocalls.
  - Schedule your standard working hours as it was in the traditional mortar-and-brick system and ensure your working environment is subject to comfortability and conveniency.
  - Files should always be sent in pdf formats prior to calls not only so they can be read on cellular phones but cannot be modified.
  - Comprehend fellows employees restraints, such as having distraction like babysitting, a plumber coming in for repair, caring for pets. Such things should be known in advance.
  - Enforce daily checkpoints with employees, part-time should be set separately outside working hours to catch up with fellow employees, teams.

In a nutshell, by putting all the above recommendations into practices, you can be assured of one thing: you will be a low risk target for black hats or any other malicious actors that can be found online. (Figure 16).



“80% of the problem can be solved by getting the cyber hygiene correct, rather than chasing the latest advanced technology. *”

Figure 16. Low-key target with the right practices enforced (Cyber Observer 2019)

9 CONCLUSION

As COVID-19 pandemic forced us into adopting a new way of living, telecommuting fully became embedded into us as a double-edged-sword. Depending on your modus operandi (MO), telecommuting either makes life easier in so many ways as we have seen all along this thesis or it destroys you if care is not taken as how you handle this new normalcy in your mundane.

Just like in our everyday life, we are surrounded by good and bad people, such environment telecommuting is throwing at us. The only difference is that in the real world the probability to identify wrong, evil-doers and stop them is fairly easy as compare to the digital world where our chances is zero to none. As in our traditional, urban society whereby there is a this dire need to build a better world for ourselves and for future generation, similarly it goes in the virtual world. However, this cannot be achieved by living in uncertainty or be totally ignorant as to what digital world presents as danger. One undeniable fact is we are at a stage whereby remote work is here to stay, so the number of individuals having the use to the public unsecure web: internet, is going to increase as days go by. As such questions we should now ask ourselves are:

- How aware are we about the risks, dangers of the tools we use online?
- Up to what level do we think our lives are safe with our electronical gadgets?
- Is our wellbeing a priority number one for us as our lives are all over the internet, living behind traces that can be tracked back to us?

Once we find solutions to these questions which require an thorough training to gain the basics of cybersecurity realms, we are then one step ahead of the hackers, which does not mean though that we are completely safe, but making it harder for them from reaching us, and build on from there to ascertain a new norm in the most secure manner.

The potential of telecommuting is undeniably positively huge, thus with adequate attention to security details and mostly training users, employees about all the concepts related to cybersecurity, we will for sure reach a state where even the common individual will feel safe online.

REFERENCES

Ahrendt, Daphne., Cabrita, Jorge., Clerici, Eleonora., Hurley, John., Leončikas, Tadas., Mascherini, Massimiliano., Riso, Sara. & Sándor, Eszter. 2020. *Living, Working and COVID*. First Publication: 28.09.2020; Updated 06.11.2020. Available https://www.eurofound.europa.eu/publications/report/2020/living-working-and-covid-19

Alarice, Rajagopal. 2019. *Cyber Security mid-year snapshot'19 report*, 22.06.2019. Available https://www.cshub.com/security-strategy/reports/cyber-security-mid-year-snapshot-2019

Alex, Braelow. 2019. *Visibility is Key to Securing Mobile Devices and Networks*, 01.09.2019. Available https://www.ipass.com/blog/visibility-is-key-to-securing-mobile-devices-and-networks/

Ana, Bera. *Ransomware Statistics*. Available https://safeatlast.co/blog/ransomware-statistics/

Aristotle The Stagirite*. Politics*, 350 B.C.E. Available https://www.goodreads.com/quotes/183896-man-is-by-nature-a-social-animal-an-individual-who

Barry, D. Moore. 2020. *26 Proven Advantages of Telecommuting For Employers*, 19.08.2020. Available https://www.greatworklife.com/proven-advantages-telecommuting-employers/

Barry, D. Moore. 2018. *26 Proven Advantages of Telecommuting For Employers*, 08.2018. Available https://www.greatworklife.com/proven-advantages-telecommuting-employers/

Beth, Braccio, Hering. 2020. *Remote Work Statistics: Shifting Norms and Expectations*, 13.02.2020. Available https://www.flexjobs.com/blog/post/remote-work-statistics/

Brian, Ulicny. 2019. *Today's enterprises face increasing risk of state-sponsored cyberattacks*, 14.01.2019. Available https://blogs.thomsonreuters.com/answerson/state-sponsored-cyberattacks/

Buffer & AngelList 2020. *The 2020 state of Remote Work*, 02.02.2020. Available https://lp.buffer.com/state-of-remote-work-2020

Buffer., Hubstaff., Doist., Remote-How., RemoteYear., Trello., Workfrom. & WeWork Remotely. 2019*. State Of Remote Work, 2019.* Available https://buffer.com/state-of-remote-work-2019

Christo, Petrov. 2020. *21+ Freelance Statistics to know in May 2020*, 24.06.2020. Available https://spendmenot.com/blog/freelance-statistics/

Christo, Petrov. 2020. *21+ Freelance Statistics to Know in May 2020*, 2020. Available https://spendmenot.com/blog/freelance-statistics/#:~:text=1.,the%20global%20work-force%20by%202030.&text=While%20it%20is%20only%20an,and%2040%25%20of%20the%20workforce.

Cornerstone 2015. *The State of Workplace Productivity Report*, 05.06.2015. Available https://www.slideshare.net/cornerstoneondemand/productivity-report

Courtney, Seiter. 2016. *Introducing the Unsick Day*, 08.11.2016. Available https://buffer.com/resources/people-report-october-2016/

Cyber Observer 2019. *29 Must-know Cybersecurity Statistics for 2020*, 27.12.2019. Available https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/

Dan, Goodin; Ars, Technica. 2020. *A Patient Dies After a Ransomware Attack Hits a Hospital*, 19.09.2020. Available https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/#:~:text=A%20woman%20seeking%20emergency%20treatment,was%20widely%20reported%20on%20Thursday

Dave, Nevogt. 2020. *Are remote workers more productive? We've checked all the research so you don't have to*, 29.10.2020. Available https://blog.hubstaff.com/remote-workers-more-productive/

Deutsche, Welle. 2020*. Firms crippled by coronavirus report miserable Q2 results,* 30.07.2020*.* Available https://www.dw.com/en/firms-crippled-by-coronavirus-report-miserable-q2-results/a-54382947

Dragomir, Simovic. 2019. *The Ultimate List of Remote Work Statistics -2020 Edition*, 28.10.2019. Available https://www.smallbizgenius.net/by-the-numbers/remote-work-statistics/#gref

Dr. Roberto, Gallardo. 2016. Work in Place: A Telework-friendly Policy Framewrok, 10.2016. Available https://www.researchgate.net/publication/314102147_Work_in_Place_A_Telework-Friendly_Policy_Framework

Elena, Carstoiu. 2020. Remote Work Trends in 2020, 06.02.2020. Available https://www.hubgets.com/blog/remote-work-trends-in-2020/

Eric, Newcomer. 2017. *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, 21.11.2017. Available https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Eric, Schad. 2020. *7 Positive Environmental Benefits of Remote Work*, 27.10.2020. Available https://www.virtualvocations.com/blog/telecommuting-survival/8-environmental-benefits-of-remote-work/

European Commission 2020. *How usual is it to work from home?*, 24.04.2020. Available https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200424-1

Europol 2020. *Make Your Home a Cyber Safe Stronghold*, 23.10.2020. Available https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-strongholdMichael, Cukier. 2020. *Study: Hackers Attack Every 39 Seconds*, 2020. Available https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

Eurostat, LFS. Variable code: Ifsa ehomp. 2020. *Telework in the EU before and after the COVID-19: where we were, where we head to*, 2020. Available https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf

Flexjobs 2020. Daily updates. Available https://www.flexjobs.com/jobs

Gaetano, Dinardi. 2020. *Telecommuting: What It Is, How It works, and Why It Matters* ,16.04.2020. Available https://www.nextiva.com/blog/what-is-telecommuting.html

Gartner 2018. *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*, 15.08.2018. Available https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Greg, Digneo. 2019 - 2020. *6 Important Remote Work Statistics To Know in 2020*. First publication: 18.09.2019; latest update: 11.03.2020. Available https://biz30.timedoctor.com/remote-work-statistics/

Greg, Kratz. 2016-2019. The Business Case: How Work Flexibility Improves Mental and Physical Health. Article published first on 20.09.2016 and 11.04.2019 being the latest update. Available https://www.workflexibility.org/business-case-work-flexibility-improves-mental-physical-health/

Hailley, Griffis. 2018. Updated: Buffer & AngelList, 2020. *The State of Remote Work 2018 Report: What It’s Like to be a Remote Worker in 2018. The 2020 State of Remote Work*, 27.02.2018. Available https://buffer.com/resources/state-remote-work-2018/ . https://lp.buffer.com/state-of-remote-work-2020

Iva, Marinova. 2020. *28 Need-To-Know Remote Work Statistics Of 2020*, 24.09.2020. Available https://review42.com/remote-work-statistics/

Jay, Chapel. 2019. Multi-Cloud, Hybrid Cloud, and Cloud Spend-Statistics on Cloud Computing, 20.03.2019. Available https://jaychapel.medium.com/multi-cloud-hybrid-cloud-and-cloud-spend-statistics-on-cloud-computing-ba4c194d2e10

Josh, Fruhlinger. 2020*. Top Cybersecurity facts, figures and statistics for 2020,* 09.03.2020*.* Available https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Kelly, Bissel. 2020. *Make every part of your business more resilient*, 2020. Available https://www.accenture.com/us-en/services/security-index?src=SOMS#block-insights-and-innovation

Kelly, Bissel. & Ryan, M. Lasalle, 2019. *Ninth Annual Cost of cybercrime Study*, 06.03.2019. Available https://www.accenture.com/us-en/insights/security/cost-cybercrime-study?src=SOMS

Lauren, Horaist. 2020. *Visibility and Threat Detection in a Remote Working World,* 24.06.2020. Available https://securityintelligence.com/posts/visibility-threat-detection-remote-work/

Larry, Ponemon. 2019. *What's New in the 2019 Cost of Data Breach Report*, 23.07.2019. Available https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

Leslie, Haeny. 2018. *Marriott-Hack: Daten von 500 Millionen Hotelgästen gestohlen*, 03.12.2018. Available https://www.it-markt.ch/news/2018-12-03/marriott-hack-daten-von-500-millionen-hotelgaesten-gestohlen

Linn, F. Freedman. 2020. *Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion*, 27.11.2020. Available https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion

Macy, Bayern. 2019. *Why remote work has grown by 159% since 2005*, 30.06.2019. Available https://www.techrepublic.com/article/why-remote-work-has-grown-by-159-since-2005/

Maddie, Shepherd. 2020. *28 Surprising Working From Home Statistics*, 7.4.2020. Available https://www.fundera.com/resources/working-from-home-statistics ; https://www.fundera.com/resources/working-from-home-statistics#:~:text=Working%20from%20home%20statistics%20suggest,rates%20fall%20by%20over%2050%25

Melissa, Eddy. &Nicole, Perlroth. 2020. *Cyber Attack Suspected in German Woman's Death*, 18.09.2020. Available https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

Michelle, Moore. 2016; 2020. *Top Cybersecurity Threats in 2020*, 13.09.2016; 01.20.2020. Available https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

MonsterCloud 2020. *Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic*, 11.08.2020. Available https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html

Moonlyte 2020. *Employees Retention Strategies that Work: Bringing remote workers on board*, 13.11.2020. Available https://www.moonlyte.com/blog/26/Employee-Retention-Strategies-that-Work-Bringing-remote-workers-on-board

Nicky, Daly. 2020. *7 Tips for Avoiding Remote Work Security Risks*, 06.04.2020. Available https://www.wrike.com/blog/tips-avoid-remote-work-security-risks/

Owllabs 2020. *Remote Work 2019*, 09.2019. Available https://www.owllabs.com/state-of-remote-work/2019

Pamela, Bump. *40 Remote Work Stats to Know in 2020*. First publication: 12.03.2020; Updated 27.05.2020. Available https://blog.hubspot.com/marketing/remote-work-stats

Panda 2020. *Did hackers steal credentials of 25,000 members of WHO, NIH and CDC?*, 30.04.2020. Available https://www.pandasecurity.com/en/mediacenter/mobile-news/hackers-credential-who-nih-cdc/

Peter, Navarro. 2018. *America's Military-Industrial Base Is at Risk*, 04.10.2018. Available https://www.nytimes.com/2018/10/04/opinion/america-military-industrial-base.html

Pritish, Raj. 2020. *Amazon Is The Most Prosperous Company During Pandemic: Financial Times*, 2020. Available https://www.nextbigbrand.in/amazon-is-the-most-prosperous-company-during-pandemic-financial-times/

PRNewswire 2018. *The End of the Traditional 9-5? IWG New Study Finds70 Per Cent of Us Skip the Office to Work Elsewhere*, 2018. Available https://www.prnewswire.com/news-releases/the-end-of-the-traditional-9-5-iwg-new-study-finds-70-per-cent-of-us-skip-the-office-to-work-elsewhere-684048561.html

Remote.co 2020. *Grow remotely*, (daily website updates). Available https://remote.co/remote-jobs/

Remoters 2020*. Remote Work Trends for 2020: The Present & Future of Remote Work [updated]*, 13.06.2020. https://remoters.net/remote-work-trends-future-insights/

RiskeBased Security 2019. *2019 on track to being the "worst year on record" for breach activity, 2019*. Available https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Rob, Sobers. 2020. *110 Must-Know Cybersecurity Statistics for 2020*, 10.06.2020. Available https://www.varonis.com/blog/cybersecurity-statistics/

Robert, Bolton. 2020. *Leading practices for remote working*, 27.03.2020. Available https://home.kpmg/xx/en/home/insights/2020/03/leading-practices-for-remote-working.html

Rosaling, Mays. 2019*. The Three Types of Telecommuter,* 2019. Available https://www.stretcher.com/stories/01/010205j.cfm

Santo, Milasi., Ignacio, González-Vásquez. & Enrique, Fernández-Maciás. 2020. *Science For Policy Briefs*, 2020. Available https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf

Security Magazine 2020. *Cybersecurity Pros are Being Reassigned to IT During COVID-19 Pandemic*, 29.04.2020. Available https://www.securitymagazine.com/articles/92255-cybersecurity-pros-are-being-reassigned-to-it-during-covid-19-pandemic

Singularityhub 2012. Telecommute-option-chart, 21.02.2012. Available https://singularityhub.com/2012/02/21/u-s-being-left-in-the-dust-of-the-global-telecommuting-revolution/telecommute-option-chart/

Susan, Moore. & Emma, Keen. 2020. *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*, 14.08.2018, Available https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Symantec 2020. *Symantec Security Center*, 2020. Available https://www.broadcom.com/support/security-center

Tamara, E. Holmes. 2019. *Nearly One-Third of Workers Have Quit Due to Non-Flexible Work Options*, 14.08.2019. Available https://www.valuepenguin.com/news/nearly-one-third-workers-quit-due-to-non-flexible-work-options

Tom, Pinchen. 2019. *10 Remote Work Statistics to Know in 2020*, 29.12.2019. Available https://justremote.co/articles/10-remote-work-statistics-to-know-in-2020#:~:text=82%25%20of%20Remote%20Workers%20Have%20Less%20Stress&text=In%20fact%2C%2044%20percent%20of,over%20the%20last%20five%20years.&text=Eighty-two%20percent%20of%20people,work%20in%20a%20traditional%20setting

Twinstate 2020. *Managing a remote team: 6 tips and solutions,* 25.06.2020. Available https://blog.twinstate.com/byod-to-uc-6-mobile-workforce-management-tips-and-solutions#:~:text=Studies%20repeatedly%20show%20workers%20aren,big%20changes%20in%20management%2C%20too

Verizon 2020. *2020 Data Breach Investigations Report*, 2020. Available https://enterprise.verizon.com/en-gb/resources/reports/dbir/

Villanova University 2020. *Telecommuting Benefits and Drawbacks for Employers*, 25.02.2020. Available https://www.villanovau.com/resources/hr/telecommuting-benefits-drawbacks-for-employers/

Working Nomads 2020. Daily website updates. Available https://www.workingnomads.co/jobs

Wwr 2020. Daily updates. Available https://weworkremotely.com/categories/remote-sales-and-marketing-jobs

Zapier Editorial Team 2019. *The Remote Work Report by Zapier*, 13.11.2019. Available https://zapier.com/blog/remote-work-report-by-zapier/