**Cybersecurity of Remote Work:**

**The Role of Every Employee in Data Protection**

Yaroslav Bilous

Vistula University

Warsaw, Poland

May 20, 2024

**Abstract**

As remote work becomes the daily norm, the risk of cyberattacks and data breaches increases significantly. Remote work turns every employee’s home into a small working space that needs to be adequately protected. This article shows how cybersecurity responsibility is distributed both between IT and Security professionals and regular employees and examines effective data protection strategies in a remote work environment, discussing the increase in remote work due to the COVID-19 pandemic, its impact on the cybersecurity threat landscape, and the critical role employees play in mitigating these risks through proper training and adherence to security protocols. It shows the importance of organizational support in providing the necessary tools and continuous education to ensure a secure remote working environment.

*Keywords:* Cybersecurity, remote work, employee responsibility, data protection

**Introduction into remote work uprising: A need that has become a benefit**

After the pandemic has begun the percentage of people working remotely has increased significantly, especially in IT sector. The thing that firstly was a compulsory measure to prevent CoVID-19 pandemic became a part of employee’s comfort and now is counted as a good addition to what company “brings to the table”. To back this up we can look through researches on remote work state in 2018, before the pandemic started and in 2023, when the pandemic is in its lowest point, if not stopped.

Based on the Gallup’s State of the American Workplace Report only 20% work full-time remotely and 43% work remotely at least 1 day a week in 2018.[2] Another study performed globally by Owl Labs in 2018 shows that 52% work remotely at least 1 per week, and only 18% were working remote full-time back then.[1] Compared to this statistics gathered in last two years shows increase in the remote work state. Based on the surveys performed by Owl Labs, Global Workplace Analytics and others we can see that percentage of work performed remotely at home has risen from 4.7% in 2019 to 61% in 2020, 69% of US responders worked remotely during pandemic and work remotely now, 55% of remote workers spend more working hours at home than at the office.[4] Since 2009 the number of people who work remotely from home has risen by 159%.[3] Based on the research by Statista 67.75% of Technology industry employees work remotely.[5]

As per reviewed researches and reports we can see that remote work becomes more and more common among different industries, especially in Technology, Consulting and Finance. As well as being a benefit to employees allowing to cut commuting costs, increase flexibility and comfort remote work also benefits companies by increasing productivity of its’ employees. By the research of Owl Labs 67% of respondents are more productive while working at home and 55% say that on average they work more hours at home than at the office.[6] More than that, according to the report companies on average have 21% higher profitability by saving around $11,315 every year on an employee who works remotely part-time. [4]

And along with all the positive sides the remote work has there comes a lot of negative security problems that raise a lot of dangerous cyber security issues of remote workplace.

**Impact of remote work on cyber security threats landscape**

As the remote work is getting more and more popular new cyber threats are rising. New ways of compromising and getting unauthorized access to information give new challenges for cyber security specialists around the world. As per the report 75% of IT professionals consider their organizations to be more vulnerable after switching to remote work. The shocking fact is that data breaches that were involving remote work have increased by 273% in 2020. The most complicated security issue related to this is working from personal devices that has become quite popular for the remote working, and which 70% of businesses have failed to secure properly.[8]

Another huge problem is human factor that can’t be completely removed and that is present in every company. Thus, 95% of cybersecurity breaches are due to human factor that is realised in one way or another. No to blame only remote employees it should be mentioned that 80% of them do not receive cyber security training.[8] As the working place in case of remote workers is their own home it is crucial to educate employees on matters of cyber security threats, because they are the only one that will be protecting their workplace. Despite the best efforts of cyber security staff their employees’ minds cannot be controlled by some IDS/IPS solutions, that are usually installed on company’s laptops, so it is important to give obligatory cyber security training to every employee in general and remote employees in particular.

Continuing on the types of security risks for “Work From Home” (WFH) there are several new factors that were not part of the on-site security policies, as well as some old factors that are just more concerning for the remote working environment. Based on the article of Fortinet regarding the impact of hybrid workforce on cybersecurity unsecured networks and devices are the main reason of WFH being more dangerous in means of cybersecurity.[7] Another research by Gitnux shows that 50% of remote employees use public Wi-Fi that can be accessed and monitored by anyone, so the problem of using unprotected networks and devices is quite common.[9] Fortinet article emphasizes 5 main types of cybersecurity threats: Ransomware, Weak Passwords, File Sharing, Unsecure Wi-Fi, Personal devices.[7] Most of these types were present before the pandemic, but personal devices risk is the new one, the one that appeared to be common only after pandemic started and employees needed to start using personal devices for work. The main problem with these devices is that these devices usually “do not have the same level of cybersecurity as a corporate computer or laptop”.[7] And despite the fact that companies try to enforce security policies to raise level of protection for personal devices it’s still the risk that can be realised to perform data breach.

There is a lot of other numbers and statistics that shows how the cyber threats landscape has changed and grown after the pandemic began, all of which show sharp increases in the number and types of attacks that are launched against the remote workers and companies. However, more important question is how to protect the data and system in reality of WFH environment.

**WFH risks mitigation methods**

As always it is in cybersecurity, after hackers identify new methods to breach the systems and perform their malicious actions, security specialists design and implement new measures to prevent hackers from harming the systems. And as remote work problems continued to show up new risk mitigation methods were found and are being implemented in most of the companies nowadays. The fundamental thing that is true both for WFH and on-site work is proper implementation of basic security controls.[10] Organizations should provide employees with the necessary tools, such as VPNs, two-factor authentication systems, and anti-virus software, to make work from home secure. The best solution, which is in line with international practices, is to provide employees with company’s laptops with the tools and security policies of the organization implemented. This way, employees will use work devices that can be maximally protected and controlled by the organization and reduce the impact of the human factor and the home workplace on security.

Another important step is to create and put into practice cyber security training for employees, especially remote employees. This training should be regularly conducted to familiarize employees with current threats and teach them the basics of data protection, and familiarize employees with the basics of countering social engineering and cyber hygiene. As per Metomic article, “annual security awareness training isn’t enough to give employees a good idea of what they should be doing to secure their sensitive data”.[11] There should be continuous regular trainings, real-time practical examples, phishing trainings etc.

Also, as the main part of work in WFH is performed over the network all possible network security controls should be strengthened.[10] The more common practice is to implement zero-trust framework, the main goal of which is to ensure that the user has all the necessary permissions to access specific data, tool, system, network etc. This framework can help to minimize possible losses from potential breach, as the account that was hacked won’t have access to all the system, just to the one the user should have access to. Good addition to it would be using user behaviour analytics tools to detect suspicious activity performed by user that can help prevent intrusion from possibly compromised accounts.[10]

The last but not least is to update and strengthen the company’s security policies, instructions, procedures and data security and protection programs to ensure that all of the security related processes in the company are up-to-date, considering new threats landscape, strategies, tools and best practices.[10] As these documents and procedures designed have crucial role in implementing security measures in practice, it is very important to keep them updated and upgraded on the regular basis. Separate policies related to an employee's responsibilities at his or her home workplace should be easily accessible and understandable to every company’s employee.

**Conclusion**

As remote work becomes more and more common, cybersecurity becomes a shared responsibility of every employee. With employees working from home and creating home workspaces, each “home office” must be secured appropriately. Companies must invest in proper security measures, for example providing secure work devices, implementing comprehensive security policies, and conducting regular cybersecurity trainings. Every employee must understand their important role in protecting sensitive information and adhere to security policies implemented by company. By creating a culture of cybersecurity awareness and giving employees all the necessary tools and knowledge, companies can mitigate the risks associated with remote work and ensure a secure working environment in the modern realities.

**References**

1. Owl Labs (2018). How often do people work remote? *Global State of Remote Work*, Retrieved May 21, 2024, from <https://resources.owllabs.com/state-of-remote-work/2018>
2. Nira (2019). Remote work is on the rise. *The Remote Work Report*, Retrieved May 21, 2024, from <https://nira.com/remote-work-report/>
3. Andrei Kurtuy (2023). General Remote Work Statistics. *65 Remote Work Statistics in 2024 [You Want to Know About]*, Retrieved May 21, 2024, from <https://novoresume.com/career-blog/remote-work-statistics>
4. Tobi Agbede (2024). Key Statistics on Remote Work. *Remote Work Statistics: 50+ Key Facts to Know in 2024*, Retrieved May 21, 2024, from <https://www.notta.ai/en/blog/remote-work-statistics#:~:text=Globally%2C%2016%25%20of%20companies%20are,work%20went%20up%20by%2016%25>.
5. Statista (2024). *Percentage of employees who work fully or mostly remote worldwide in 2023, by industry*, Retrieved May 21, 2024, from <https://www.statista.com/statistics/1451594/remote-work-share-by-industry-globally/#statisticContainer>
6. Owl Labs (2021). Flexibility is essential for workplace success. *State of Remote Work*, Retrieved May 21, 2024, from <https://owllabs.com/state-of-remote-work/2021>
7. Fortinet (2020). Types of Security Risks with Work From Home. *Work from Home: Evolving Cybersecurity Risks*, Retrieved May 22, 2024, from <https://www.fortinet.com/resources/cyberglossary/work-from-home-cybersecurity-risks>
8. Jannik Lindner (2024). Highlights: The Most Important Statistics. *Remote Work Cybersecurity Statistics: Latest Data & Summary*, Retrieved May 22, 2024, from <https://wifitalents.com/statistic/remote-work-cybersecurity/>
9. Gitnux(2024). Highlights: Remote Work Cybersecurity Statistics. *Remote Work Cybersecurity Statistics [Fresh Research]*, Retrieved May 22, 2024, from <https://gitnux.org/remote-work-cybersecurity-statistics/>
10. Mary K. Pratt (2024). Cybersecurity best practices in remote work environments. *10 remote work cybersecurity risks and how to prevent them*, Retrieved May 22, 2024, from <https://www.techtarget.com/searchsecurity/tip/Remote-work-cybersecurity-12-risks-and-how-to-prevent-them>
11. Rich Vibert (2024). How can organisations ensure security is being adhered to and managed effectively? *The Data Security Risks Of Remote Working and How To Mitigate Them*, Retrieved May 22, 2024, from <https://metomic.io/resource-centre/the-challenges-of-dlp-for-remote-working-and-how-to-manage-it>