World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Check for updates

Cybersecurity and trade secret theft in remote work environments: Lessons from the COVID-19 era

Daphne Ekpe *

Intellectual Property and Technology Law, American University, Washington, DC, United States.

World Journal of Advanced Research and Reviews, 2022, 16(02), 1288–1293

Publication history: Received on 28 September 2022; revised on 25 November 2022; accepted on 28 November 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.16.2.1116

Abstract

The increase in remote work occasioned by the COVID-19 pandemic has greatly affected the protection of trade secrets and the maintenance of good cybersecurity. This means that companies that allow employees to work from distant locations are now more exposed to cyberattacks and attacks because there are many entry points. The most important weaknesses involve insufficient password security, obsolete software and insufficient shielding for endpoints.

Existing laws do not explicitly define how to protect trade secrets in remote work. The provision of the Defend Trade Secrets Act (DTSA) provides a framework for organizations to ensure reasonable security of their trade secrets. However, the nature of remote jobs will make it harder to comply with many potentially conflicting data protection laws. Addressing this new risk would require the adoption of strong data encryption, secure remote access and regulatory policies for handling data.

Keywords: Remote work; Cybersecurity; Trade secrets and theft; COVID-19; Legal issues

1. Introduction

Trade secrets are a crucial aspect of intellectual property which provide businesses with a significant edge, especially in today's competitive landscape (CRS Reports, 2014). They are often confidential and contain pieces of information ranging from proprietary formulas and algorithms to customer lists and marketing strategies that are essential for innovation, market differentiation and sustained profitability. (Norian, 2011)

Due to the pandemic, more companies started working remotely, changing the traditional office setting and introducing both advantages and obstacles for businesses worldwide. Although remote work is flexible, convenient and cheaper, it has unintentionally given cyber criminals and malicious insiders more opportunities to attack and access valuable trade secrets (Vaka, 2020). This essay suggests that working remotely has caused a rise in trade secret theft, so understanding and combating the new challenges requires strong cybersecurity practices and legal frameworks.

This essay will explore the evolving nature of trade secrets in the remote work era, examine the specific vulnerabilities arising from this new paradigm, analyze the cybersecurity weaknesses that enable trade secret theft, delve into the complex legal and compliance challenges, and finally, offer lessons learnt and best practices for mitigating these risks and safeguarding valuable intellectual property.

* Corresponding author: Daphne Ekpe.

2. Vulnerabilities and protection of trade secrets in the remote work era

Several international laws dictate trade secret protection, each of which uses a different definition of what a trade secret is and how it can or should be protected. (Martinis, Gaudino, & Respess, 2013) The Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement of the World Trade Organization (WTO) sets the standards for protecting intellectual property rights, including trade secrets. In line with TRIPS, countries are required to guarantee the effective protection of trade secrets, so different entities are expected to take reasonable steps to secure their secrets. (Durkin et al, 2021)

The Defend Trade Secrets Act (DTSA) in the United States allows companies to sue for trade secret misappropriation in federal courts, thereby providing federal-level protection. It also encourages businesses to take reasonable measures to maintain the secrecy of their information, thus prompting them to follow more rigorous data protection policies, especially in remote work settings. (Brennan 2021) The Uniform Trade Secrets Act (UTSA), which is adopted by most US states, complements this by defining what qualifies as a trade secret and setting up remedies for misappropriation. (Risch, 2007)

The EU Trade Secrets Directive ensures consistency across EU member states through the adoption of a common set of standards by each nation, under which companies are required to put appropriate measures in place to protect their confidential information. (Neethu, 2018) Canada and Australia have enacted robust trade secret legislation that addresses the unlawful acquisition of business secrets. For instance, in the case of Canada, the Commonwealth's Criminal Code was adopted. (Dafniotis, 2022)

Remote work has created a new challenge for protecting trade secrets, leading organizations to adapt their strategies. Although there are laws in place, they do not specifically focus on the risks brought by remote jobs. (Jason, 2021) As such, simply using physical security, such as barring access to documents and monitoring people on site, is not effective for protecting data when workers use many different devices from multiple locations.

Trade secret protection requires more attention from cybersecurity now more than ever. This is because the idea of an "expanded attack surface" comes with newer complications. Due to people working remotely, cybercriminals have more opportunities to attack (Atstāja, 2021). Most home networks are not as well protected as business networks and can be easily threatened. Devices that workers use for work, even under BYOD, could also be compromised and cause data breaches (Gartner, 2020). As such, workers are more at risk of being eavesdropped on, phished, or having their data intercepted because they now rely more on digital communication. Due to the peculiar circumstances surrounding remote jobs, it is now crucial to go beyond perimeter protection to strengthen security and limit data access.

The dispersed nature of an organization's remote workforce makes it more difficult to encourage a good security culture among staff. It is important to provide innovative ways of educating remote employees about trade secret protection and security practices. There must be clear communication of policies, regular security updates, and accessible resources that remote workers need to build a security-conscious mindset. Therefore, they should be taught to deal with passwords safely, protect their devices, and ensure data safely. Additionally, the absence of direct oversight reiterates the need for technical controls, which must be used to monitor and manage access to sensitive information and thus aim to achieve a balance between security and employee privacy.

3. Cybersecurity weaknesses enabling trade secret theft

Where cybersecurity is vulnerable, it offers a lot of opportunities for the theft of trade secrets from staff who work remotely. These vulnerabilities arise from the nature of remote work in the sense that the workers are not in one central office, and they rely on technology and digital communication, making them easily targeted by cyber attackers (Škiljić, 2020).

One key area of such weakness is inadequate password security. Many employees today still use predictable passwords or simply reuse ones they have used before (Yubico, 2021). As a result of this, their accounts are susceptible to credential stuffing, where hackers use their credentials to steal data on other websites. What makes things worse is the fact that many organizations may not require multi-factor authentication (MFA) for their remote workers' access to their accounts. Even where an individual has very strong passwords, but MFA is not always in place, their account may still be at risk.

Another vulnerability that can cause theft of trade secrets is outdated and unpatched software and systems. Most time, older software versions contain known security flaws which attackers can easily take advantage of (Mustafa & Abdullah, 2021). Where employees neglect to update their systems regularly, it becomes easier for hackers to target them with attacks, and this risk is amplified, especially because IT departments have less direct control over individual employee devices and software.

A major challenge also exists with endpoint security. Remote devices such as regular laptops or phones are often less secure than the security measures companies provide on their computer systems (Bonin, 2020). This consequently makes remote workers more vulnerable to different cyber threats, especially to attackers trying to access a company's network and steal trade secrets.

Additionally, data loss prevention is not always adequate in remote work scenarios (Jason, 2021). More data can be stolen as users rely more on cloud services, personal emails and file-sharing apps. Sensitive information may be exposed where a strong Data Loss Prevention (DLP) strategy is not embraced, whether employees are careless or not.

Security in the cloud is another factor that is becoming increasingly important to consider. Due to the switch of storage, collaboration and communication of organizations to the cloud, ensuring the security of these services becomes essential. Where trade secrets are not adequately protected by cloud storage due to a weak cloud configuration, they can be accessed without permission. For this reason, organizations still need to take care of their security when using cloud storage, even where they rely on a third-party company.

Moreover, the absence of direct oversight and physical monitoring makes remote work prone to cyberattacks. Since IT departments do not manage employee personal computers, network security or data directly, noticing and halting security issues requires more effort. Also, since the network is not fully visible to everyone, attackers may take advantage by accessing confidential data and taking away important information. It is therefore important to approach cybersecurity clearly, with an eye on addressing the problems unique to people using company systems outside the traditional office.

4. Legal and compliance challenges

Due to an unprecedented increase in remote work largely aided by the COVID-19 pandemic, there is a spike in new legal and compliance issues in the field of cybersecurity and trade secret protection. With the traditional perimeter gone, many people now access, process, and save important information from their various homes and on personal devices, which are often less secure. Since operations are now more dispersed, the company must adapt to the many regulations and rules in each area. Some of these unprecedented challenges will be explored in detail in the subsequent paragraphs.

One of the primary legal challenges is defining what constitutes "reasonable measures" for trade secret protection in the context of remote work (Fisher Phillips, 2022). The Defend Trade Secrets Act (DTSA) in the U.S., alongside similar laws globally, requires organizations with trade secrets to take reasonable steps to protect their valuable information. Originally, this would constitute the use of secure servers, limited access to certain office spaces and the application of clear desk policies within a physically defined workspace, etc. However, because remote jobs do not fit into these parameters (Fisher Phillips, 2022), the courts and lawyers may now have to consider a scrutiny of Virtual Private Networks (VPNs) used by employers for encryption, as well as the remote access tools to check for their adequacy when considering reasonable measures for remote work. Additionally, the use of personal devices under a BYOD policy also increases complexity since the employers are not usually in charge of the security policies on these devices.

The potential overlap and conflict of data protection laws also introduce new compliance challenges (Lueck, 2020). Remote work across different geographical locations results in the complications of guaranteeing compliance with all relevant data protection laws across diverse jurisdictions (Ribeiro 2021). Additionally, handling and prosecuting cases of trade secret theft becomes more challenging with employees working remotely from different countries, subject to different laws. For example, if a remote worker in a country with weaker intellectual property protections breaches trade secrets of an organization in the EU or California, pursuing legal action while also needing to comply with the legal requirements of GDPR or CCPA may be difficult.

The maintenance of consistent security controls and comprehensive audit trails across a dispersed workforce presents another considerable challenge. Audit logs are extremely important for tracking user activity, identifying security breaches, and showing proof to regulatory authorities (Ahmad, 2019). Reviewing and compiling audit logs becomes even more complex because employees access company files remotely. Thus, there is a need for stricter solutions and policies regulating data access, modification, login capturing at every endpoint, secure log storage, and audit retrieval.

Another potential legal challenge is the balance of employees' electronic monitoring, essential for accountability and security, with a reasonable expectation of employees' privacy (Ball et al., 2021). While employers have a legitimate interest in protecting their assets and ensuring compliance with data protection and trade secrets regulations, there is a need to balance this with employees' fundamental right to a reasonable level of privacy. Drawing a line between electronic monitoring activities that may be deemed excessively intrusive or disproportionate across various jurisdictions may present new legal challenges.

The scope of employment and what qualifies as "improper means" in trade secret theft cases where the employee is working remotely also presents another legal challenge. The distinction between what belongs to the company and what an employee knows or has learnt in the course of the job can be a fine one, especially as remote employees rely on personal devices for work. Improper means involve accessing company servers without permission, transferring confidential files to personal devices, or using company credentials for personal benefit after leaving an organization. Thus, proving "improper means" of acquisition, an essential component of trade secret theft claims under the DTSA and other statutes, becomes more difficult in the remote context.

5. Lessons learned and best practices

When dealing with defining reasonable measures for remote work, organizations should embrace robust data security that caters to the peculiarities of remote jobs (Atstāja, 2021). This may require installing secure remote access tools like VPNs with multi-factor authentication, encrypting all important information sent across the internet and on any networked device, and setting up clear procedures on data handling and proper device use (Sreekandan & Lakshmikanthan, 2020). It is also necessary to train remote workers to secure their home networks and educate them against phishing and unsafe internet practices (Sreekandan & Lakshmikanthan, 2020).

Also, organizations should ensure they are prepared globally to keep up with the different variations of data protection across different jurisdictions. They should apply the strictest data protection policies in all places where they have operations and where their staff work remotely. It may be necessary to follow GDPR-level standards across the globe as a basic rule. Ensuring good data control, providing relevant training on data protection to remote staff, and detailed procedures for working with data and international data should be top priorities.

Organizations need to promote transparency and fairness in managing employee privacy when monitoring their employees. Guidelines must clearly state what should be observed, why, how the collected data should be used and how long it should be kept. Furthermore, employees ought to thoroughly understand these policies and explicitly agree to monitoring (Ball, 2021). Electronic monitoring should also be reasonable, and where possible, organizations should choose non-intrusive ways of monitoring remote staff (Moore, 2011). Organizations can also embrace regular review of their monitoring practices from time to time to ensure they are needed and appropriate.

To avoid issues with employment scope and the use of improper methods in remote trade secret cases, companies should outline policies for using their property, working remotely with their own devices and handling private information. The policies must describe what qualifies as a trade secret and explain the different ways such information should not be obtained or shared. When an employee leaves their remote job, the organization should hold an exit interview, explaining the confidentiality rules and what can happen if trade secrets are disclosed (Pooley & Cundiff, 2021).

6. Conclusion

Cybersecurity and trade secret protection have been reshaped as a result of an increase in remote work, occasioned by the COVID-19 pandemic. Due to the peculiarity of remote jobs, traditional methods of data security have become insufficient. The use of personal devices, reliance on home networks and dependence on cloud-based storage options have expanded the base for cyber criminals to invent new risks and make certain existing risks more severe.

For this reason, organizations are faced with a more complex task. To stay secure, they must adopt unique end-to-end cybersecurity measures with strong encryption, additional verification and increased protection. Moreover, laws and their interpretations are adapting to keep up with these new changes. To address the unique challenges of working remotely, the global definition of what constitutes careful use of trade secrets must be updated and uniform. It is therefore important to approach cybersecurity breaches and trade secret theft by preparing adequately and addressing all issues thoroughly. In addition, companies should train their workers, clearly explain their security policies and remain aware of new threats.

References

[1] Ahmad, A., et al. (2019). Secure and transparent audit logs with BlockAudit. Journal of Network and Computer Applications, 145, 102406.

[2] Atstāja L, et al. (2021). Cyber Security Risks and Challenges in Remote Work Under The COVID-19 Pandemic. Proceedings of the 16th International Strategic Management Conference. 2021;2357-1330.

[3] Ball, K. et al. (2021). Electronic Monitoring and Surveillance in the Workplace. EU Science Hub.

[4] Bonin, B. (2020). Pandemic-Driven Remote Working and Risk Management Strategies. ISACA Journal. Vol. 5.

[5] Brennan, M. (2021). "Reasonable [Cybersecurity] Measures" for Digital Trade Secrets. Univ N H Law Rev. 19(3):1-25.

[6] CRS Reports (2014). The role of trade secrets in innovation policy. https://www.everycrsreport.com/reports/R41391.html

[7] Dafniotis, P. (2022). Trade secret protection and remedies in Canada. Trade Secrets. Mondaq. https://www.mondaq.com/canada/trade-secrets/1166342/trade-secret-protection-and-remedies-in-canada

[8] Dhakal, A. (2021). Rethinking Trade Secrets Under the Work-From-Home Model. NYU Journal of Intellectual Property & Entertainment Law. https://jipel.law.nyu.edu/rethinking-trade-secrets-under-the-work-from-home-model/

[9] Durkin, A. (2021). Addressing the Risks That Trade Secret Protections Pose for Health and Rights. Health and Human Rights Journal. https://www.hhrjournal.org/2021/06/16/addressing-the-risks-that-trade-secret-protections-pose-for-health-and-rights/

[10] Emenike, S. (2021). Data loss prevention in a remote work environment. DiVA portal. https://www.diva-portal.org/smash/get/diva2:1578629/FULLTEXT01.pdf

[11] Fisher Phillips, 2022. Protecting Trade Secrets in Remote and Hybrid Workplaces. Fisher Phillips. https://www.fisherphillips.com/en/news-insights/protecting-trade-secrets-remote-hybrid-workplaces.html

[12] Gartner (2020). Bring-Your-Own-Device (BYOD) risk posture. https://www.gartner.com/en/documents/3992495

[13] Jason R. et al. (2021). Remote Working Pre and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy. arXiv. 2021.

[14] Lueck, M. (2020). GDPR in the new remote-working normal. Computer Fraud & Security, 2020(8), 14–16.

[15] Martinis, L. de, Gaudino, F., & Respess III, T. S. (2013). Study on Trade Secrets and Confidential Business Information in the Internal Market. Prepared for the European Commission. Sn.

[16] Moore, D. (2011). Employee Monitoring: Evaluative Surveillance v. Privacy. SSRN Electronic Journal. http://dx.doi.org/10.2139/ssrn.1973423

[17] Mustafa, A. & Abdullah, A. (2021). Application and Software Security: Studying How to Secure Applications and Software from Vulnerabilities and Attacks. Published 2021.

[18] Natter B, Ma X. (2020). The Defend Trade Secrets Act: An Overview and Key Developments. Haug Partners. https://haugpartners.com/article/the-defend-trade-secrets-act-an-overview-and-key-developments/

[19] Neethu, R. (2018). Hush-hush in the fashion closet and EU trade secret law. J Intellect Prop Law Pract. 2018; 13(11): 896-902.

[20] Norian M. (2011). Trade Secret: Definition, Examples, Laws, Vs. Patent. Investopedia. https://www.investopedia.com/terms/t/trade-secret.asp.

[21] Pooley, J. & Cundiff, V. (2021). The Sedona Conference Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle. The Sedona Conference. https://thesedonaconference.org/sites/default/files/publications/Sedona%20WG12%20Employment%20Life%20Cycle%20%28June%202021%20publ%20comm%29_06-20-21.pdf

[22] Ribeiro, S. (2021). Remote Work and Data Protection: How do Organizations Secure Personal Data Protection Compliance from Home? https://doi.org/10.34630/bobcatsss.vi.4983

[23] Risch, M. Why Do We Have Trade Secrets? Marquette Intellectual Property Law Review. 2007; 11(1): 1-52.

[24] Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. Croat Int Relat Rev. 26 (86): 1-24.

[25] Sreekandan, N. & Lakshmikanthan, G. (2020). Beyond VPNs: Advanced Security Strategies for the Remote Work Revolution. International Journal of Multidisciplinary Research in Science, Engineering and Technology. 3(5):1283-1294

[26] Yubico. 54% of all employees reuse passwords across multiple work accounts. Help Net Security. June 10, 2021. https://www.helpnetsecurity.com/2021/06/10/employees-reuse-passwords-across-multiple-work-accounts/