ISSN: 2755-0214

Journal of Economics & Management Research

SCIENTIFIC Research and Community

Review Article

Open Access

How Did Businesses Deal with the Cybersecurity Risks and Challenges that Come with New Business Model of Remote Work, Role of a Risk Manager

Pranith Shetty

Information Security & Risk Officer, Morgan Stanley, New York, United States of America

ABSTRACT

Businesses have always been finding ways to improve , gain a competitive edge in the markets, get more customer share as compared to their peers. In trying to achieve all these objectives, they have to come up with new business models and strategies. The COVID-19 pandemic, however, forced the businesses to adapt or fail, the new operation model of remote work was the only way out for, if not all then majority businesses. As a result, these firms did thrive, more startups showed up to the competition as well, economies jumped back and quickly recovered to normalcy. While moving away from previous business strategies and models in adopting the new remote work culture invites its owns set of challenges as well as cybersecurity risks. These risks can be tackled on a use case basis based on mitigating controls and measures that security staff members come up with, however, Risk managers are very well positioned in a firm to drive a strategic risk response while communicating these risks between engineers and accountable executives. Risk management now is no longer a tool that enterprises needed to gain profits its now an essential mechanism that aids in survival of businesses, Risk managers are now more in demand than ever, these roles enable comprehensive risk reporting to senior leadership helping them understand the holistic risk posture. This article provides insight into the various aspects of remote work culture, positives and risk, furthermore talks about the role of risk managers combined with techniques or methods that can help mitigate the risk identified.

***Corresponding author**

Pranith Shetty, Information Security & Risk Officer, Morgan Stanley, New York, United States of America.

Received: February 09, 2022; **Accepted:** February 16, 2022; **Published:** February 23, 2022

Keywords: Work from Home, Remote Work, Cybersecurity, COVID, Pandemic, Risk Management

Introduction

Businesses had staff members working from home occasionally even before COVID-19 pandemic, as a result the underlying infrastructure was always there to enable their employees and ensure businesses are not impacted as a result of the pandemic, businesses were forced to have their offices closed and staff working from home [1].There was instantaneous economic recession triggered by Covid-19 shutdown, wreaking havoc on small and large businesses, offices had to be shut down to contain the spread, mandates were in effect, passed by state and national governments, the crisis nearly shutdown entire industries like the hospitality, travel industries for example. Businesses had to massively pivot to new strategies that would help them stay afloat and generate revenue in the short term [2].

All of these strategies resulted in a new form of cybersecurity threats, because if not all, majority of staff members and employees were working from home and accessing corporate networks, there was a rise in challenges and cybersecurity risks, business were targeted under the pretext of Covid-19 through phishing emails with Covid titles, home systems were targeted to gain access to corporate networks, social engineering tactics were used preying on human emotions, collaboration tools were hacked and many more avenues were attacked by cyber criminals trying to take advantage of the pandemic [3].

However, organizations did adapt and came up with defense measures against these attacks through strengthening corporate access via VPNs and advanced concepts like ZTNA (Zero Trust Networks) and SSE (Secure Service Edge) which have been described in one of the following sections. Measures and infrastructure were supplemented to enable staff to work from home with minimal disturbances and risks. An information security and risk manager has a key role to play here in this new context, Risk manager is similar to captain of a ship where ship is a reference to business, manager is responsible to ensure the business has a smooth sailing in the waters of Risk. Risk manager of a ship looks at things far away and ensures there is no to minimal impact to the business. With the increase in risks and change in risk management framework needed, Risk manager is a sought after role by businesses [4].

Rationale for Study

The study here aims at understanding the context behind work from home strategy, and the way businesses adapted to this culture to stay afloat and profitable, the new range of businesses that started thriving as a result of the pandemic. It's also interesting to understand the rise of threats impacting the new business model and how did businesses build the defense structure, pivoted from their legacy measures. What role do Information Security and risk managers play in this context and how do they ensure the risks as per the new business model are accounted for and guided through the risk management lifecycle.

Literature Review

As per this article 41% of the financial executives believe the digital shift caused by covid is permanent, digitization of services and the new framework is here to stay [1-16].

As per this article due to the pandemic, lockdown has affected the working situation of banking customers , 24% have less disposable income and 16 million customers have changed the way they bank [17].

As per this article healthcare related areas have also seen a significant rise in cyberattacks, WHO (World Health Organization) for example has reported a fivefold increase in cyberattacks in later April 2020, Ransomware, social engineering, data breaches all have seen a spike in their occurrences and these attacks span across various sectors [18].

Businesses Adapted to Remote Work and its Positives

Faced with the mandate to stay home, businesses had to figure out a way to enable their staff, who are a core driving force behind any business model, the following sections dive a little bit into the changes that enabled businesses [5].

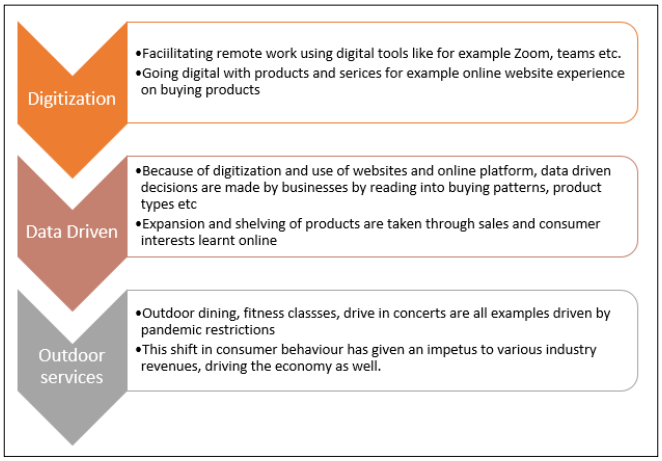


Figure 1: Changes that Enabled Businesses, during COVID Pandemic

Digitization of the industry has enabled people to work from wherever they choose to, online shopping experiences have enabled consumers and businesses, work life balance has been prioritized and work can be performed beyond boundaries bearing in mind the regulations. Food delivery apps and industries have massively helped the hospitality industry. Supply chain sector took a hit during the onset of pandemic but then rose steadily through the digitization avenue helping companies across sectors.

Work from Home Risks and COVID-19 Impact

Work from home does offer benefits but it's also important to understand the risks associated

- **GDPR and Privacy Related Risks:** Remote work means employees can work out. Of anywhere, employers have less visibility and control. In the event of data breach, it would be difficult to contain the incident within the borders of the regulatory line of control, however there can be access control policies in place and access mechanisms that only allow access to employees within specified geographical locations to enforce privacy regulations.
- **Phishing Email Risks:** Phishing attacks prey on human emotions and with staff working out of different locations it becomes easier for the attackers to target individuals, training employees on how to detect and avoid phishing emails can reduce the risk posed by these emails.
- **Weak Passwords:** This is a very significant attack vector since exposing a weak password is very easy for attackers through various cybersecurity attack techniques, enforcing strong access control measures, use of MFA (Multifactor Authentication), single sign on using corporate VPN are some of the techniques to help mitigate this control gap.
- **Risk of Unsecured Home Devices:** employees using personal devices are always at risk since personal devices do not have inherent controls like VPN, password enforcement and policies etc., moreover they are accessed via home networks, absent firewalls and other network defense controls. Using corporate devices and zero trust mechanism as described in one of the following sections will help mitigate this risk [8].

Method & Use Cases

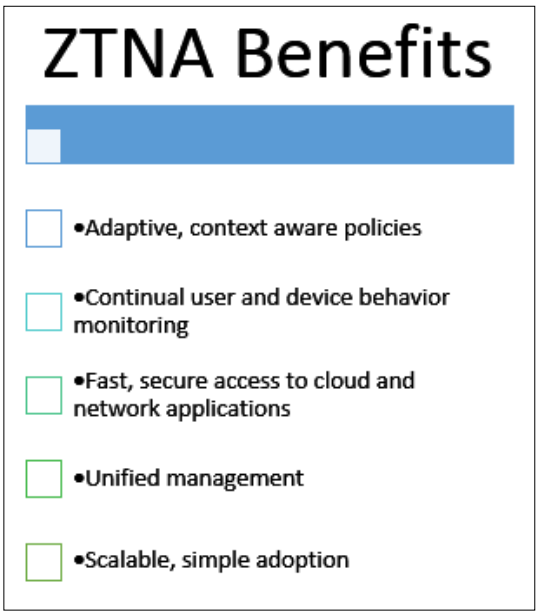
Risk managers play a crucial role in delivering critical information at right time to senior leadership to make right decisions, bringing in the comprehensive risk portfolio. Risk managers do need a risk management framework that can enable them to deliver risk mitigation strategies that business require, bearing in mind the risk appetite [4,16]

Several measures and techniques have already been discussed in this article, however there are few industries tried and test measures that help mitigate the cybersecurity risk stemming out of staff working remotely, following pandemic measures and regulations.

Shipping corporate laptops or devices with security features enabled can mitigate the risks coming from employees using their personal devices. Multifactor authentication and single sig on features also contribute to the mitigation measures.

Zero trust network access is another concept implementation that is tried and tested in firms that face challenges with hybrid and remote working and enables IT infrastructures built from multiple environments [13].

Following is some of the quick benefits by Zero Trust Network Security (ZTNA)



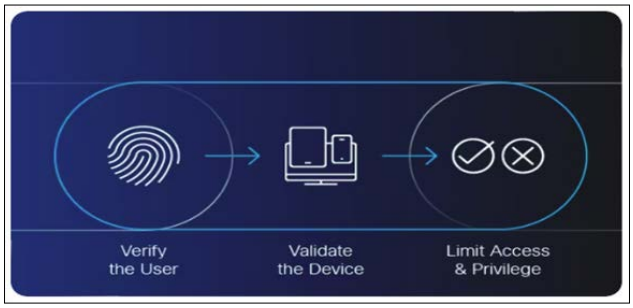


Figure 2: ZTNA by Cisco [13]

Many customers have used it and are still using the implementation of this concept, Risk managers can massively help in identifying risks coming out of the hybrid and remote work scenarios, these risks when identified through various channels and collaboration between teams, these risks post identification can be reported to Senior management.

For Example: During the start of the pandemic, corporate laptops had to be shipped via third parties to different corners of the globe, there are risks involved with shipping, data breach, exposure etc. Risk managers can work with the responsible stakeholders in support services and help quantify that risk, post which they can ensure management response on those risks based on the rating and compensating controls. Similarly, if there are data breaches involving 3rd parties, Risk managers can work with Vendor management teams and ensure contractual obligations are in place, alternatives, mitigating controls for the risks identified. All of these cases ensure the involvement of governance forums very similar to the steering committees where CIOs (Chief Information Officers) Senior Directors and partners of the firm participate, CISOs (Chief information Security Officer) are present alongside Accountable executives and engineering, product, design teams etc.

These frameworks and processes can be applied regardless of industry that organizations are in, small and large firms, there needs to be a dedicated Information security and risk manager.

Conclusion

While the pandemic did hint at recessions with some businesses folding in, due to lack of innovation or flexibility, other businesses did thrive dur to their adaptive strategies, adoption of technology, being flexible with their workforce, eventually this helped them in the long run. The new strategies did attract cybersecurity related threat variants, however, there are technologies as mentioned in this paper, that can help defend firms and its resources. The role of a risk manager also is pivotal since the risks identified through various channels can be communicated back and forth between staff members and management thus ensuring a appropriate risk response.

References

1. Pandemic caused digital shift in financial services. Available: https://tink.com/press/digital-financial-shift/.
2. Guillén MF (2020) How Businesses Have Successfully Pivoted During the Pandemic. Harvard Business Review. Available: https://hbr.org/2020/07/how-businesses-have-successfully-pivoted-during-the-pandemic.
3. Morgan B (2020) 10 Examples Of How COVID-19 Forced Business Transformation, Forbes. Available: https://www.forbes.com/sites/blakemorgan/2020/05/01/10-examples-of-how-covid-19-forced-business-transformation/?sh=526c748f1be3.
4. Andrew Hunt, "Pandemic (COVID-19) has Changed the Role of Risk Managers," www.360factors.com. https://www.360factors.com/blog/covid-19-changed-the-role-risk-managers/.
5. Waller H (2022) 5 Ways Businesses Have Adapted to the COVID-19 Pandemic. Howl Marketing. Available: https://howl.marketing/5-ways-businesses-have-adapted-to-covid-19/.
6. EMILY BARONE (2022) The Pandemic Forced Thousands of Businesses to Close—But New Ones Are Launching at Breakneck Speed, Time. Available: https://time.com/6082576/pandemic-new-businesses/.
7. [Deborah Lovich, Frank Breitling, Jonathan Feldman, Bharat Khandelwal, Chris Matte (2020) Work Will Never Be the Same—Savvy Business Leaders Are Adapting to Change That's Already Here, BCG Global. Available: https://www.bcg.com/publications/2020/how-business-leaders-are-adapting-during-covid-19.
8. redcentric (2021) The top 5 security concerns of remote working. Redcentric. Available: https://www.redcentricplc.com/network-security/top-5-security-concerns-of-remote-working/.
9. Irwin L (2021) The Cyber Security Risks of Working From Home, IT Governance UK Blog. Available: https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home.
10. BusinessWire (2021) Cyber Threats Have Increased 81% Since Global Pandemic. Available: https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic.
11. CISA (2020) Confronting Heightened Cybersecurity Threats Amid COVID-19. Available: https://www.cisa.gov/resources-tools/resources/confronting-heightened-cybersecurity-threats-amid-covid-19.
12. CISA (2020) COVID-19 Exploited by Malicious Cyber Actors. Cybersecurity and Infrastructure Security Agency CISA. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-099a.
13. What Is Zero Trust Network Access? Cisco. Available: https://www.cisco.com/c/en/us/products/security/zero-trust-network-access.html.
14. Lohrmann D (2020) 2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic. Government Technology. Available: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.
15. risk management - Glossary | CSRC. Available: https://csrc.nist.gov/glossary/term/risk_management.
16. Risk Appetite - Glossary | CSRC. Available: https://csrc.nist.gov/glossary/term/Risk_Appetite.
17. COVID's impact on the financial services industry. www.mparticle.com. Available: https://www.mparticle.com/blog/covid-19-financial-services/.
18. Leonid Grustniy (2021)The great lockdown: How COVID-19 has affected cybersecurity. Available: https://usa.kaspersky.com/blog/pandemic-year-in-infosec/24451/.