Why In-Office Work Is The Real Threat to Cybersecurity



Opinions expressed by Entrepreneur contributors are their own.

Imagine a home filled with sophisticated locks, CCTV cameras, and a state-of-the-art security system. Yet, the owner leaves the back door wide open. This is precisely what’s happening in the world of corporate cybersecurity. As organizations fret over the potential risks of remote work, new research suggests the real dangers lurk within the office itself. That finding from a groundbreaking study from the Farmer School of Business at Miami University is definitely a surprise to me and my clients who I help transition to hybrid and remote work, and it will inform some valuable conversations going forward.

The unexpected benefits of remote work on cybersecurity

The Farmer School of Business researchers discovered that remote workers exhibit a higher level of cybersecurity awareness and take more security-related precautions than their in-office counterparts (forthcoming in the July issue of *Computers & Security*). That's right – working from home might actually make employees more vigilant when it comes to cybersecurity. In my emailed interview with the author Joseph K. Nwankpa, he told me "When we surveyed remote workers, we expected the results to reveal cybersecurity complacency, but surprisingly, the survey revealed remote cyber vigilance."

This surprising outcome can be attributed to the so-called "Peltzman Effect" and the complacency framework, which the study draws upon to explore how remote working may trigger a moral hazard regarding employee cybersecurity awareness and security-based precaution-taking. Remote employees tend to feel a heightened sense of responsibility for their own cybersecurity, while office workers often become complacent, trusting their companies to handle cyber threats on their behalf.

Related: Employers: Hybrid Work is Not The Problem – Your Guidelines Are. Here's Why and How to Fix Them.

Complacency: The Achilles' heel of office workers

Imagine being on a cruise ship with an impeccable safety record. You might feel so secure that you skip the safety drill and neglect to learn the location of the lifeboats. This is the complacency effect in action. Office workers, surrounded by the perceived safety of their company's cybersecurity measures, may be less likely to follow best

practices and take necessary precautions.

The study cites prior research that reveals how employees working within the corporate office and boundaries trust their firms to develop, maintain and update security countermeasures to mitigate cybersecurity threats and risks. As a result, these employees are not apt or mindful of security threats and concerns, leading to constrained cybersecurity awareness.

On the other hand, remote workers, like sailors navigating stormy seas, understand that they must be constantly vigilant. This heightened awareness leads them to take more security-based precautions, ultimately keeping their company's digital assets safer.

Indeed, the human element of security is enhanced through a switch to remote work. Thus, Nwankpa stated "Our study found that working from the office within corporate firewalls and security boundaries induced employees to exhibit risky cybersecurity behavior, such as diminished cybersecurity awareness and precaution-taking. However, switching to remote work made employees feel insecure, leading to heightened cybersecurity awareness and cybersecurity precautionary measures."

The pivotal role of information security policy compliance

The study also found that information security policy compliance played a significant role in remote workers' heightened cybersecurity awareness. This suggests that companies must prioritize and enforce their security policies to ensure that all employees, whether in the office or at home, are adequately prepared to handle cyber threats.

The research model used in the study examined the impact of remote working on security-based precaution-taking and the

role of cybersecurity awareness in the relationship between remote working and security-based precaution-taking. The data collected from 203 remote workers across the U.S. provided strong support for the research model, indicating that remote working is positively associated with cybersecurity awareness and security-based precaution-taking.

Furthermore, the study reveals that as remote workers gain cybersecurity awareness, they are more likely to apply security-based precaution measures. This reinforces the idea that fostering cybersecurity awareness among remote workers can lead to better protection of organizational information assets against threats.

Related: Why Cybersecurity Needs to be Prioritised as Small Businesses Face the Cost-of-Living Crisis

Remote Work: A potential solution to cybersecurity woes

Contrary to popular belief, the findings of this study demonstrate that remote work can actually improve cybersecurity. Companies can leverage this knowledge to their advantage, promoting remote work arrangements and fostering a culture of vigilance and cybersecurity responsibility among their employees.

One way to achieve this is by understanding the relationship between cybersecurity awareness and security-based precaution-taking. By focusing on this relationship, organizations can clarify how and when remote working can create positive cybersecurity behavior among end-users, as suggested by the study.

Organizations should not shy away from embracing remote work arrangements, as the study reveals that these can lead to better cybersecurity outcomes. By fostering a culture of

trust, personal responsibility, and cybersecurity awareness among remote employees, companies can empower their workforce to take the necessary precautions and maintain a high level of vigilance, ultimately leading to a more secure digital environment.

The importance of training and employee engagement

To further enhance cybersecurity in a remote work setting, organizations should invest in comprehensive training programs that cover both technical and behavioral aspects of cybersecurity. By making employees aware of the potential threats and risks, as well as providing them with the tools and knowledge needed to protect themselves and the company, businesses can significantly reduce their vulnerability to cyberattacks.

In addition, organizations should actively engage their remote employees and encourage open communication about cybersecurity issues. By involving employees in the decision-making process and addressing their concerns, companies can create a sense of ownership and shared responsibility for the organization’s cybersecurity.

Reevaluating Cybersecurity Strategies for a Hybrid Workforce

As the business world moves towards a more hybrid workforce, with a mix of office-based and remote employees, it is crucial for organizations to reevaluate their cybersecurity strategies. Companies must consider the unique challenges and opportunities presented by remote work and adapt their policies and practices accordingly.

This may involve updating security protocols, implementing new

technologies, and rethinking the traditional office-centric approach to cybersecurity. By embracing the unexpected benefits of remote work and adapting to the evolving digital landscape, organizations can create a more secure and resilient future.

The groundbreaking study from the Farmer School of Business at Miami University opens the door for further research into the distinctions between remote and office work and their implications on cybersecurity. Future research could explore how different remote work arrangements, such as hybrid models or fully remote workforces, may impact cybersecurity awareness and precaution-taking behavior among employees.

Moreover, researchers could investigate the role of various factors, such as organizational culture, leadership, and technology, in shaping employees' cybersecurity behavior in both remote and office environments. This would provide valuable insights to help organizations develop more effective strategies for managing cybersecurity in an increasingly connected and remote world.

Related: Cybersecurity Practices That Protect Your Small Business

Cognitive Biases and their Impact on Cybersecurity

Cognitive biases can significantly influence how employees perceive and respond to cybersecurity threats, both in remote and office settings. By understanding the impact of these biases, organizations can tailor their cybersecurity strategies to address these psychological factors and promote more effective security behaviors among their workforce. Let's explore two specific cognitive biases that may impact cybersecurity in the context of remote work and office environments: the status quo bias and the optimism bias.

The status quo bias refers to the tendency for people to prefer maintaining their current state or situation, even when change could potentially bring about benefits or improvements. In the context of cybersecurity, employees working in a corporate office environment may be more prone to the status quo bias, as they might assume that their organization's existing security measures are sufficient to protect them from cyberthreats.

This complacency can lead to a lack of personal responsibility and a decreased likelihood of adopting new security behaviors or updating existing practices. The Farmer School of Business study highlights this issue, revealing that employees working in corporate offices often trust their organizations to handle cybersecurity threats and, as a result, may neglect their own role in safeguarding company data and assets.

To counteract the status quo bias, organizations should continuously emphasize the evolving nature of cyber threats and the importance of individual responsibility in maintaining security. Encouraging employees to stay updated on the latest security best practices and providing regular training on new threats can help keep cybersecurity at the forefront of their minds and reduce the impact of the status quo bias.

The optimism bias refers to the inclination of individuals to underestimate the likelihood of negative events occurring, while overestimating the probability of positive outcomes. In the context of remote work and cybersecurity, the optimism bias may manifest as office-based employees believing that they are less likely to fall victim to cyberattacks than their remote counterparts.

This overconfidence may lead office-based workers to overlook potential security risks and neglect precautionary measures, such as adhering to company security policies. The Farmer School of Business study supports this assumption by showing that remote workers are more likely to have a higher level of

cybersecurity awareness and take more security-related precautions than those working in an office.

To mitigate the effects of optimism bias, organizations should provide remote employees with clear and realistic information about the cybersecurity risks associated with remote work. Sharing real-life examples of cyberattacks targeting office-based as well as remote workers and emphasizing the importance of personal responsibility can help raise awareness and encourage employees to be more vigilant.

Conclusion

The study from the Farmer School of Business at Miami University serves as a wake-up call for organizations to rethink their approach to cybersecurity in the age of remote work. By embracing the benefits of remote work, fostering a culture of cybersecurity awareness, and adapting their strategies to the evolving digital landscape, companies can ensure the protection of their valuable digital assets and navigate the treacherous waters of the cyber world with confidence.

https://www.entrepreneur.com/science-technology/why-in-office-work-is-the-real-threat-to-cybersecurity/452562