International Journal of
**Technology and
Systems**
(IJTS)

The Human Element in Cybersecurity: Exploring Cognitive Biases While Working Remote

Journal of Technology and Systems
ISSN : 2788-6344 (Online)
Vol. 7, Issue No. 1, pp 1 – 5, 2025
www.carijournals.org

The Human Element in Cybersecurity: Exploring Cognitive Biases while Working Remote

Author: Pratik Koshiya

ISC2 Certified Information Systems Security Professional

https://orcid.org/0009-0003-1781-9266

Accepted: 23rd Dec, 2024, Received in Revised Form: 14thJan, 2025, Published: 28th Jan, 2025

Abstract:

Virtual work opened a whole lot of change when it came to the cybersecurity landscape. Technology has made many contributions to secure remote workplaces, but the human element has always been a targeted attack vector to mitigate cyber threats. This paper explores the influence of human behavior and cognitive biases on the vulnerabilities that affect remote work environments due to poor security decisions coming because of some particular biases and how the features of remote work amplify their effects. The paper also suggests appropriate techniques for organizations on how to tackle these issues through effective training, awareness programs, and by improving security policies. Understanding and mitigating the human factors involved in Cybersecurity would give organizations an edge in developing more secure and resilient remote work environments.

Keywords: *Cybersecurity, Virtual Work, Cognitive Biases, Remote.*

Introduction:

While the COVID-19 pandemic fast-tracked the transition to remote work, it revolutionized organizations' operations, and it also added a brand-new dimension of cybersecurity concerns. Of course, technology has a great role to play in securing remote workspaces; Yet the human factor is the most influential of them all in preventing cyberattacks. This happens because, most often, the weakest link in the security chain is the employee, whose actions and thought patterns can also contribute greatly to vulnerabilities in the cybersecurity domain.

This paper discusses the intersection of human behavior, cognitive biases, and cybersecurity in the remote workspace. The paper would explain specific biases that drive poor security decisions and how risks amplify in a work-from-home scenario.

Remote Work and Vulnerabilities:

Working from home has introduced new challenges and further opened vulnerabilities pertaining to human behavior and cognitive biases. Some of the key contributors to this component include:

Reduced Supervision: Less control and more autonomy while working from home may cause employees to be less careful with their online behavior and to deviate from security protocols.

Addressing human error, most focus on traditional office settings, where employees work under structured supervision and have direct access to IT support. This oversight fails to account for the unique challenges presented by remote work environments, including increased autonomy, reliance on personal devices, and diminished organizational oversight.

Isolation: Feeling isolated and no social interaction and engagement can lead remote workers more susceptible to social engineering attacks that exploit their loneliness and desire for social connection. In past, incident demonstrates the vulnerability of organizations to social engineering attacks that exploit human trust and manipulate employees. It emphasizes the need for robust security awareness training and strong internal security controls to prevent unauthorized access to sensitive systems.

Dependency on Technology: More and more attacks on personal property and networks will result from added reliance on digital media for communication and even greater dependence on personal devices and residential broadband networks. Inadequate use of virtual private networks (VPNs), weak password practices, and insufficient encryption protocols, all of which expose sensitive data to greater risks.

Remote workers who rely on email, instant messaging, and video conferencing that also almost all individuals make use of nowadays, are prime targets by cybercriminals. Phishing attacks rely on the human need for trust and take cognitive shortcuts using any real forms of communication to create fake authenticity. Psychological distance created by remote workers, since there are fewer social cues through interaction within a work group because communication will happen between people through a screen. And it continues to put up more barriers against verifying potentially suspicious messages or willingness to report possible threats.

Impact of cognitive biases and cyber vulnerabilities on cybersecurity decision-making:

There are errors that arise through the psychology of an individual, which can lead to a rational judgment deviation resulting in errors-predictable and manipulable-by an individual in making decisions. Such cognitive biases place employees at high risk for phishing and other forms of social engineering and cyberspace-based attacks in cybersecurity environments. The sample might be optimism bias, convincing an individual that they are less likely to become a victim than others of a fake but documented phishing emails and malware. This is typical in Cybersecurity industries. The point is that such biases often lead someone to underestimate risks, overvalue competence, or even make incorrect decisions about aspects related to cybersecurity. For Example: optimism bias, employees possibly believe that they are not prone to any cyber-attacks, and this may lead an employee to disregard information security training, reuse weak passwords, fail to pay attention to security alerts, etc. Similarly, Overconfidence bias means people think they can detect phishing attempts or identify malicious links and so are more likely to fall for scams.

Cognitive bias may also be identified as “anchoring” which is a process where individuals use the first piece of information to make a decision. For example, A remote worker is testing a new file sharing app for their team. During the onboarding presentation the software vendor says the app has “state of the art encryption” and is “used by Fortune 500 companies”. This becomes the anchor for the worker’s perception of the app’s security. When the IT department later raises concerns about the app’s data privacy, the employee minimizes these issues because they believe the app must be secure because of the initial claims of encryption and Fortune 500 usage. For remote workers, if an organization notified them at an early stage using tailored message about threats in simple language for technical and non-technical users then most recent cyber-attacks can be tackled. The availability bias can also cause employees to overplay recent or vivid cybersecurity incidents and skew their risk assessments. For example, after hearing about a colleague’s experience with a phishing attack, an employee might become super vigilant about phishing but ignore other major vulnerabilities like unsecured network connections

Behavioral Patterns and Cybersecurity Risks

More human behaviors contribute to the vulnerabilities while working remotely. For example, in a scenario where a person is multitasking, remote jobs which present an interaction between family commitments, leisure activities, and the time spent executing house chores with a simultaneous job execution. All these can affect a person's attention to detail and thus increases the risk of error, such as clicking a hasty link from a phishing email or a person forgetting to check the authenticity of the sender or communication involved in email.

Specific to remote work environments, for convenience-seeking behavior, it is prominent in remote work situations which may or may not couple with the complete lack of oversight. For example, for example, it says in the 2024 Report concerning Verizon Data Breach investigations that more than 68% of cases involve some human element that involves remote employees. Remote employees admitted bypassing security protocols and procedures to facilitate their work. This behavior consists of urgency and overconfidence bias partially. This is typical for places with pressure to meet deadlines and not enough secured devices for very cyber attacked employee in an organization since remote employees compromise easily in terms of convenience and go for less secured Wi-Fi, sharing devices or information with family, or even skipping virtual private networks (VPNs) to hasten their work-related tasks. All these activities expose the companies to various risks such as data breach or unauthorized access. However, the issue of stress coupled with fatigue, both of which may result from working remotely, increases the level of cybersecurity risk for organizations. The reason is that stressed or fatigued employees may tend to compromise on some important policies, such as using the same password repeatedly, delaying software update application or operating systems, and many more, which ultimately weakens the entire cybersecurity posture for the organizations and can end up getting compromised.

Recommendations for Organizations

What factors need to be taken into consideration in the human aspect of cybersecurity, an integrated education, behavioral interventions, and technological enhancements would be lined up for them, synergistically creating a solid defense system. For instance, create a behavioral nudge training program to teach employees everything about phishing tactics (education), something that creates real-time alerts to verify suspicious links (behavioral interventions), with developing multi-factor authentication systems (technological enhancements). While this integrated strategy aligns individual awareness, it also facilitates reduced incidence of mistakes through proactive and automated measures. First, the educational institutions must set up training programs that will educate employees on common threats but also train them on the cognitive biases under risky behaviors. For instance, a phishing-simulated attack may make an employee realize what optimism bias and overconfidence really do in terms of instilling a false sense of invulnerability.

Behavioral nudges may also be an effective means of drawing individuals' attention to protect themselves against unsafe behaviors. For example, reminders to change passwords or use of secure networks can be delivered through chain of command. Organizations can also establish a culture of accountability and shared responsibility by creating transparency and encouraging employees to come forward with mistakes and errors without fear of retribution.

But first, a good authentication scheme is one of the best countermeasures to minimize the extent of damage caused by human error. Endpoint security tools will monitor and block suspicious activities on remote devices, while virtual private networks (VPNs) ensure secure transmission of data. Of course, such measures should be employed which provide good user experience to minimum frustration and reduce the temptation to bypass them.

Conclusion

The human factor plays a very vital role in cybersecurity, especially with remote work. Human behavior can easily be understood by the kinds of cognitive biases that come into play as well as the strategies to minimize their effect when one is considering a more secure and more resilient remote work environment.

Biases such as optimism, overconfidence, and availability affect perception of risk and decision-making while behaviors such multitasking or being a convenience seeker introduce organization to greater threats. Isolation, on the contrary, magnifies the effects of remote work, employees tend to communicate more with one another through digital communication rather than other means. Organizations must thus take an integrated, more holistic view incorporating behavioral insights into education programs and may be those easy-to-use solutions. This way, strengthening the defense of humans will bring much more towards creating a cohesive framework that can withstand complex instances expected during remote work operations.

References

Ref: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak#:~:text=The%202016%20Democratic%20National%20Committee,out%20by%20the%20Mueller%20investigation.

https://insurica.com/blog/colonial-pipeline-ransomware-attack/