

Zack Fok

CYSE200T

November 17, 2024

BLUF (Bottom Line Up Front)

Cyber technology has made it easier for workplace deviance to occur by allowing anonymity, granting quick access to sensitive information, and enabling misuse through actions like cyberloafing, data theft, and insider threats. To address these risks, companies need strong cybersecurity policies, monitoring systems, and a positive work culture to keep everyone safe and productive.

Key Risks of Cyber Technology in Workplace Deviance

Cyber tools make it easy for people to act anonymously, which can lead to problems like harassment or fraud. Sensitive data is more accessible than ever, creating opportunities for employees to steal or misuse it. Some may also spend work hours on personal activities (cyberloafing) or introduce security risks by using unauthorized apps or devices. Remote work setups, with less oversight, make these issues even harder to control.

Mitigating Strategies

Organizations can fight back by putting clear cybersecurity rules in place and teaching employees how to use tech responsibly. Monitoring tools can catch suspicious activity, and role-based access controls ensure that only the right people see sensitive information. Regular system checks and audits are crucial, but the real game-changer is fostering a workplace culture where people value integrity and accountability.

Conclusion

While cyber technology has made work more efficient and connected, it also creates new challenges in managing workplace behavior. From employees misusing resources to more serious risks like data theft, organizations must be ready to handle these threats. By combining strong security measures with a supportive and honest workplace environment, companies can stay ahead of these risks and create a safe, productive space for everyone.