

**Cyber Technology in Workplace Deviance**

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

April 9, 2025

**Assignment:**

How has cyber technology **created** opportunities for workplace deviance?

## Cybercrime vs. Workplace deviance

Cybercrime is cyber-related behavior that is against the law, and it is behavior society deems morally and/or ethically wrong because society judges the behavior as a threat to social order (Payne & Hadzhidimova, 2018). Workplace deviance is voluntarily, deliberately, and intentionally violating important organizational norms, policies, or rules, harming the organization and/or members/employees (Wikipedia, 2025a) (HR Zone, 2024). Though workplace deviance is sometimes less damaging than cybercrime on the front end, an insider threat's cumulative effect can lead to more significant impacts that negatively impact an organization's financial and operational success.

CISOS must develop and implement strict cyber technology strategies, infrastructure, and networks to help monitor insider behavior while preventing insiders from exfiltrating data beyond the organization's network. Examples include implementing of Data Loss Prevention (DLP) policies and firewalls and restricting data transfers from USB or storage devices. IT Departments may block connections to the company network from unapproved or "Shadow IT" systems and devices by locking unused device ports, whitelisting company-approved devices, and turning off "Auto-Run" or "Auto-Play" features to prevent programs from automatically running without administrative permission on local workstations. Lastly, CISOs may also work closely with Human Resources (HR) to "establish proactive measures using validated risk and talent management assessments to identify potential insider cyber threats during the recruitment and hiring phase" (Jones, 2023).

## Mediums & Examples of Workplace Cyber Deviance

Many examples of workplace deviance use cyber technology (Jones, 2023). First, employees can exploit their privileged access or gain access without permission to company data, systems, or resources and steal the information for personal self-gain or revenge, including posting or sharing proprietary and sometimes embarrassing company information on public platforms. Depending on the data type, some employees may store or hoard it for use on a personal project and profit in areas like the stock or real estate market. Lastly, “Logic Bombs” and sabotaging companies via malware are real threatening events. Logic Bombs are not fictitious events that occur only in movies like *Jurassic Park*, *The Rock*, and *Mission Impossible*.

Second, employees may inappropriately or offensively communicate with one another through online messaging services and platforms like Skype or Microsoft Team Meetings. That may include cyberbullying and cyber harassment, where some may attempt to continually communicate with a target to disrupt their workflow for self-pleasure. Mutual flirtatious banter and unprofessional ‘locker-room’ talk may qualify as inappropriate and offensive when judged against the company’s Acceptable Use Policy (AUP) and fundamental laws governed by the U.S. Department of Labor.

Third, many employees are notorious for using the abovementioned deviances to cyberloaf. Cyberloafing is when employees spend excessive work time on non-work-related internet activities and tasks, like surfing social media accounts, replying to personal emails, or making online purchases through stores like Amazon. During the COVID-19 pandemic, scores of employees abused their remote privileges not to work at all. Many remote employees worked multiple jobs for different employers during the same business hours, using specialty software and hardware to appear physically present and working without interruption.

Fourth, employees may pirate the organization's digital content and licensing for specific programs to avoid purchasing the software for themselves using their funds. In addition to stealing digital content, employees may use their account permissions to adjust accounting and inventory numbers to steal physical/tangible items like construction or networking tools and supplies. They may adjust the numbers for the tools and supplies to appear they never existed in the first place, or someone may sell them to an "unknown" vendor on a prior date.

In conclusion, workplace deviance is a serious issue that may not look important or dangerous at the front end but can create more damage and harm if left unchecked and undeterred. In the above examples of workplace deviance, the criminal justice system may consider each deviant behavior illegal, breaking the law in some fashion, thereby warranting immediate termination and possible civil and criminal prosecution against them. For example, the misuse of information or unauthorized access and distribution of sensitive information may violate Intellectual Property and Trade Secret Laws; cyberloafing violates standard AUPs and labor contracts employees sign before the start of employment; inappropriate flirting via electronic communication can violate state and federal laws of sexual harassment. I have witnessed the abovementioned occurrence with other employees while employed with different organizations, resulting in their immediate termination, with a few prosecuted in the civil and criminal courts and sentenced to prison time.

## References

- HR Zone. (2024, November 8). *What Is Workplace Deviance?* Retrieved from HRZONE:  
<https://hrzone.com/glossary/what-is-workplace-deviance/>
- Jones, J. W. (2023, November 21). *Employee Cybercrime and Deviance: A Loss Prevention Psychology Perspective*. Retrieved from LPM: Loss Prevention Magazine:  
<https://losspreventionmedia.com/employee-cybercrime-and-deviance-a-loss-prevention-psychology-perspective/>
- Payne, B. K., & Hadzhidimova, L. (2018). Cybersecurity and Criminal Justice: Exploring the Intersections. *INPRESS at International Journal of Criminal Justice Sciences*, 18.
- Wikipedia. (2025a, March 14). *Workplace Deviance*. Retrieved from Wikipedia:  
[https://en.wikipedia.org/wiki/Workplace\\_deviance](https://en.wikipedia.org/wiki/Workplace_deviance)