

Why Cybercrime?

A Group Reflection

Amiah Armstrong, Jasmyn Wilhelm, and Louis Ferrara

Department of Sociology and Criminal Justice

CRJS 310: Cybercrime Foundations

Roderick Graham

08 November 2024

Why Cybercrime?

Cybercrime has become a complicated problem in our digital age that affects everyone, from big businesses to citizens. Given the vast amount of information available through the Internet Crime Complaint Center's Annual Reports and the findings from Graham and Smith's (2024) *Cybercrime and Digital Deviance*, it seemed relevant and ideal to create a presentation on this subject. We used technological resources like Google Slides, Microsoft Word, and audio narration to make this subject interesting and comprehensible for viewers. Once put together, these resources enabled my team to organize ideas and make the topic of cybercrime easier to understand and impactful.

Multiple resources were employed in the preparation of our presentation to make the issue easier to relate to and allow a greater understanding of it. Amiah Armstrong used a microphone to record the audio narration; Louis Ferrara used Google Slides to create and arrange the slides; and I used Microsoft Word to outline and draft the written reflection's content. A productive workflow was made possible by these tools: Word helped in organizing my thoughts, while Google Slides provided options for visual layout collaboration and topic transitions. Amiah was able to customize the presentation with the microphone, which will increase the audience's interest in the material. These resources worked together to guarantee that our team could communicate our findings to the audience in an organized and straightforward way.

From the Internet Crime Complaint Center's Annual Reports and the main ideas of Graham and Smith's *Cybercrime and Digital Deviance* (2024), certain insights that highlighted the patterns and complexity surrounding cybercrime were selected. Since they would be highly relatable to the audience, these insights were chosen to show the most common forms of cybercrime, their growth patterns, and the societal effects. My group wanted to express the

Why Cybercrime?

practical extent of cybercrime by focusing on actual data and significant patterns, going beyond theories to offer a realistic perspective that encourages critical thinking on measures to prevent it.

Although Deterrence Theory is mentioned in the team's presentation, Rational Choice Theory offers an alternative perspective on cybercrime. Cybercrime, according to rational choice theory, is the outcome of intentional decisions made by people who weigh the risks along with potential benefits. According to this theory, people commit cybercrimes when they believe that the potential advantages outweigh the risk of being caught. Rational Choice Theory stresses personal decision-making and how expected risks and rewards influence behavior, while Deterrence Theory focuses on deterring crime by threatening consequences. Rational Choice Theory can help in directing preventative actions that target the fundamental decision-making processes that motivate future offenders by giving insight into these reasons.

If someone were to ask my group what the purpose of criminological theory is, we would respond that it gives us an organized approach to understanding why crime happens and how society can reduce it. Frameworks for examining the underlying causes, patterns, and social environments of criminal behavior are provided by criminological theories. Whether or not the problems are social, psychological, or economic, they can also function as guides for legislators, law enforcement, and social groups to create solutions. In the end, criminological theories aim to decrease crime by revealing it with insights obtained from data and offering both preventative and corrective strategies.

As a group, we gained deep awareness of the significance of criminological theories in developing responses to cybercrime during this research. Specifically, deterrence theory offered a framework for considering cybercrime as a behavior that can be managed through organized

Why Cybercrime?

preventative actions. By focusing on raising the dangers associated with cybercrime, we

discovered that concentrated tactics might significantly decrease the number of these crimes.

Using theories from criminology to cybercrime is essential in creating adaptable, evidence-based

methods to protect people and organizations against damage in our ever-changing digital world.

Why Cybercrime?

References

Annual Reports, Internet Crime Complaint Center (IC3). (n.d.).

<https://www.ic3.gov/AnnualReport/Reports>

Graham, R. S., & Smith, S. K. (2024). Cybercrime and Digital Deviance.

<https://doi.org/10.4324/9781003283256>

Google. (n.d.). Google Slides.

<https://www.google.com/slides/about/>

Microsoft Corporation. (n.d.). Microsoft Word.

<https://www.microsoft.com/en-us/microsoft-365/word>