

Memo

To: Professor Klena

From Stevie Johnson, Law and Digital Forensics 404

Subject: Cyberterrorism

Date: March 11, 2026

1. **Act of Cyberterrorism?** The actions of TheDarkOverlord Solutions are classified as a cybercrime or cyber extortion rather than cyberterrorism. Cyberterrorism usually involves political or ideologically motivated attacks intended to cause fear or disrupt critical infrastructure. The actions conducted in this case were primarily motivated by financial gains through ransom demands. (Maras)
2. **Methodology.** Based on chapter 1 Entering the World of Cybercrime. TheDarkOverlord Solutions could have gained access to the school districts servers through many methods like phishing emails, malware such as trojans or spyware, exploiting unpatched vulnerabilities. Social engineering techniques from chapter 6 could have also been used to trick staff into revealing login information or installing the malicious file. (Maras)
3. **Privacy Act Violations?** The releasing of personal information about students and teachers would not violate the Privacy Act of 1974, because that law applies to how U.S. federal government agencies collect, maintain, and disclose personal records. TheDarkOverlord solutions are a private criminal group not a federal agency so this act would not apply to them. (Maras)
4. **Fourth Amendment Violation?** Their actions would not be a Fourth Amendment Violation because that amendment protects against unreasonable search and seizures conducted by the government, not private individuals. Because the hackers are private threat actors and are not working for or under law enforcement, authorities could use the information as evidence if it was obtained independently. (Maras)

Work Cited

Maras, Marie Helen. *Computer forensics: Cybercriminals, Laws, and Evidence*.
2nd ed., Jones & Bartlett learning, 2016