There are white-hat, grey-hat (CIA), and black-hat hackers who pose ethical questions for developers in the field. Find an example (nonpolitical) that can be used in your presentation for Project Two to illustrate threat levels.

Respond to at least two of your peers by commenting on their examples.

To complete this assignment, review the [Discussion Rubric](https://learn.snhu.edu/d2l/common/dialogs/quickLink/quickLink.d2l?ou=2019750&type=content&rcode=snhu-3178245).

Relations, M. (2025, June 6). *Account compromise leads to Crash Records Data Breach*. Texas Department of Transportation. https://www.txdot.gov/about/newsroom/statewide/account-compromise-leads-to-crash-records-data-breach.html

Earlier this summer, the Texas department of Transportation (TxDot), suffered a cybersecurity breach due to a breach of employee’s account. This is the work of a “blackhat hackers”, who used this breach to gain access to TxDot’s Crash Record Information System (CRIS). The breached account was used to download nearly 300,000 crash reports, that include sensitive & personal information. In the wrong hands, this information can cause irreparable harm with all the personal data leaked.

The motivations behind such an attack are characteristic of cybercriminal activity. The hackers' actions extend beyond simple data theft, venturing into realms such as ransomware, where critical data is encrypted and held hostage, and double extortion, where victims are pressured to pay to prevent the public release of their stolen information. The acquired data could also be weaponized for highly targeted fraud, phishing schemes, and identity theft, posing a direct and severe threat to the privacy and financial security of affected individuals.

In response to the breach, TxDot implemented multiple mitigations such as securing the compromised account, removing additional systems offline, & working with law enforcement \* it’s own cyber security division to investigate the full extent of the breach. They also took steps to notify all potentially afflicted parties.

This incident is just one of many examples that can serve as a reminder of how important it is to have robust security with multiple layers security. It highlights the need for organizations to proactively strengthen defenses, enforce stringent access controls, and conduct ongoing employee training to thwart credential-based attacks. For the public, it emphasizes the necessity of monitoring personal accounts for suspicious activity and exercising caution with communications following data exposure.

Relations, M. (2025, June 6). *Account compromise leads to Crash Records Data Breach*. Texas Department of Transportation. https://www.txdot.gov/about/newsroom/statewide/account-compromise-leads-to-crash-records-data-breach.html

Hey there Andrew, now this takes me back. Unexpected memory.

I definitely appreciated what Geohot was doing for the iphone ecosystem, actually following his guides to root a few ipod touches for myself & friends back in the day. Great times. I think it’s most important to remember that grey hat hackers are often individuals with immense talent who just like the challenge & the freedom that it entails by sharing such information. Just they may operate with a different level of risk for how they shar eit versus a more professional entity.

Your point about "what would have made it white-hat" is crucial. The shift from gray-hat to white-hat isn't about the *discovery* of the vulnerability, but almost entirely about the *process* of its disclosure. Coordinated disclosure isn't just a formality; it's the mechanism that protects the very users the researcher might claim to be helping.

It serves as a great reminder that in security, the impact of an action matters just as much as the intent behind it.

Evening Kain, great write up!

So your telling this me this was finally a case of a vendor using the password for their password & it coming back to cause issues? Obviously not that simple. It was a great breakdown of each class of hacker & potential motivations. The attackers' skills were sophisticated in their lateral movement and malware deployment, but the initial entry was brutally simple: exploiting a trusted third-party relationship with weak security. This completely reshaped how enterprises think about their "attack surface," forcing them to realize that their security is only as strong as the weakest link in their entire digital supply chain.

Let this serve as a reminder that having technical skills is a tool. Multiple levels of ethics is behind those skills, toeing the line between positive construction & negative destruction. In this case, the hackers had the talent to find the flaw yet they chose to expose it in the most harmful way.