

Journal One

Nicholas Duggins

05/24/2026

I would rank the NICE Workforce Framework as follows with the bottom two choices being interchangeable. My first selection would be "Protection and Defense" ranking at number one with the most work roles I would like to do as a career in the future. PD has jobs such as Digital Forensics, Defensive Cybersecurity, and Threat Analysis. Digital Forensics is my number one choice because I initially wanted to do Forensic science before changing my major. Digital Forensics is described as "Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerability mitigation" (2026). These rank as number one because of the real time work advantage among others when it comes to threats and vulnerabilities along with the ability to mitigate and solve.

Rankings 2-3 in respective orders would be Investigations and Implementation and Operations.

Investigations being number two for almost the same reasoning as rank number one with jobs including Cybercrime Investigation and Digital Evidence Analysis. These jobs again work to solve a problem or crime; it takes not just knowledge but intuition and foresight. Implementation and Operations also interest me due to its key factors of being a front-line defensive job with maintaining installation, configuration, and system analysis. These seem to be a "technician" type of career of maintaining, working on, and fixing.

My least two in rankings that I would consider being interchangeable would-be Oversight and Governance along with Design and Development. I consider these my lowest not because I am uninterested in them but because of my knowledge in this field or lack thereof. I am sure with more learning and experience this may change, however with important jobs such as, Cybersecurity Architecture and Enterprise Architecture for DD and then Cybersecurity Instruction or even Program Management I see myself unexperienced.

References:

National Initiative for Cybersecurity Careers and Studies. (2026, April 16). NICE Workforce

Framework for Cybersecurity (NICE Framework). <https://niccs.cisa.gov/tools/nice->

[framework#:~:text=The%20NICE%20Framework%20is%20comprised%20of%20the%20following,rquired%20to%20perform%20tasks%20in%20a%20Work%20Role](https://niccs.cisa.gov/tools/nice-framework#:~:text=The%20NICE%20Framework%20is%20comprised%20of%20the%20following,rquired%20to%20perform%20tasks%20in%20a%20Work%20Role)

Journal Entry Two

Nicholas Duggins

06/01/2026

The principles of science can be applied to cybersecurity because both rely on facts, evidence, and logical thinking. Understanding these principles helps cybersecurity professionals make better decisions when protecting systems and responding to threats. Relativism means that people can have different viewpoints based on their experiences. In cybersecurity, one company may see a certain threat as a major risk while another company may not because their systems and priorities are different.

Determinism is the idea that things happen for a reason. In cybersecurity, security incidents usually have a cause, such as a phishing email, weak password, or software vulnerability that allowed an attacker to gain access. Objectivity means looking at the facts instead of personal opinions. Cybersecurity professionals need to use evidence from logs, alerts, and reports when investigating incidents instead of making assumptions. Scientific principles involve observing, testing, and using evidence to reach

Conclusions.

Cybersecurity teams use these methods when they test systems for vulnerabilities and investigate cyberattacks. Ethical neutrality means focusing on the facts without letting personal feelings affect the results. When investigating a security incident, professionals should follow the evidence regardless of who may have caused the problem. Parsimony means the simplest explanation is often the best one. For example, if a user cannot log in, it is usually better to check for a password issue before assuming the network has been hacked. Skepticism means questioning information until it can be verified. In cybersecurity, this is important because phishing emails and scams often try to trick people into trusting something that is not legitimate. Overall, these principles help cybersecurity professionals think critically, make decisions based on evidence, and better protect organizations from cyber threats.

Journal Entry Three

Nicholas Duggins

06/07/2026

PrivacyRights.org Data Breach Analysis

After reviewing PrivacyRights.org, I think the site provides a valuable resource for researchers who want to study data breaches and cybersecurity trends. According to Privacy Rights Clearinghouse, (Data breaches 2026) there have been "nearly 100,000 reported data breaches since 2005, at your fingertips." With that much information available, researchers can identify patterns in cyberattacks, determine which industries are most frequently targeted, and study the types of data that are most often exposed. The database also allows users to search by organization, breach type, state, or data source, making it easier to compare incidents and identify broader trends.

Researchers could use this information to better understand how cybercriminals operate and how do organizations respond to security incidents. By analyzing breach of data over time, they can determine whether certain attack methods are becoming more common and evaluate which security measures appear to be the most effective. This information can help organizations improve their cybersecurity programs and reduce the risk of future breaches.

I think sociology would benefit greatly from this information because data breaches affect Millions of people can influence how much trust individuals place in companies and technology. Criminology would also benefit because cybercrime continues to grow, and researchers can use breach data to study criminal behavior and attack patterns. Economics is another field that could use this Information because data breaches often result in financial losses for businesses and consumers. Overall, PrivacyRights.org provides researchers with a large amount of real-world data that can be used

to better understand cybersecurity threats and their impact on society.

Reference

Data breaches. Privacy Rights Clearinghouse. (2026, June 5). <https://privacyrights.org/data-breaches>

Journal Entry 4

Nicholas Duggins

06/21/2026

Maslow's Hierarchy of Needs has five levels, and I feel like technology connects to each one in different ways depending on how I use it in everyday life. At the physiological level, technology helps with basic needs like food, rest, and daily routines. For example, I use apps like DoorDash or Uber Eats when I don't have time to cook or go out to get food. It makes it easier to meet basic needs quickly. I also rely on my phone for alarms, so I wake up on time, and sometimes I use sleep or health tracking features to keep my schedule on track. Even simple things like reminders for eating or drinking water help me stay balanced when I'm busy.

At the safety level, technology is important for security and stability. I use banking apps to manage money instead of going to a physical bank, and I can instantly check transactions to make sure everything is correct. Two-factor authentication and secure passwords also help protect my accounts from being hacked. Even navigation apps like Google Maps make me feel safer when I'm driving somewhere unfamiliar because I can avoid getting lost or unsafe.

At the love and belonging level, technology is basically how I stay connected with other people. I use texting, FaceTime, Snapchat, and Instagram to talk to friends and family every day. Even when I'm not seeing people in person, I can keep up with their lives and stay involved. It makes relationships easier to maintain, especially when everyone is busy or far apart. At the esteem level, technology can build confidence and a sense of accomplishment. When I finish assignments online or do well in a class, it feels rewarding. I also get feedback instantly through grades, comments, or messages, which helps me understand how I'm doing. Even small achievements online can make me feel more confident in my abilities.

At the self-actualization level, technology helps me grow and learn new things. I can look up

anything I want, watch tutorials, or learn skills like coding or cybersecurity. It gives me the chance to improve myself and explore interests outside of school.

Journal Entry 5

Nicholas Duggins

06/27/2026

Journal Entry 5: Ranking Individual Motives in Cybercrime

After reviewing the different motives behind cybercrime, the reasons people commit these offenses depend on both the individual and the circumstances surrounding the crime. While some motivations are more common than others, cybercriminals are often driven by a combination of factors rather than a single reason. Based on what I have learned, I ranked the seven primary motives from the one that makes the most sense to me (1) to the one that makes the least sense (7).

1. For Money

Financial gain is the most logical and common motivation for cybercrime. Many sophisticated cyberattacks operate like businesses, where the goal is to steal sensitive information, deploy ransomware, commit fraud, or extort organizations for profit. Because cybercrime can generate significant financial rewards with relatively low risk compared to traditional crimes and money are the strongest motivating factor.

2. Revenge

Revenge is another powerful motivation because it is driven by strong emotions and personal conflict. Individuals seeking revenge often target specific victims to cause emotional, financial, or reputational harm. As discussed by WLAW5008 (2019), every case of revenge pornography causes lasting damage to the victim, demonstrating how personal grievances can motivate extremely harmful cyber offenses.

3. Entertainment

Some individuals engage in cybercrime simply because they find it exciting or entertaining. Curiosity, the challenge of bypassing security systems, or the thrill of hacking can motivate illegal behavior. Lovejoy (2021) described a hacker involved in the scraping of approximately 700 million

LinkedIn records who claimed he committed the attack "for fun," despite later selling the stolen data.

This example shows that entertainment and financial gain can often overlap.

4. Multiple Reasons

Cybercriminals are not always motivated by a single factor. In many cases, several motives exist at the same time. For example, someone may initially hack into a system out of curiosity or boredom but later decide to profit from the stolen information. This combination of motives makes cybercrime more difficult to understand and prevent because motivations can change throughout the attack.

5. Boredom

Although boredom may seem like a minor reason, it can contribute to cybercrime and other harmful online behavior. Individuals with too much free time may engage in online trolling, hacking, or other forms of digital misconduct simply for something to do. Sonjica (2021) also noted that boredom can increase children's vulnerability to cyberbullying and online grooming because they may spend more time online creating and sharing content, increasing their exposure to potential offenders.

6. Political

Political motivations, often associated with hacktivism, involve using cyberattacks to promote an ideological or political cause. These attacks may include website defacements, data leaks, or distributed denial-of-service (DDoS) attacks intended to spread a message or disrupt organizations. While this motivation is understandable within political conflicts, it is less common because it requires a strong commitment to a particular ideology.

7. Recognition

Recognition is the motive that makes the least sense to me. Some hackers seek status, respect, or bragging rights within online communities by claiming responsibility for attacks. However, publicly taking credit for cybercrimes increases the likelihood of being identified by law enforcement because it

creates additional digital evidence. Considering the risks involved, seeking recognition alone seems like one of the least practical motivations for committing cybercrime.