Would You Rather?

Estimated time: 10 minutes

What is critical thinking?

Critical thinking involves objectively analyzing information to make reasoned judgments. It goes beyond technical knowledge, delving into an individual's analytical and reasoning capabilities. This skill is particularly significant in cybersecurity due to the field's rapid evolution, complexity, and constantly changing environment. Additionally, cybersecurity involves various stakeholders, ruthless adversaries, and a continuous influx of new technologies.

In this activity, you will apply critical thinking skills to respond to three scenarios. Remember to base your decisions on technological ethics and security. First, consider the potential consequences of each option at a personal, societal, and global level. Then, analyze each scenario thoughtfully and make a choice. Finally, use critical thinking to justify your perspective on the ethical and security dilemmas presented.

Learning objectives

After completing this activity, you will be able to:

- Apply critical thinking skills to navigate complex scenarios that lack straightforward answers
- Analyze situations from various perspectives
- Evaluate the advantages and disadvantages of different alternatives
- Align decisions with ethical standards and personal values

Instructions

Scenario one

Would you rather keep your online activities private and untracked, even if it means giving up on personalized experiences and convenience?

I would rather keep my online activities private, even if it means sacrificing convenience. As someone transitioning from a background in criminal justice into cybersecurity and compliance, I’ve seen firsthand how data exposure and digital overreach can lead to real harm, especially for vulnerable populations.

Reasoning:

Personally, I prefer to stay in control of my digital footprint and reduce the risk of target ads, profiling, or misuse of my data.

Societally, normalizing deep data collection conditions people to trade privacy for convenience without fully understanding the consequences.

Globally, it reinforces a surveillance economy that can easily be abused by corporations and governments if left unchecked.

Values Reflected:

My background in law in compliance drives my belief that privacy is a right, not a feature. This decision aligns with my values around personal autonomy and ethical data stewardship, both central to a strong cybersecurity foundation.

(or)
Would you rather allow trusted companies to access your data for a customized online experience?

Scenario two

Would you rather opt for basic security measures with simple passwords for convenience?

(or)
Would you rather have highly secure digital accounts requiring multifactor authentication (MFA), biometrics, and complex password protocols, even if it limits your ease of access?

I'd choose strong security protocols over ease of access. Coming from criminal justice, I understand how often people underestimate the risks until it's too late, As someone preparing for a role in cybersecurity, I can't afford to model weak practices.

Reasoning:

Personally, I've already adopted strong password managers, MFA, and secure workflows in my own life, the inconvenience is minimal compared to the cost of a breach.

Professionally, I believe that if I'm going to advise others on risk management and compliance, I need to hold myself to the same standards.

From a user-centered standpoint, security can be made easier without compromising protection, it's about smart design, not fewer layers.

Values Reflected:

Security isn't just a preference, it's responsibility. As someone with my background, I see usability as important, but never more important than protecting people's data and digital identities.

Scenario three

Would you rather support unrestricted technological innovation with the potential risk of ethical and privacy concerns?

I support regulated innovation. I want to see progress, but I want it done right. My experience in the legal system showed me what happens when new systems move faster than our laws, it is always the most marginalized who suffer first.

Reasoning:

Personally, I’ve seen how unregulated platforms can enable harm, from biased algorithms to exploitative practices.

Societally, strong regulation builds user trust and forces companies to prioritize safety alongside speed.

Globally, frameworks like GDPR prove that it is possible to balance innovation with ethics, and I believe we should build on that momentum.

Values Reflected:

As a future GRC or compliance analyst hopeful, I believe innovation needs to be tempered by ethical standards and long-term accountability. I’ve lived in systems where power without oversight causes ral damage. That’s exactly what cybersecurity professionals should be working to prevent.

(or)
Would you rather advocate for strict government regulations on new technologies, protecting individual rights but potentially hindering innovation?

Summary

Critical thinking is instrumental in navigating complex scenarios with immediate and long-term consequences. In scenario one, data privacy versus personalization, critical thinking prompted an in-depth analysis of the importance of privacy against the allure of personalized services.

In contrast, scenario two, security versus usability, demanded a balance between strong security measures and ease of user access, challenging us to prioritize elements that could significantly impact daily convenience and safety.

The third scenario, innovation versus regulation, required a thoughtful analysis of the benefits and dangers of unrestricted technological advancements.