

Reflection on Ethics & Career Application

Nicholas Dorsey

Old Dominion University

Professor Nathan Nicol

PHIL 355E: Cybersecurity Ethics

05 Aug 2025

This course has reshaped the way I see my future role in cybersecurity as I want and intend on becoming an ethical hacker or penetration tester. I came in thinking that being an ethical hacker or penetration tester was mostly about technical skills, finding vulnerabilities, writing reports, and handing them off. What I didn't expect was how much ethics, responsibility, and decision-making would be part of the job. Three lessons in particular stand out to me, and they're ones I know I'll carry with me throughout my career.

The first takeaway is that legality and morality or being ethically correct are not always the same thing. Early in the semester, we discussed scenarios where actions might be fully legal but still questionable from an ethical standpoint. That stood out a lot to me. In cybersecurity, I'll be working in spaces where I might be asked to do something that's within the law but still feels wrong, maybe because it violates user trust or exploits a loophole at someone's expense. On the flip side, there may be times where doing the right thing could technically cross a legal line, like certain forms of security research. This changed how I think about my possible role, not just as someone who follows the rules, but as someone who weighs the impact of my choices on real people and acts with integrity even when the law isn't enough of a guide.

Thinking about this in terms of my future work, I know there will be moments where I have to make judgment calls quickly. It's easy to imagine a penetration test where I find a vulnerability that could be exploited in ways my client never considered. Technically, my contract might not require me to report certain types of findings, but ethically, hiding them could put people at risk. The lesson I'm taking with me is to always consider not just the rules, but the bigger picture and the potential harm or benefit to others.

My second takeaway is about loyalty in the workplace. I used to think loyalty meant sticking by your boss, leadership, and co-workers. Now I see it differently. True loyalty in a professional sense is to the mission and objectives of the organization, not the individuals running it. Leaders can make mistakes, act out of self-interest, or even push for decisions that go against the organization's values. As a cybersecurity professional, my responsibility will be to the purpose I serve, protecting systems, data, and people, not to any one person's agenda.

This shift in perspective will help me stay grounded. I've seen firsthand in other jobs how personal loyalties and office politics can lead people to make decisions that harm the overall mission. In cybersecurity, that kind of misplaced loyalty could have huge consequences, from data breaches to loss of public trust. By focusing on the mission, I can keep my work aligned with the core goals of the organization, even if that means disagreeing with a superior.

The third takeaway is about whistleblowing. Before this class, I'll admit I mostly saw whistleblowers as people who "turned" on their organization. I didn't think much about their motivations or the bigger picture. Now I see that whistleblowing can be an act of accountability, and sometimes it's the only way to bring unethical practices to light. In cybersecurity, where the stakes involve sensitive data, national security, and public trust, being willing to speak up when something is wrong is critical.

Whistleblowers aren't always traitors, they can be protectors of the very values an organization claims to stand for. That shift in perspective makes me more aware of my own

responsibility to act if I see harm being done, especially in a field where silence can let damage grow. If a company is hiding a serious vulnerability or misleading the public about a breach, remaining quiet might protect my position, but it would betray the people who rely on the organization to keep their data safe.

These three lessons connect in a powerful way: they're all about responsibility, responsibility to people, to principles, and to truth. As I move toward a career as an ethical hacker or penetration tester, I know my technical skills will be important, but my ethical judgment will matter just as much. Whether it's questioning if a request is truly right, staying loyal to the mission instead of individuals, or speaking up when something is wrong, these are the guideposts I'll use to navigate my career. Cybersecurity is about more than code and vulnerabilities, it's about protecting what matters, and these takeaways will help me do that with integrity.

Looking ahead, I plan to integrate these lessons into my professional development. I want to be the kind of cybersecurity expert who can be trusted not only for technical expertise, but for fairness, honesty, and moral clarity. In an industry where threats are constantly evolving and the pressure to act fast can lead to shortcuts, I believe these principles will set me apart. They are not just things I learned for a class, they're values I hope and intend to live by.