**Cybersecurity Ethics in Software Engineering**  
Joshua Farrell  
CSU Global  
 CSC502: Ethical Leadership in Software Development  
Dr. Shaher Daoud  
 2025

#### 

**Cybersecurity Ethics in Software Engineering**

Firewalls, encryption, and detection are important to cybersecurity but one mistake from a human can bring it all down. Cybersecurity isn’t just about advanced computational methods and state-of-the-art anti-criminal techniques. People still have to use them. Software engineers must keep this in mind when building features as even the strongest walls have a weakest point. User design, communication, and accountability are key areas to improve when looking at building stronger cybersecurity in software engineering.

Responsibility is a glaring issue in this relationship. Most leaks or breaches happen when someone clicks a phishing link or reuses the same password everywhere. Tambe Jagtap (2023) found that even after training, people still fell for phishing attempts. Mistakes can be reduced by deploying AI monitoring and catching mistakes before they get to users. Developers should heed this insight and design systems that prevent as much user error as possible, ethically shifting the responsibility to the engineer and off of the user.

Training is a very important step in cybersecurity implementation strategy. Grobler et al. (2021) says that most training is done in a bland and boring manner full of jargon that is easily forgettable. In my personal experience, I was sat in front of laptops and was told to watch the videos at the beginning of jobs and the videos were never to be spoken of again. If the videos were funnier, more memorable, or if there were consequences for misclicking links, businesses could save hundreds to hundreds of millions of dollars.

People also react to risks differently. Alshaikh et al. (2021) says that personality traits, age of user, and technology skills all affect security risks differently. Engineers shouldn’t assume their systems will affect all users similarly. They must build in parameters that account for malleability in human behavior. Not all users are the same. A sixty year old user at a company will react differently to a 25 year old user. These points should be taken into account when dealing ethically with cybersecurity threats in software engineering.

Culture also plays a large part. Companies will often blame a user when they click a bad link. Was it the user’s fault or did the system set them up for failure? Nurgalieva et al. (2023) talk about human-focused cybersecurity. These systems help support the users instead of making things harder. Ethical engineering would ask what systems were in place during a breach and how they could be improved so that a user avoids a mistake. The more effort put into systems that account for a wide variety of users, the stronger a company’s security can be.

**My Take on the Human Side of Security**

In my view, cybersecurity and software development need to treat users as people and not as problems. Humans are not infallible. It is up to software engineers to account for this risk when building systems just as much as any other risk. Thinking through design, training, and communication will inevitably decrease risk. Simple and important questions should be asked. Is it easy for the user to succeed? Is being secure top-of-mind for the user?

Trust is a major factor in software development and cybersecurity..When a person uses a program, they trust that the program will help them and not do them harm. When engineers build tools that are safe and easy to use, they take responsibility and help the world.

Another step forward would be in partnerships between cyber teams and developers. If they get together and think from the perspective of an attacker, they can discover meaningful pain points to address. What if there was an app that highlights and explains why a risk is dangerous or explains the repercussions of a risky click? This would absolutely reduce risky clicks and teach a cautious approach.

**Conclusion**

Cybersecurity is not just an extra layer of protection but a shared responsibility between all parties. The responsibility, though, starts at the code writing. When software engineers develop ethical programs and take responsibility for their code, it is safer for users, companies, and ultimately society as a whole.

**References**

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2021). User characteristics that influence judgment of social engineering attacks in a BYOD setting. *Computers and Security, 103*, 102189. https://www.researchgate.net/publication/323455755\_User\_characteristics\_that\_influence\_judgment\_of\_social\_engineering\_attacks\_in\_social\_networks

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cybersecurity. *Frontiers in Big Data, 4*, 583723. https://www.researchgate.net/publication/349959811\_User\_Usage\_and\_Usability\_Redefining\_Human\_Centric\_Cyber\_Security

Nurgalieva, L., Malik, B., Nugmanov, R., Iliyasov, D., & Ataniyazova, Z. (2023). Human centric cybersecurity: Understanding and mitigating human error in digital systems. *International Journal of Cybersecurity Intelligence and Cybercrime, 6*(2), 53–59.  
https://www.researchgate.net/publication/385685188\_Human-Centric\_Cybersecurity\_Understanding\_and\_Mitigating\_the\_Role\_of\_Human\_Error\_in\_Cyber\_Incidents

Tambe Jagtap, V. (2023). A systematic review of current cybersecurity training methods. *IEEE Transactions on Learning Technologies*. https://www.researchgate.net/publication/385685188\_Human-Centric\_Cybersecurity\_Understanding\_and\_Mitigating\_the\_Role\_of\_Human\_Error\_in\_Cyber\_Incidents