Ethics in Cybersecurity

Ethics in Cybersecurity

In security, new technologies present new challenges. For every new security incident or risk, the right or wrong decision isn't always clear.

For example, imagine that you're working as an entry-level security analyst and you have received a high risk alert. You investigate the alert and discover data has been transferred without authorization.

You work diligently to identify who made the transfer and discover it is one of your friends from work. What do you do?

Ethically, as a security professional, your job is to remain unbiased and maintain security and confidentiality.

While it's normal to want to protect a friend, regardless of who the user in question may be, your responsibility and obligation is to adhere to the policies and protocols you've been trained to follow. In many cases, security teams are entrusted with greater access to data and information than other employees. Security professionals must respect that privilege and act ethically at all times.

Security ethics are guidelines for making appropriate decisions as a security professional. As another example, if you as an analyst have the ability to grant yourself access to payroll data and can give yourself a raise, just because you have access to do so, does that mean you should? The answer is no. You should never abuse the access you've been granted and entrusted with.

Let's discuss ethical principles that may raise questions as you navigate solutions for mitigating risks. These are confidentiality, privacy protections, and laws.

Let's begin with the first ethical principle, confidentiality. Earlier we discussed confidentiality as part of the CIA triad. Now let's discuss how confidentiality can be applied to ethics. As a security professional, you'll encounter proprietary or private information, such as PII. It's your ethical duty to keep that information confidential and safe. For example, you may want to help out a coworker by providing computer system access outside of properly documented channels. However, this ethical violation can result in serious consequences, including reprimands, the loss of your professional reputation, and legal repercussions for both you and your friend.
\
The second ethical principle to consider is privacy protections. Privacy protection means safeguarding personal information from unauthorized use. For example, imagine you receive a personal email after hours from your manager requesting a colleague's home phone number. Your manager explains that they can't access the employee database at the moment, but they need to discuss an urgent matter with that person.

As a security analyst, your role is to follow the policies and procedures of your company, which in this example, state that employee information is stored in a secure database and should never be accessed or shared in any other format. So, accessing and sharing the employee's personal information would be unethical. In situations like this, it can be difficult to know what to do. So, the best response is to adhere to the policies and procedures set by your organization.

A third important ethical principle we must discuss is the law. Laws are rules that are recognized by a community and enforced by a governing entity.

For example, consider a staff member at a hospital who has been trained to handle PII, and SPII for compliance. The staff member has files with confidential data that should never be left unsupervised, but the staff member is late for a meeting. Instead of locking the files in a designated area, the files are left on the staff member's desk, unsupervised. Upon the employee's return, the files are missing. The staff member has just violated multiple compliance regulations, and their actions were unethical and illegal, since their negligence has likely resulted in the loss of private patient and hospital data.

As you enter the security field, remember that technology is constantly evolving, and so are attackers' tactics and techniques. Because of this, security professionals must continue to think critically about how to respond to attacks.

Having a strong sense of ethics can guide your decisions to ensure that the proper processes and procedures are followed to mitigate these continually evolving risks.

Ethical concepts that guide cybersecurity decisions

Previously, you were introduced to the concept of security ethics. **Security ethics** are guidelines for making appropriate decisions as a security professional. Being ethical requires that security professionals remain unbiased and maintain the security and confidentiality of private data. Having a strong sense of ethics can help you navigate your decisions as a cybersecurity professional so you're able to mitigate threats posed by threat actors' constantly evolving tactics and techniques. In this reading, you'll learn about more ethical concepts that are essential to know so you can make appropriate decisions about how to legally and ethically respond to attacks in a way that protects organizations and people alike.

Ethical concerns and laws related to counterattacks

United States standpoint on counterattacks

In the U.S., deploying a counterattack on a threat actor is illegal because of laws like the Computer Fraud and Abuse Act of 1986 and the Cybersecurity Information Sharing Act of 2015, among others. You can only defend. The act of counterattacking in the U.S. is perceived as an act of vigilantism. A vigilante is a person who is not a member of law enforcement who decides to stop a crime on their own. And because threat actors are criminals, counterattacks can lead to further escalation of the attack, which can cause even more damage and harm. Lastly, if the threat actor in question is a state-sponsored hacktivist, a counterattack can lead to serious international implications. A **hacktivist** is a person who uses hacking to achieve a political goal. The political goal may be to promote social change or civil disobedience.

For these reasons, the only individuals in the U.S. who are allowed to counterattack are approved employees of the federal government or military personnel.

International standpoint on counterattacks

The International Court of Justice (ICJ), which updates its guidance regularly, states that a person or group can counterattack if:

- The counterattack will only affect the party that attacked first.
- The counterattack is a direct communication asking the initial attacker to stop.
- The counterattack does not escalate the situation.
- The counterattack effects can be reversed.

Organizations typically do not counterattack because the above scenarios and parameters are hard to measure. There is a lot of uncertainty dictating what is and is not lawful, and at times negative outcomes are very difficult to control. Counterattack actions generally lead to a worse outcome, especially when you are not an experienced professional in the field.

To learn more about specific scenarios and ethical concerns from an international perspective, review updates provided in the “Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations” or access the Tallinn Manual online.

Ethical principles and methodologies

Because counterattacks are generally disapproved of or illegal, the security realm has created frameworks and controls—such as the confidentiality, integrity, and availability (CIA) triad and others discussed earlier in the program—to address issues of confidentiality, privacy protections, and laws. To better understand the relationship between these issues and the ethical obligations of cybersecurity professionals, review the following key concepts as they relate to using ethics to protect organizations and the people they serve.

Confidentiality means that only authorized users can access specific assets or data. Confidentiality as it relates to professional ethics means that there needs to be a high level of

respect for privacy to safeguard private assets and data.

Privacy protection means safeguarding personal information from unauthorized use. Personally identifiable information (PII) and sensitive personally identifiable information (SPII) are types of personal data that can cause people harm if they are stolen. **PII** data is any information used to infer an individual's identity, like their name and phone number. **SPII** data is a specific type of PII that falls under stricter handling guidelines, including social security numbers and credit card numbers. To effectively safeguard PII and SPII data, security professionals hold an ethical obligation to secure private information, identify security vulnerabilities, manage organizational risks, and align security with business goals.

Laws are rules that are recognized by a community and enforced by a governing entity. As a security professional, you will have an ethical obligation to protect your organization, its internal infrastructure, and the people involved with the organization. To do this:

- You must remain unbiased and conduct your work honestly, responsibly, and with the highest respect for the law.
- Be transparent and just, and rely on evidence.
- Ensure that you are consistently invested in the work you are doing, so you can appropriately and ethically address issues that arise.
- Stay informed and strive to advance your skills, so you can contribute to the betterment of the cyber landscape.

As an example, consider the **Health Insurance Portability and Accountability Act (HIPAA)**, which is a U.S. federal law established to protect patients' health information, also known as PHI, or protected health information. This law prohibits patient information from being shared without their consent. So, as a security professional, you might help ensure that the organization you work for adheres to both its legal and ethical obligation to inform patients of a breach if their health care data is exposed.

Key takeaways

As a future security professional, ethics will play a large role in your daily work. Understanding ethics and laws will help you make the correct choices if and when you encounter a security threat or an incident that results in a breach.

Holly: The importance of ethics as a cybersecurity professional

Hi, I'm Holly and I'm a Cloud Security Architect with Google Cloud. At the beginning of my adult career, I sold hosiery while I was going to school. That led me into an opportunity to work in banking, which then led me into an opportunity to work in telecommunications. From there I managed to get myself into a security vendor and learn security. Part of the way that I was able to change from my original half of my tech career being a database administrator to getting into cybersecurity was through getting certificates like you're doing today. Those really helped me gain credibility with potential employers when I didn't have the experience in this particular field yet. Ethics are really the crux of cybersecurity, you need to be able to be ethical in all of your actions in order to be a cybersecurity professional. Examples of unethical behavior are usually honestly just slight laziness, people taking shortcuts and not really thinking about the consequences of their actions. So, certainly when people share passwords to systems or give out private information, or look into systems for their own personal information or purposes about people they know or about celebrities. One of the most difficult situations that I ever faced in my technology career related to ethics was shortly after 9/11, my boss's boss's boss came to me with a bunch of keywords that were clearly related to the attack in New York and asked me to query the database that I administered that had everybody's text messages in it for the entire telecommunications company without anything in writing and without a court order. I was in a very uncomfortable position to tell someone that much senior than me that I wasn't comfortable doing that. I suggested that he bring something in writing to me to do that and he found someone else who did it for him. When you're faced with one of these difficult decisions, it's good to think about what would be the consequences of your decision. My encouragement to those of you out here taking this program is that the rewards that you get from helping to protect your company or your users or your organization from cyber criminals is really great. We get to be the good guys and help protect our industry and our customers from cyber attacks and cyber criminals. That's rewarding.

Wrap-up

You are now better prepared to understand and help make decisions regarding assessing and managing risks. Let's review what we've covered.

We discussed security frameworks and controls and how they're used to develop processes and procedures that protect organizations and the people they serve. We also discussed core components of frameworks, such as identifying security goals and establishing guidelines to achieve those goals.

Then, we introduced specific frameworks and controls, including the CIA triad and the NIST CSF, and how they are used to manage risk.

And finally, we discussed security ethics, including common ethical issues to consider, such as confidentiality, privacy protections, and laws.

You're almost there, only one more section to go in this course. Coming up, you'll learn about common tools and programming languages used by security analysts to protect organizational operations. Hope you're as excited as I am to keep going!