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 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.