Lab - Create Your Personal Code of Ethical Conduct

Objectives

Part 1: Research Approaches to Ethical Decision Making

Part 2: Research Code of Ethics

Part 3: Develop Your Own Personal Code of Ethical Conduct

Background / Scenario

When confronted with an ethical dilemma, what do you consider when making a decision?

Suppose you find a new USB 3.0 flash drive in the computer lab, what would you do? A student in your class says they found a site on the internet that has all of the class exams and quizzes with answers, what would you do?

Working in Cybersecurity is not always about stopping cyber attacks. As a Cybersecurity specialist, your organization may entrust you with some of the most sensitive data. As a result, you will be confronted with challenging ethical dilemmas, which may not have an easy or clear answer. For example, when researching a security breach, are the personal devices of employees and their personal content included?

The focus of this lab is to research approaches or perspectives for ethical decision making. Next, you will research code of ethics and finally you will create your own personal code of ethical conduct.

Required Resources

- PC or mobile device with Internet access

Instructions

Part 1: Research Approaches to Ethical Decision Making

There are several approaches or perspectives on Ethical Decision Making, including Utilitarian ethics, the Rights approach and the Common Good approach. Other ethical decision models include the Fairness or Justice approach as well as the Virtue approach.

In this part, you will research each ethical decision model or framework and then formulate the underlying principle from that approach.

Use an internet browser to research approaches to ethical decision making.

Step 1: Research Utilitarian ethics

Define the underlying principle for the Utilitarian Ethics approach.

[Answer]

Underlying Principle - The Utilitarian approach focuses on maximizing the overall good. It advocates for decisions that produce the greatest benefit for the greatest number of people, even if it means sacrificing the interests of a few.

Answers will vary but should include on maximizing the greatest good for the most people.

Step 2: Research the Rights approach to ethical decision making.

Define the underlying principle for the Rights approach to ethical decision making.

[Answer]

Underlying Principle - The Rights approach emphasizes the respect for individual rights. It focuses on protecting the fundamental rights and freedoms of individuals, ensuring that no person is used as a means to an end, and treating people as ends in themselves.

Answers will vary but should include the fundamental rights of the individual and how we live our lives, as well as respecting others and how they live their lives.

Step 3: Research the Common Good approach to ethical decision making.

Define the underlying principle for the Common Good approach to ethical decision making.

[Answer]

Underlying Principle - The Common Good approach stresses that decisions should benefit the community as a whole. It promotes actions that serve the well-being of all, particularly those values and goals that are shared within a society, ensuring that the community thrives together.

Answers will vary but should include the focus of community. Individuals should pursue the values and goals shared by other members of the community.

Step 4: Research the Fairness or Justice approach to ethical decision making.

Define the underlying principle for the Fairness or Justice approach to ethical decision making.

[Answer]

Underlying Principle - The Fairness or Justice approach highlights the importance of equality and impartiality in decision-making. It seeks to ensure that outcomes are fair and just, avoiding favoritism or discrimination, and ensuring that similar cases are treated in the same way.

Answers will vary but should include the fairness of the outcome. Is the outcome equal for everyone? The outcome should not impose favoritism nor discrimination.

Part 2: Research Code of Ethics

Most organizations develop their own code of ethics. Developed by management, this document is based on values and principles to promote the company business with honesty and integrity.

In this part, you will research computer code of ethics and cybersecurity code of ethics.

Use an internet browser to research code of ethics.

Based on your research, create a list of at least ten items. The list should be sequential from most important to least important.

Answers will vary, but may include some of the items below:

1. **Information stored on the computer should be treated as seriously as written or spoken words.**
2. **Respect the privacy of others.**
3. **Creation and usage of malware is illegal and must not be practiced.**
4. **Should not prevent others from accessing public information.**
5. **Overwhelming other's system with unwanted information is unethical.**
6. **Sending inappropriate messages through email or chat is forbidden.**
7. **Do no harm with a computer**
8. **Comply with legal standards**
9. **Be trustworthy**
10. **Maintain confidentiality**

List of ten items for a computer and cybersecurity code of ethics, arranged from most important to least important:

1. Respect the privacy of others.

   Always respect the confidentiality of personal data and refrain from unauthorized access or sharing of information.

2. Do no harm with a computer.

   Avoid actions that can cause harm to individuals, organizations, or systems through the misuse of technology.

3. Information stored on computers should be treated as seriously as written or spoken words.

   Data integrity is critical. Misuse, distortion, or unauthorized dissemination of information should be avoided.

4. Creation and usage of malware is illegal and must not be practiced.

   Writing or distributing malicious software to cause harm or exploit vulnerabilities is unethical and illegal.

5. Comply with legal standards.

   Always adhere to laws governing the use of technology, data protection, and cybersecurity in all actions.

6. Be trustworthy.

   Maintain honesty and integrity in all technology-related activities, ensuring that you are reliable and truthful in your conduct.

7. Maintain confidentiality.

   Safeguard sensitive information and ensure that it is only accessible to authorized individuals.

8. Overwhelming others' systems with unwanted information (e.g., spamming or DDoS attacks) is unethical.

   Avoid intentional overloading of systems or sending unsolicited, harmful data that disrupts services.

9. Do not prevent others from accessing public information.

   Information intended for public access should remain freely available without undue restrictions or barriers.

10. Sending inappropriate messages through email or chat is forbidden.

    Refrain from transmitting offensive, harmful, or inappropriate content that could violate professional and personal ethics.

Part 3: Develop Your Own Personal Code of Ethical Conduct

A code of conduct provides guidelines for acceptable as well as unacceptable specific behaviors.

Based on your research, develop a list of your own personal code of ethical conduct.

Create a code of ethics list of at least ten items. The list should be sequential from most important to least important.

[Answer]

1. Do no harm with technology.

   I will never use a computer to intentionally harm individuals, organizations, or society.

2. Respect the privacy of others.

   I will respect the confidentiality and privacy of data belonging to others and never access it without proper authorization.

3. Do not interfere with others' work.

   I will not intentionally disrupt, interfere, or obstruct other people's work, data, or systems.

4. Never use technology to steal.

   I will not use technology for unauthorized access, theft of data, or exploitation of digital resources.

5. Be truthful in all digital interactions.

   I will always act with integrity, ensuring that I do not spread false information or misrepresent facts.

6. Respect intellectual property.

   I will not copy, distribute, or use proprietary software, data, or content without permission or proper compensation.

7. Do not misuse computer resources.

   I will not access or use computing resources without proper authorization or compensate for their usage when required.

8. Respect others' intellectual output.

   I will acknowledge and give credit to others for their work and ideas and never pass it off as my own.

9. Consider the social impact of technology.

   I will consider the societal, ethical, and moral implications of the software I develop or the systems I manage.

10. Promote fairness and equality.

    I will use technology in ways that promote fairness, equality, and respect for all individuals and communities.

Reflection Questions

1. Is there a Cyber Security incident you remember where the company acted ethically or the company acted un-ethically? Explain.

   [Answer]

   One notable cybersecurity incident in Indonesia where a company acted unethically was the **Tokopedia data breach in 2020**. Over 91 million users' personal data, including usernames, emails, and encrypted passwords, were leaked and sold on the dark web. While Tokopedia eventually forced a password reset and worked with authorities, the company initially downplayed the severity of the breach and delayed fully disclosing it to the public. This lack of transparency and the slow response to notify users put many at risk, raising concerns about the company's ethical responsibility in handling the breach.

   Answers will vary but may include Equifax data breach.

2. What is a weakness or drawback to Utilitarian Ethics?

   [Answer]

   A significant drawback of Utilitarian Ethics is its **disregard for individual rights**. In focusing on the greatest good for the majority, it may justify actions that infringe upon the rights or well-being of individuals or minority groups, which can lead to unfair outcomes.

   Answers will vary but may include the lack of fundamental individual rights.

3. Based on your list of code of ethics, which is the most challenging item in your list to implement?

   [Answer]

   The most challenging item to implement is **considering the social impact of technology**. As a cybersecurity specialist, it is difficult to predict all potential societal consequences of a system or program. Furthermore, decisions about public disclosure of incidents are often made at a higher organizational level, outside of the cybersecurity specialist's control.

   Answers will vary but may include those items that are out of the control of the cybersecurity specialist. Example when to notify the public of a security incident.