Nama : Rizqi Hendra Ardiansyah
Kelas : SIB-4C
NIM : 2141762145
No.Absen : 11

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.

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.

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.

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.

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.

1. Protect Privacy – Ensure the confidentiality of sensitive personal and organizational data.
2. Do No Harm – Avoid actions that can harm individuals, organizations, or the public.
3. Maintain Integrity – Be honest and truthful in all professional activities.
4. Protect Systems and Networks – Ensure the security of systems and networks against unauthorized access or breaches.
5. Respect Intellectual Property – Do not use or distribute copyrighted software or data without permission.
6. Avoid Conflicts of Interest – Avoid situations that may lead to bias or personal gain at the expense of professional responsibilities.
7. Be Transparent – Disclose known security risks and vulnerabilities promptly and accurately.
8. Avoid Misuse of Privileges – Do not exploit your access to systems and data for unauthorized purposes.

9. Comply with Laws and Regulations – Follow all relevant legal and regulatory requirements, including cybersecurity laws.
10. Commit to Continuous Improvement – Continuously update skills and knowledge to adapt to evolving security threats.

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

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.

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.

Question:

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

1. Thou shalt act with integrity and honesty in all computing practices.
2. Thou shalt respect the privacy and confidentiality of others information.
3. Thou shalt ensure that all actions taken with technology are legal and ethical.
4. Thou shalt not use technology to cause harm or damage to individuals or systems.
5. Thou shalt protect and preserve the confidentiality of proprietary and sensitive information.
6. Thou shalt seek proper authorization before accessing or using others digital resources.
7. Thou shalt not plagiarize or misuse intellectual property and creations of others.
8. Thou shalt be mindful of the impact of technological decisions on society and the environment.
9. Thou shalt respect and follow guidelines and policies established by organizations and institutions.
10. Thou shalt continuously strive to improve and update one's skills and knowledge in ethical computing

Answers will vary but may include the ten commandments below.

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid (without permission).
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for other humans

Reflection Questions

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

   One example of a **company acting ethically** during a cybersecurity incident is **Mozilla's response to the Heartbleed vulnerability** in 2014. Heartbleed was a major bug in the OpenSSL cryptographic software library that allowed attackers to read sensitive data from servers, such as passwords and private keys. Upon discovering the vulnerability, Mozilla quickly issued security updates for Firefox and its other services. In addition to patching the issue, Mozilla was transparent with users about the vulnerability, encouraged them to change their passwords, and provided guidance on how to secure their systems. The company's quick response, communication with its users, and commitment to transparency exemplified ethical behavior in handling the incident.

   On the flip side, an example of a company acting **unethically** occurred in **Uber's 2016 data breach**. Hackers gained access to the personal information of 57 million riders and drivers. Instead of disclosing the breach promptly, Uber paid the hackers $100,000 to cover it up and concealed the incident for over a year. The company even failed to notify affected individuals and regulators, which is required by law in many jurisdictions. This cover-up was revealed in 2017, leading to public outrage and legal consequences. Uber’s actions were widely criticized as unethical, particularly because it prioritized its reputation over the safety and privacy of its users. These two incidents show how ethical and unethical responses to cybersecurity breaches can have a lasting impact on a company's reputation and trust with its users.

   Answers will vary but may include Equifax data breach.

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

   A significant weakness or drawback of **Utilitarian ethics** is that it can lead to **moral compromises** by justifying actions that harm individuals or minority groups if doing so leads to a greater overall benefit. This "ends justify the means" approach can allow for ethically questionable actions, as long as the result maximizes happiness or reduces suffering for the majority.

   For example, under strict utilitarian reasoning, it could be considered acceptable to sacrifice the well-being or rights of a few people if doing so benefits a larger number of others. This can result in the **neglect of individual rights** and justice for minorities, as utilitarianism focuses on aggregate outcomes rather than fairness for each person.

   In essence, **utilitarianism risks undermining individual rights**, as it does not inherently prioritize protecting individuals from harm if it leads to a perceived greater good. This can be problematic in situations where ethical considerations need to balance both the collective good and the rights and dignity of each person..

   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?

   The most challenging item to implement in a code of ethics, based on the principles often emphasized in ethical frameworks, is **balancing transparency with confidentiality**. While transparency is key to fostering trust and accountability, there are situations where maintaining confidentiality is essential to protect privacy, security, or sensitive information. For instance, in the field of cybersecurity, being transparent about breaches or vulnerabilities is ethically important to keep stakeholders informed and allow them to protect themselves. However, full disclosure might also expose vulnerabilities to malicious actors, putting systems and data at greater risk. Striking the right balance between being open and protecting confidential information can be a complex, context-dependent decision that often presents ethical dilemmas.This tension between transparency and confidentiality requires careful consideration of the potential consequences, making it one of the most difficult ethical principles to consistently apply in real-world scenarios.

   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.