Name: Jiyad Khan Roll #: 19I-1771 Case #: 6 Date: 29/03/2023

**A Four-Step Analysis Process for Ethical Dilemma**

**Step I. Understanding the situation**

A. List and number the relevant facts.

**Number Fact**

1. The IT manager at a bank discovers that one of the tellers has been accessing customer accounts without authorization.
2. The IT manager informs the teller's supervisor and the bank's security officer.
3. The bank's security officer decides not to take any action because he believes the teller is a valuable employee and that the IT manager is overreacting.
4. The IT manager disagrees with the security officer's decision and reports the incident to his own supervisor.
5. The IT manager's supervisor tells him to drop the matter and not to go over the security officer's head.
6. The IT manager feels pressured to keep quiet and decides not to pursue the matter any further.

B. Which of these raises an ethical issue? Why? What is the potential or resulting harm?

Fact (number) Potential or resulting harm

1. Privacy violations of the customers whose accounts were access without authorization.
2. None
3. Failure to take appropriate action in response to a security breach.
4. None
5. Failure to take appropriate action in response to a security breach.
6. Failure to take appropriate action in response to a security breach.

C. List the stakeholders involved.

* The company's IT department
* The company's management team
* The company's employees
* The customers using the company's online service
* The government agencies responsible for regulating the industry
* The privacy advocates and organizations concerned with protecting personal information
* The shareholders of the company
* The company's competitors
* The media and public opinion
* The individual whose personal information was compromised in the data breach.

**Step II. Isolating the major ethical dilemma**

What is the ethical dilemma to be resolved NOW?

State it using the form: Should **someone** do or not do **something**? Note: Just state the dilemma here; leave any reasoning for Step III.

Should the IT employee report the security breach, even though it may result in negative consequences for the company and potentially harm the company's reputation?

**Step III. Analyzing the ethicality of both alternatives in Step II**

**Consequentialism**

1. If action in Step II is done, who, if anyone, will be harmed? The company may suffer financial losses due to legal action, damage to its reputation, and loss of customer trust.
2. If action in Step II is not done, who, if anyone, will be harmed? It could lead to further security breaches and the potential harm to individuals whose data is compromised.
3. Which alternative results in the least harm, A or B? [✔ ] A [ ] B
4. If action in Step II is done, who, if anyone, will benefit? It will benefit the company's stakeholders and potentially the general public, as they will be made aware of the security breach and the company can take steps to mitigate the damage caused by it.
5. If action in Step II is not done, who, if anyone, will benefit? It could benefit the company in the short term by avoiding negative publicity and damage to its reputation.
6. Which alternative results in the maximum benefit, D or E? [✔ ] D [ ] E

**Right and Duties**

G. What **rights** have been or may be abridged? What **duties** have been or may be neglected? Identify the stakeholder and the right or duty. When listing a right, show its corresponding duty and vice versa.

|  |  |  |
| --- | --- | --- |
| **Stakeholder** | **Right** | **Corresponding Duty** |
| IT Employee | Right to protect the company's information assets and maintain the confidentiality of sensitive information | Duty to report security breaches and protect the company's assets from potential harm |
| Company | Right to maintain its reputation and financial stability | Duty to address security breaches and take appropriate action to mitigate potential harm to its assets and reputation |
| Customers and clients | Right to have their personal and sensitive information protected | Expectation that the company will fulfill its duty to protect their information from security breaches |
| Regulators and legal authorities | Right to enforce compliance with regulations and laws related to data privacy and security | Duty to investigate security breaches and hold companies accountable for any noncompliance |

**Kant’s Categorical Imperative**

1. If action in Step II is done, who, if anyone, will be treated with disrespect? IT employee may be perceived as disloyal or untrustworthy by their colleagues and superiors who prioritize the company's reputation over ethical principles.
2. If action in Step II is not done, who, if anyone, will be treated with disrespect? IT employee chooses not to report the breach, they may be disrespecting their own values and the trust placed in them by the company and its stakeholders.
3. Which alternative is preferable, H or I? [✔ ] H [ ] I
4. If action in Step II is done, who, if anyone, will be treated unlike others? IT employee may be treated differently from other employees in the company.
5. If action in Step II is not done, who, if anyone will be treated unlike others? IT employee may be going against their ethical obligations to protect the company's data and may be enabling further breaches and potentially harming the company in the long run.
6. Which alternative is preferable, K or L? [ ] K [✔ ] L
7. Are there benefits if everyone did action in Step II? Yes, it would benefit organizations as a whole. Individuals can better understand the core issue at hand and make informed decisions that align with ethical principles and values. This can lead to better decision making, improved organizational ethics, and increased trust and credibility with stakeholders.
8. Are there benefits if nobody did action in Step II? No, there may be potential benefits for the company in the short term, such as avoiding negative publicity or financial losses. However, in the long term, the company may face greater risks and consequences if the security breach is not addressed. These risks could include further breaches, loss of customer trust, legal liability, and damage to the company's reputation.
9. Which alternative is preferable, N or O? [✔ ] N [ ] O

**Step IV. Making a decision and planning the implementation**

**A. Make a defensible ethical decision.**

**Based on the analysis in Step III, answer the question in Step II. Indicate the letters of the categories that best support your response. Add any arguments justifying your choice of these ethical principles to support your decision. Where there are conflicting rights and duties, choose and defend those that take precedence.**

Based on this scenario, my ethical decision is as follows:

**Decision:** The Company should not implement a system to monitor its employees' use of the internet without first addressing the employees' concerns and implementing adequate safeguards to protect their privacy.

**Ethical categories that support my decision:**

Privacy (P)

Responsibility (R)

**Argument:**

Privacy is a fundamental right that should not be violated without a compelling reason. While the company has legitimate reasons for wanting to monitor its employees' internet use, such monitoring could easily be abused if proper safeguards are not put in place. Employees have a reasonable expectation of privacy while using company computers, and this expectation should be respected.

Furthermore, the company has a responsibility to protect its employees' privacy and to address their concerns. The potential benefits of monitoring internet use must be balanced against the potential harms to employee morale, trust, and privacy. By taking the time to address employees' concerns and implement appropriate safeguards, the company can demonstrate its commitment to ethical conduct and responsible management.

Therefore, I believe that the ethical principles of Privacy and Responsibility take precedence in this situation, and that the company should not implement the monitoring system until these principles are adequately addressed.

**B. List the specific steps needed to implement your defensible ethical decision.**

The following steps can be taken to implement a defensible ethical decision in IT, specifically for Case 6:

1. **Identify the ethical issue:** The first step is to clearly identify the ethical issue in Case 6, which involves a software developer who has discovered a major security flaw in a company's product but has been ordered not to disclose it to customers.
2. **Gather relevant information:** Next, gather all relevant information related to the ethical issue. This includes company policies, legal regulations, and professional codes of conduct, as well as any other information that may be relevant to the situation.
3. **Identify stakeholders:** Identify all stakeholders who may be affected by the decision, including customers, employees, shareholders, and the developer himself.
4. **Evaluate options**: Evaluate all possible options for addressing the ethical issue. This may include reporting the security flaw to a regulatory agency, reporting the flaw to the company's management, or keeping the flaw confidential.
5. **Consider consequences:** Consider the consequences of each option, including the potential impact on stakeholders, legal and financial consequences, and potential harm to the developer's career.
6. **Choose a course of action:** Choose the option that is most likely to result in the best overall outcome for all stakeholders involved.
7. **Implement the decision**: Implement the chosen course of action, including any necessary communication with relevant parties, such as the company's management or regulatory agencies.
8. **Reflect on the decision:** After implementing the decision, reflect on the process and outcome to identify any areas for improvement in future ethical decision-making situations.

By following these steps, the software developer in Case 6 can make a defensible ethical decision that takes into account all relevant information and stakeholders.

**C. Show how the major stakeholders are affected by these actions.**

The major stakeholders in this case and how they are affected by the actions taken by the IT manager are as follows:

**The IT Manager:** The IT manager is responsible for identifying the security flaw in the network and determining whether or not to inform the CEO. The decision made by the IT manager will have a significant impact on their career, as well as their reputation within the company. If the IT manager chooses to inform the CEO about the security flaw, they may be viewed as a whistleblower, which could have negative consequences for their career. However, if the IT manager chooses not to inform the CEO, they could be seen as neglecting their duty and jeopardizing the security of the company.

**The CEO:** The CEO is responsible for the overall management of the company and making decisions that impact the company's success. If the IT manager informs the CEO about the security flaw, the CEO will need to decide how to address the issue. If the CEO decides to take action, it could result in significant financial costs for the company, as well as damage to the company's reputation. If the CEO does not take action and the security flaw is exploited, it could result in significant financial and reputational damage to the company.

**The Customers:** The customers of the company rely on the company to protect their personal and financial information. If the security flaw is exploited, it could result in the loss of customer data, which could lead to identity theft and other forms of fraud. This could result in significant financial and reputational damage to the customers.

**The Shareholders:** The shareholders of the company invest in the company with the expectation of receiving a return on their investment. If the security flaw is exploited, it could result in a significant decline in the company's stock price, which could negatively impact the shareholders' investments.

**The Employees:** The employees of the company rely on the company for their livelihood. If the security flaw is exploited, it could result in the loss of customer data, financial losses, and damage to the company's reputation, which could lead to layoffs or other negative consequences for the employees.

**D. What other longer-term changes (political, legal, technical, societal, organizational) would help prevent such problems in the future?**

The following are some longer-term changes that could help prevent such problems in the future:

**Legislative action:** Governments could pass laws that make it illegal to send unsolicited emails or messages, or to collect and use personal information without consent. Such laws would need to be enforced and penalties imposed to deter violators.

**Technical measures:** Software companies could develop more sophisticated spam filters and firewalls to prevent unwanted messages and block spam at the source. Additionally, they could also develop tools to help users control their privacy settings and restrict the use of their personal data.

**Societal changes:** Educating the public about the dangers of spam and how to avoid it could help to reduce its prevalence. For example, individuals could be taught to recognize phishing scams and how to protect their personal information online.

**Organizational changes:** Companies could implement policies and procedures to prevent spam, such as prohibiting the use of company email accounts for unsolicited messages or requiring employees to complete training on cybersecurity and privacy practices.

**International collaboration:** Spam is a global problem, and international cooperation may be necessary to address it effectively. Governments, industry groups, and individuals could work together to share information and best practices, and to develop a coordinated approach to combating spam.

**E. What should have been done or not done in the first place (at the pivot point) to avoid this dilemma?**

To avoid this dilemma, several actions could have been taken at the pivot point:

**Thoroughly vetting third-party software vendors:** Before purchasing software from a third-party vendor, it is important to conduct a thorough evaluation of the vendor's reputation, experience, and track record. This can include researching the vendor online, seeking references, and conducting interviews.

**Conducting comprehensive testing:** It is essential to thoroughly test software before deploying it in a production environment. This can include functional testing, security testing, and performance testing. Comprehensive testing can help identify any bugs or vulnerabilities that may exist in the software.

**Negotiating clear contractual terms:** When purchasing software from a third-party vendor, it is important to negotiate clear contractual terms that address issues such as bug fixes, software updates, and liability in the event of a security breach. These terms should be agreed upon before any software is deployed.

**Maintaining ongoing communication with the vendor:** IT professionals should maintain ongoing communication with third-party vendors to ensure that they are aware of any issues or concerns related to the software. This can include regular meetings, status updates, and ongoing testing.