The Hong Kong Polytechnic University

ENG3004

Society and the Engineer

Assignment 1

Cheng Ka Hei

22033044D

17/02/2022

First of all, as an engineer, we have a well-established principle: having the responsibility of loyalty to our clients and employers. We are required to preserve the confidentiality of information. This information is mainly about the business, how to run it, and the information on its services and products. It would directly affect the company's ability to compete in the marketplace.

Besties, this information seems non-valuable for the public and would not interest them in general. However, this information is precious for the culprit. For example, the information about the development project is valuable to the contractor as if they know the project details before the invitation and can develop strategies to win the bid. It is unfair to another contractor. The culprit would try to bribe the engineer who obtained the information, getting the information before the formal invitation. Then, they get profit by selling the information to the contractor.

In addition, the culprit would not only aim to leak confidential information on potential projects and tender information to profit but also steal the product design from other companies to get income. The product design belongs to confidential information, which affects the company's competition in the marketplace. Releasing produce needs a long time to develop and involves a lot of money. The culprit would steal the design and sell it to another company. That company would save colossal money to develop the design and easily beat the original company. The orange company may go bankrupt if that product is their main product.

Although the culprits' methods are breeding like flies, the company can still protect itself. There are three categories to ensure that the employee handles privileged information correctly.

The first category is the implement proper access control. Information classifying is the first step toward privileged information being appropriately handled. The company's privileged information should be classified into different security groups based on its risk exposure and degree of sensitivity. For example, a company's product design should be classified into the most intimate security group, and only the high-class and relevant employees can assess it. On the contrary, information like staff roster and company building map can be classified into low-security risk groups, meaning that most employees can assess. Meanwhile, the

company should regularly review the classification to prevent some leaks. Therefore, the risk of privileged information exposure will decrease.
In addition, by assessing rights in directory management company can practice the need-to-know principle. The information should be assessed by the user whose job function is required. The different roles should have different access right. For example, a product engineer, a tester, and a mechanic are involved in product design. The access right of the engineer should be higher than the tester and mechanic. He/she may have access to information like the product's design and the product's code.
On the contrary, the tester and the mechanic should have the low access right. The tester only needs to know what he/she tests and how to write a report to the engineer. The mechanic only needs to maintain the product and which tool should he/she use, but not the product's design. Therefore, role-based access would practice the need-to-know principle.

Without flexible identity management, the need-to-know principle will be a virtually impossible fantasy. In a company, the roles change frequently, and it is necessary that keep authorizations up-to-date with flexible and automated identity management at all times to ensure every employee in the company is being managed in the system. Therefore, the leak would be erased.

The second category is monitoring the release of information. Providing clear guidelines is an ingredient in the recipe for information release monitoring. The company should clearly state how to keep information safe and handle the release of classified information in the guideline. For example, the information can only be kept on the hard drive the company certified. The personal data storage device is not allowed to keep the privileged information. The punishment of guideline violation is necessary, such as civil claim and criminal procedure, as deterrence is helpful to avoid mistakes.

Computer security should be ensured lest the attack of the hacker. As stated above, the culprit would steal and sell the sensitive information to get profit. If this information is released, it will harm the company competing in the marketplace. So that computer security should not be ignored company, the company should appoint an IT security engineer to raise the computer security level to avoid hacker attacks. At the same time, the company should limit the employee websites that are not allowed to browse through the company computer and Wi-Fi, lest the data be stolen and hacked.

Moreover, the monitor release information should be according to the need-to-know principle. That means this information still needs to handle by different assess right. For example, the decision on a product design release should be made by the senior management or the board of directors. Then, public relations get and release the information with permission. If the information decided not to release, neither the public relation nor other department staff would not have the right to access the information.

Meanwhile, the authorization of clients is essential. The company should obtain authorization before confidential information disclose if the information involves the clients. Thus, it can prevent unnecessary entanglement.

The third category is ensuring proper management controls. The company should communicate the policy clearly to all staff to preserve confidentiality. The company should inculcate the company's policy and punishment on all employees. Thus, the preservation awareness of employees would be raised. The more awareness the employee has, the more safety the confidentiality maintains. The company provides clear communication and reviews the policy regularly to minimize the risk effectively.

A prelude to the privileged information being appropriately handled by the employee is to require the employee to sign the agreement, which requires all employees not to leak and misuse the information either during employment or leave the company. By no means should employee leak and misuse proprietary information. Employees, who leak or abuse proprietary, have to assume serious consequences. The company should always alert the employee.

In conclusion, practicing these three categories can help the company realize that the employee handles privileged information appropriately.

Reference:

Sandmann, K. (2022, June 30). *The five stages of implementing the need-to-know principle*. VNClagoon. Retrieved February 17, 2023, from https://vnclagoon.com/need-to-know-principle/

Security: The need-to-know principle. TECHCOMMUNITY.MICROSOFT.COM. (2021, May 28). Retrieved February 17, 2023, from https://techcommunity.microsoft.com/t5/azure-sql-blog/security-the-need-to-know-principle/ba-p/2112393