ENG3004 - Individual Assignment 1

Student Name: Chan Ying Chik Student ID: 22031499D Date: 13/2/2023

Question:
Recommend how the company can make certain that the privileged information is handled properly by the employee?

The ex-employee Devine caused major losses to Apple due to the sale of Apple's important confidential information, such as new product forecasts, blueprints, prices and product features, and some of Apple's partners, suppliers and OEMs Provided data about Apple Inc. In return, Devine received financial benefits. Devine leaked Apple's confidential information, and the scheme to steal trade secrets enabled these suppliers and OEMs to better negotiate with Apple, ultimately costing Apple $2.409 million (Zhou, 2020).

Every company has its privacy, some are program software, some are food formula, or customer information. The business must address these issues, to prevent information leaks risks effectively, due to that could potentially use to competitors or criminals. Employees are supposed to maintain the confidentiality of information (whether or not it is considered proprietary) entrusted to them not only by the Company, but also by suppliers, customers and others related to the business. Once the company's information is disclosed by employees, not only the customers will be damaged, but the company's reputation will also be greatly reduced, people's confidence in the company will be reduced, cause people use the company's services less. Therefore, now I will recommend how the company can make certain that the privileged information is handled properly by the employee.

In my opinion, the first and most important thing that the privileged information can handled properly by the employee is the employee should sign a non-disclosure agreement, according to the Hong Kong Intellectual Property Exchange Center: "A non-disclosure agreement is a legally binding contract, which can also be called a non-disclosure agreement. The agreement stipulates that one party to the contract will disclose confidential information to the other party. For example, trade secrets and industrial knowledge, the party receiving the information must keep the information confidential and must not use such confidential information properly. Where one party discloses information to the other party, or both parties disclose information to each other, a non-disclosure agreement can be signed.” In general, where intellectual property rights, patented innovations, or commercial secrets are

involved, they will sign pertinent non-disclosure agreements when employing personnel, or when employees are participating in connected projects, to guarantee that their commercial secrets are not disclosed. Agree on the details of the confidentiality, including the content, parties accountable, the duration, the duties, and the consequences of a breach of the agreement. Alternatively, they can sign to a "non-competition agreement" that forbids them engage in business activities related to the company or in direct competition while they are employed and after resignation (Tse, 2020).

In May 2010, defendant Qi, in violation of the confidentiality agreement signed with Haier Group, illegally disclosed the important production data of Haier washing machines to a company in the same industry by email, and resigned from the post of director of the business department of Haier Group in July of that year. After serving as the deputy general manager of the above-mentioned company, the defendants Zhang Mou, Wang Mou, and Zhang Mou in this case illegally provided the above-mentioned company with important information about the production and procurement of Haier washing machines in July and October 2010. The commercial data caused a total of 29.5235 million yuan of direct economic losses to Haier Group. As can be seen, even with non-disclosure agreements, people still leak company information for some reason. Therefore, company should have some training for employees (Zhou, 2020).

The biggest risk of confidentiality information being leaked is frequently a company's own workers. This is frequently the result of inadequate training, which isn't always for malevolent motives. Employees can increase their security awareness by participating in "confidentiality knowledge training" as part of their induction training after successfully joining the company. This training emphasizes the value of information protection and states that no one has the right to alter, copy, download, or delete company materials. In order to avoid any malevolent revenge, businesses should also be aware of their employees' emotions, care about their everyday lives and jobs, and allow them to feel happy, trusted, and encouraged (Zhou, 2020).

For the training, you can have the option of doing internal training or contracting a third party organization to do so. if you need assistance with passwords, phishing, or other IT-related issues, professional guidance from an outside IT firm is a better choice.

Thirdly, control access. Commercial leaks are often through in email, electronic documents, and other network forms, and enterprise leak cases are closely related to data. As a result, the organization should set up a data protection mechanism, restrict who has access to confidential files, and set restrictions on what can be copied, downloaded, and deleted. When employees carry out unusual operations on files, the management will be notified right away by the system; the enterprise can also keep track of who has accessed what files in the past and determine whether any employees have ever viewed anything unrelated to their jobs.

For any information that's stored digitally it's incredibly important that you use passwords, firewalls, and encryption to restrict access. You must make sure that passwords are secure as well as frequently updated if you plan to use them to restrict access to sensitive data, combining upper- and lowercase letters with special characters is the best way to create passwords (Fraser, 2020).

Furthermore, the security of the shipment is crucial when sending confidential information to a different business or client. If a physical document needs to be delivered, it is better to utilize a reputable courier service or preferable, have someone you trust within your organization deliver it, such as a friend or a very senior employee.

You can send a digital document to a third party via email or a file-sharing application. You must ensure that the service provider you are utilizing is one you can trust if you utilize a file-sharing tool. Additionally, encrypted files are a wonderful option if you wish to have several layers of security (Fraser, 2020).

Moreover, using OneDrive or Cloud management is effective if all the documents are kept online, it is manageable. On the other hand, if there are any documents you need to keep on hand, the best course of action in this situation is to have lockable storage lockers that only you or senior management can access.

The lockable storage cabinets should be kept in a closed room and hard to find. That is inaccessible to everyone as an extra measure of security, only few select people have use to authority. Avoid information leakage due to contact with a large number of employees (Fraser, 2020).

After that, you can find that after using a locked locker to store secret information, there will be an increasing amount of paper confidential information and no place to

put fresh confidential papers. All you need to do is information management, throwing away some confidential documents that are no longer important or published. Instead of simply tossing documents in the garbage, you should use confidential waste bins and shredders. Despite how prevalent digital data has become, the majority of organizations still conduct a significant amount of daily paperwork. If you must discard sensitive documents, shred them or place them in a confidential garbage container. You should never believe that just because a document has been thrown away, it will not be seen by anybody else due to problems like identity theft.

However, it is advised to engage a reliable document destruction service provider if there are a lot of confidential papers. They can make sure that the paper is shredded into fragments that are so small and plentiful that it would be nearly hard to piece the information back together and put your business at jeopardy (Fraser, 2020).

Last but not least, when an employee leaves the organization, the company can comprehend the grounds for the resignation, the person's intended destination and career goals, and strive to come to an amicable agreement. After all, it may be some complaint or unhappiness when an employee resigns. In order to convey thanks for the employee's time spent working, the employer can now speak face-to-face with the departing employee. People may always be motivated by a superior's support, which can also improve the firm's reputation. Employees will not be upset about their future career growth opportunities and divulge corporate secrets.

Bain International, a well-known consulting business, has an "emotional investment" in departing workers. They have created a database specifically for resigned workers, put up a page for connecting with them, kept tabs on their career developments, and regularly update the resigned employee’s database. In the future, they also expect to have the chance to mend their working ties with departing staff (Zhou, 2020).

In conclusion, when managing confidential information of your company, whether it relates to clients or staff. If you don't make sure that data is safeguarded appropriately, your company's reputation will suffer and lose customers. As a result, you have a responsibility to take the required actions to safeguard it, such as use the ways that I say it above.

Reference

Zhou, J. (2020, July 6). *僱員離職=資料洩漏？企業如何保證內部信息/資產安全？: Champ partners*. Champ Partners Limited. Retrieved February 15, 2023, from https://www.champpartners.com/zh-hant/blog/how-to-safeguard-trade-secrets/

Tse, T. (2020, April 2). *保密協議（NDA）日漸普及 遭個別僱主濫用加入「不准講公司壞話」條款*. JobsDB Hong Kong. Retrieved February 15, 2023, from https://hk.jobsdb.com/en-hk/articles/%E7%94%9A%E9%BA%BC%E6%98%AF%E4%BF%9D%E5%AF%86%E5%8D%94%E8%AD%B0-nda-%E5%8D%94%E8%AD%B0%E6%97%A5%E6%BC%B8%E6%99%AE%E5%8F%8A-%E5%83%B1%E4%B8%BB%E5%8A%A0%E5%85%A5%E4%B8%8D%E5%90%8C%E6%A2%9D%E6%AC%BE/

Fraser, M. (2020, May 14). *5 top tips for handling confidential information in your business*. Grant McGregor Blog. Retrieved February 15, 2023, from https://blog.grantmcgregor.co.uk/2017/5-top-tips-for-handling-confidential-information-in-your-business