**Solutions against security breaches in Amazon Company**

**Recommendation Report summary and Problem statement:**

There are breaches found inside this company. These breaches are usually coming from inside the company because of the lack of professionalism of our employees. However, there are also breaches due to the security of our systems. Hackers have tried and sometimes succeeded in breaking into our security and stealing very important data.

Because of these attacks and infiltration, we are having a huge financial loss, it could cost almost 5 million dollars but most importantly the degradation of our business image and trust towards our customers leads to less collaboration.

**Description of our Solutions:**

The solution that seems the most logical would be to have a professional organization react and overview these attacks. There are several organizations that are specialized in fighting against cyber-attacks. They will be paid and therefore responsible for supervising the work. One of these organizations emphasizes that they are “Responsive and available, our expert’s team works in an emergency context to restore the security of your company.” In a company such as ours, it is vital to have these securities.

Amazon being a big company could also implement our own line of defense by assessing and implementing security controls. We could do this by creating a cyber security strategy, developing cyber security policies, conducting security risk assessments, and installing spam filters and anti-malware software. By doing all of these we are making sure to train our computer science workers to fight these attacks.

Finally, to help our employees keep the data that our company collects, it would be wise to implement a confidentiality clause. Indeed, “Confidentiality clauses are an important mechanism, not only to protect sensitive information that may give you an edge over your competitors but also to prevent employees from stealing your business information”

**Conclusion:**

To conclude, we firmly believe that the way to fight against those attacks is to either hire an external organization to supervise and fight against the attacks. Or we could set up our own defense by forming and teaching our computer scientists. To prevent the data from being stolen by employees, creating a confidential clause for each employee would help the company keep its promises to the customers.

**References:**

*Free it & cyber security policy templates for 2022*. PurpleSec. (2022, October 24). Retrieved November 2, 2022, from https://purplesec.us/resources/prevent-cyber-attacks/

*How to react in the event of a cyber-attack against my company?* How to react in the event of a cyber-attack? | Ziwit Incident Response. (n.d.). Retrieved November 2, 2022, from https://www.ziwit.com/en/incident-response

Yap, K. (2022, January 7). *Confidentiality clauses: What are they & how can you enforce them?* Sprintlaw. Retrieved November 2, 2022, from https://sprintlaw.com.au/articles/what-is-a-confidentiality-clause/