Best case study examples

Business, Company

Memo

Dear Law enforcers,

Here at Healthcare, Inc. we are deeply grieved and concerned about the recent incident whereby our digital healthcare records were hacked by an unknown person who posted the content in their own website. The invasion of our privacy is one of the worst criminal acts committed against our company in its history. The crime has left us as shocked as anyone else who expected us to maintain the highest standard of cyber/data security. We would therefore like to respond to your questions and show our position regarding to the incident. This will enable you to understand how competent and knowledgeable we are at what we do. We would like you to understand that we did everything within our ability to maintain privacy of our data and did nothing to provoke the incident. We also wish to provide necessary information to help you in your investigations. In order to ensure that we provide the necessary information, we promise that we will stick to what is required of us to provide.

First, we would like to refer to the specific scenarios in the case. Recently, our IT department was in its normal duties of reviewing our data for the purpose of our company operations when it realized an abnormal situation. Our new digital healthcare records were posted on the internet. The first step of our team was to report the matter to relevant security authorities in order to ensure that we comply with legal procedures of the case (Alexander, 2008). Of course, we didn’t want to pursue the criminals on our own without consulting relevant authorities because it would be tantamount to taking the law into our own hands. We then checked with all our employees to ensure

that all of them were not linked to the criminal act in any way. Although we may not conclusively argue that all our employees are not linked to the incident, we are confident that neither the employees nor the managers have any clue regarding to the crime. However, the information gathered from some of the employees and the management team may be important for you in pursuit of the criminals.

We understand that the offending company has gone offline. Going through the records of our employees and managers, we have determined that none of them has any links with the offending company. Furthermore, our company has been receiving several visitors to our premises including patients, partners, suppliers and government officials. All the visitors often provide their names and contacts in our visitor’s book. Among all visitors none has reportedly accessed our database center in the IT department. However, a few partners and agents including advertisers visited our IT personnel in their offices. They left without arriving at any agreement with our IT department who were planning to strike a partnership deal with the advertisers. The next meeting was scheduled for October 5, this year. Our team has called the advertisers since the crime occurred, and they are anticipating our meeting with them on October. That was the last time we met with any visitors of specific connection with the IT department.

Concerning the authenticity of our new digital healthcare records, we would like to indicate categorically that we followed the direction of the federal government when we acquired the new digital records. Last year, the federal government required the conversion to digital records. We complied with this requirement by converting our own system to the digital records. In fact, we

used a government-approved vendor for a no-bid installation of hardware and software to secure the digital records. The fact that the vendor we chose is approved by the government indicates that our new digital records were in good condition and met the required standards. For this reason, we recognize the fact that our company has not only faced a detrimental crime but has also been prevented from complying with the government's direction.

Our company is highly committed to meeting required standards and complying with the requirements of the law. By hacking our new digital records, the offending persons are preventing us from achieving our compliance goals and objectives. Furthermore, our operations have been also affected by the crime. The digital records contain a lot of information that is of significance to our strategic operations. Our clients have also been affected in that we cannot be able to meet their needs effectively without our data. The research and development department is also not able to meet its objectives because the data they need in their research and development activities were stored in the digital records. The fact that such information has been posted to another website for many people to see has a great impact on us. Our competitors will be able to read our strategic operations and use them against us in the highly competitive market. Criminals can also use the information to plan for their attack against us (Brenner, 2010). We do not feel secure and it will be our great happiness if the offenders will be prevented from committing further cyber crimes in the future.

We also understand that our services to the society are important for the success of both the society and us. We are committed to Corporate Social

Responsibility and ethics. In order to survive well in the market, we prioritize the welfare of our stakeholders including clients, creditors, suppliers and the community (Gadiesh & MacArthur, 2008). By not maintaining privacy, we risk revealing the secrets between us and our stakeholders. It is not in any way our plan to reveal the secrets of our stakeholders and we wish to maintain a good relationship with them. That is why we consider the malicious act committed against us as outrageous and unwelcome in our company's mission and activities. We understand that the community owes us the best services, and we can only achieve that through unquestionable privacy in our activities. Therefore, hacking our system just places us in the same position of a victim as our stakeholders. We apologize to our stakeholders and the public at large and we promise that we will do our best to collaborate with you in your investigation until the offenders have been identified and appropriate measures taken against them by the relevant authorities. We also hope that the information we have provided is helpful to you in your investigation.

Healthcare, Inc. Representative

References list

Alexander, P. (2008). Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers. Westport: Greenwood Pub. Group.

Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Santa Barbara, Calif: Praeger.

Gadiesh, O., & MacArthur, H. (2008). Lessons from private equity any company can use. Boston, Mass: Harvard Business School Press.