Essay on layered security plan

Business, Company

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Introduction

This is the intentional or unintentional release of some piece of secure information to a non-trusted environment. There are several incidents that can be grouped as part of the data breaches. Organized crimes, national governments and careless disposal of information are some of the major propagators of data breach. A data breach is an example of a security incident that leads sensitive and confidential data being leaked or transmitted to individuals who do not have the authority to access that piece of information or data. Data braches may involve personal credit card information or health records, trade secrets or intellectual property information being leaked to third parties. There were more than 220 million data breaches cases in the United States between 2005 and 2008. Some of these breaches are recorded in the Chronology of data breaches. In this study we are going to consider two security breaches that occurred in the health sector. They include:

i. Lawrence Memorial Hospital, Mid Continent Credit Servies, Inc. (Blue Sky Credit), BrickWire LLC Lawrence, Kansas MED DISC

In this case, the breach resulted into the exposure of personal information

belonging to different patients and health providers. Financial information belonging to patients who made their payments online was availed on the internet between September 20th 2011 and October 28th 2011.

ii. Los Angeles, California EDU PORT: November 4, 2011 UCLA Health System

Los Angeles

This breach resulted into a loss of external computer drives that contained personal information for the patients. This breach resulted into exposure of other sensitive information that belonged to different workers at the institution also.

There are several ways of controlling data breaches that are unique to the types of breaches encountered. However, there are some steps that are universal to most types of data breaches. The following is a six step procedure that can be followed in order to prevent such data breaches occurring:

1. Stop incursion by the targeted attacks

This can be achieved through shutting down all the avenues that hackers can use in order to gain access into a company’s resources. Core systems protection should be implemented so as to stop the hackers from exploiting system vulnerabilities.

2. Identify threats through correlating real-time alerts with global intelligence

This can be best achieved through allowing the security information system to flag any suspicious network activity for investigation. This can help in protecting the system from any kind of external attack before such attack is

carried out.

3. Protect information proactively

The system should be able to accurately identify sensitive information and proactively protect them wherever they are sent or stored. This can be achieved through using unified data protection policies across different servers used by the company.

4. Automate security through the use of IT compliance controls

Organizations have to enforce IT policies across their networks in order to control their networks and any piece of sensitive data within their systems. this will help in preventing sensitive information from being exposed to any unauthorized person.

5. Prevent data exfiltration

This involves using a mechanism to prevent further filtration of confidential data incase a hacking activity has been successful. This can be achieved through implementing a software solution that can take care of the data loss and prevent the leakage of sensitive information.

6. Integration of some prevention and response strategies into the security operations of the system.

This can be achieved through the implementation of a breach prevention plan and comeback plan that can be integrated into the operations of the team in charge of data security in the firm. This can help in motoring all the activities in the network thus preventing further security breaches.

References

1. Information That Matter, A data breach responsible disclosure project associated with OWASP Singapore.

2. The Breach Blog, Data breach commentary and analysis