Project 1

Data breach incident plan “**what is a data breach incident response plan?**”

The company should have prepared with a breach incident breach plan.

Physical devices stealing or injection.

Third party vendor mistake

Domain or website high-jacking

Theft of high priority information or trade secret

Spam or phishing attacks

intentional destruction of mission critical data

network penetration for identity theft or business espionage

develop an incident plan

test an incident plan

recover from an incident

companies that handles personal information have to be prepared to respond promptly to a data breach

technical and physical

“**Breach Response**”

responsibilities

respond

When a breach occur the first thing to do is to stop it

Document as much as you can to what happened

State requirement

Determine in advance how to communicate

Restore the trust of the customers

GetWell provides servieses to hospitals and to patients either directly or through their hospitals. Except for the attackers, all other procpectives have aligned goal to have a robust secure system that meet the CIA.

To develop the system, we need to adhere to the basic security system development lifecycle, which usually consists of 5 phases:

1. Initiation
2. Development
3. Implementaion/ assessment
4. Operation / maintainance
5. Disposition

Devices: Sean

1. Identify Assets:
2. Assess Risk
3. Plan and Deploy countermeasures
4. Implemnt Bussiness continuity plan
5. Monitor for threats and manage Vulnerabilities
6. Detect Attacks
7. Respond to incidents

Incident

The system should has three major phases for each of the different procpectives:

1. System Design.
2. System Implementaion.
3. System Operation, including reacting to a certain incident.

Operation:

Threat lifecycle management:

1. Monitoring
2. Detection
3. Response

**Introduction**

Personal health information are very special and sensitive. Thus, many regulation govern the process of exchanging such information. Regardless of the size of the institution that deals with this kind of data, it must comply with the some health regulations, like HIPAA. An enterprise like GetWell that process millions of records each day must have special kind adaptation to deal with the risk of a leak.

Not only that GetWell deals with PHI and PII, but also, it has different kinds of equipments that can directly provide critical care to the patients.

**System**

It is important to make a distinction between different subsystem in the GetWell architecture to define boundaries and hence responsibilities. There are three basic system that exchange sensitive information, and can be summarized as the following:

1. **GetWell system**: any software or hardware that is managed directly by GetWell, including:
   1. Datacenteters
   2. Remote employees laptops
   3. Websites and emails
   4. Medical devices
   5. Tablets
   6. Multiple Wi-Fi access points.
2. **Third-Party systems**: Any service or software that is being used by GetWell or its clients and managed by third party, such as:
   1. Microsoft services.
   2. SalesForce
3. **Client Systems**: Any hardware or software that is being used by GetWell clients to view, retrieve or update information with GetWell, such as:
   1. Client IT infrastructure
   2. Patients personal devices.
   3. Multiple Wi-Fi access points.

Equipments

Robots, sugar infusions,

**Cybersecurity and Risk Management Framework**

According to NIST’s definition for risk management, it is " *the ongoing process of identifying, assessing, and responding to risk.”* Except for the attackers, all prospective have aligned goals of a robust secure system that meet the user needs.

Since GetWell operates in a highly regulated environment, we assume that it adhere to some Risk Management Framework(RMF) and to cybersecurity framework.

If GetWell did not adhere to some kind of cybersecurity framework, then it must start immediately.

**Cybersecurity Framework**

Since we assumed that GetWell has a cybersecurity framework which consists of the following phases:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

The phase in which GetWell detect the breach starts from the Detect phase. However, the response plan has been designed and documented in the previous phases, along with the rules

**Preparation phases: Identify and Protect**

GetWell assets are being identified and categorized. The business impact is used along with the vulnerability, threats, and likelihood to determine risk, and then risk categories are being prioritized and used to identify the proper response.

The cybersecurity roles and responsibilities for GetWell’s and third-parties employees are established.

Finally, risk management process are established and agreed to by organizational stakeholders.

**Detect Phase**

There will be different plans for each source of the data breaches, but it is very important to pinpoint the source of the problem. A plan for an incident when data is stolen from patients’ devices is different from a plan when data is stolen from data centers. For example, actors can steal the 10 records from multiple patients personal devices and claim, based on the published data, that they have the whole 20 million records.

Also, we need to identify whether the breach is digital or physical, and whether it is GetWell’s or a third party’s mistake.

**Response Phase**

GetWell works in different countries and probably different states in the US; therefore, multiple actions must be taken based on the federal and the state laws.

Also, if the company is covered by HIPAA, it must comply with its Breach Notification Rule. That is, GetWell needs to notify HHS, the affected individuals, and possibly the media within 60 days of the breach discovery.

Recover Phase

**Risk Management Framework**

The cybersecurity framework by NIST consists of 5 basic steps:

Any RMF usually consists of 6 basic phases all accompanied with special phase of preparation:

1. Categorization
2. Selection
3. Implementation
4. Assessing
5. Authorization
6. Monitoring

**Categorization**

This phase is really important because it defines the center assest to Getwell. What is important and what is not. What kind of information needs to be protected the most? How the environment in the e

The assets are the patient personal information, the employees and the. Also, making sure that the equipments are fully isolated if the

Things to be considered:

* The GetWell system boundaries are a, b and c.
* Identified the information as personal information, b, and c.
* The impact-level prioritization
* Documentation
* Must reflect GetWell risk management strategy
* Characteristics of the system

**Selection**

Mmmm

* Selecting the best design for security and privacy controls.
* Documentation
* System-specific, hybrid, or common control?
* Developing continuous monitoring strategy that reflects GetWell risk management strategy.

**Implementation**

Mmm

* Security and privacy controls are implemented according to the plans.
* Make sure that the methods are conform to best practices.
* Create the configuration baselines

**Assessment**

This phase aim to assess of the implemented security and privacy controls, and report initial bugs and potential problems.

* Developing a plan to assess the security and privacy controls being design and implemented
* Security and privacy assessment report
* Remediation for the findings

**Authorization**

Once the defendors are done with the assessment phase, it is then shown to the executive and security seniors for final authorization to the remediation.

* A plan of action for remediation for the findings in the assessment report.
* Risk determination
* Risk Response

**Monitoring**

In this phase, we usually detect the wild attacks.

* System and environment change
* Ongoing assessment
* Ongoing risk response
* Authorizatin update
* Reporting

If you use a cloud infrastructure sourced from a cloud services provider, you must impose all legal or regulatory requirements that apply to your enterprise on your supplier as well. This is your responsibility, not the provider’s. Taking the HIPAA regulations as an example, any subcontractors that you employ (for example, a cloud services provider) must have a clause in the contract stipulating that the provider will use reasonable security controls and also comply with any data privacy provisions.

Incident Response Plan

Forensic

Who did it

Which part of the system was compromised

How did it happened

What is the first step

What about the website? Take it down?

What

What happen when a system failed? Audit?