Healthcare Risk Management Policy

Matthew Austin

CIS 225: Information Security Policy Analysis and Implementation

29 November 2018

Karen Quagliata, PhD, PMP, CISA, CISSP

***1. Background***

This organization is need of a risk management framework protect its employees, clients and assets from risk. This risks can be external and/or internal. The risks that are external political issues, natural disasters, exchange rates, interest rates, etc. The risks that are internal are non-compliance, information breaches, etc. This organization specializes in healthcare that will use the established risk framework such as NIST and from that framework build upon to meet tend to our specifications. Without be able to manage the risk that this organization may face the organization can shape the objectives that it wants to complete in the future.

***2. Framework Requirements***

Following this framework's requirements include:

* Being aware of the background and the premise of the company, so that you can better understand your role in the company.
* Understand the the role and responsibilities of all the other stakeholders and professionally get to know them, so that the workflow can be smoother.
* Strictly following the rules that policy sets in place, non-compliance will not be tolerated, as it can lead to internal threats arising.

The risk register will include:

* *Dates* of the risks that are identified and/or modified.
* *Description* of the risk.
* *Risk Type:* stating whether it’s business, project or stage:
  + Business risks relate to the delivery of achieve benefit.
  + Project risks relate to the management of the project.
  + Stage risks are associated with a specific stage of the plan.
* *Likelihood of Occurrence:* Provides an assessment of whether the will occur (from High, Medium, or Low)
* *Severity of the Effects:* Provides an assessment of the impact the occurrence of the risk would have on the organization
* *Countermeasures:* Actions taken to prevent, reduce or transfer the risk
* *Owner: The individual responsible for ensuring that risks are appropriately engaged with countermeasures undertaken.*
* *Status: Indicates whether this is a current risk or if risk can no longer arise and impact the organization.*

The Data Classification that will be covered is:

* Confidential Data
  + Employee Health Information.
  + Employee Records.
  + Research Information.
  + Employee Information.
* Patient Medical/Health Information (HIPAA)
  + Identification Numbers (Social Insurance Number (S.I.N.), OHIP, Hospital PIN).
  + Full patient name, full address, postal code.
  + Biometric identifiers (fingerprints, voiceprint).
  + Medical Records.
  + Personal and Demographic Information (marital status, birth date, age, height, weight, email address).
  + Dates (except year) related to an individual, account / medical record numbers, health plan beneficiary numbers.
  + Medical images.
* Employee Information (PIPEDA)
  + Identification Numbers (Social Insurance Number (S.I.N.), Employee ID);
  + Personal financial information, including non-organization income level and sources (bank account, income).
  + Insurance and benefit information.
  + Demographic information (name, marital status, birth date, race, ethnic origin).
  + Personal Information of employees (email address, religion, educational level, tax return information).
  + Certain management information (performance evaluations, agreements, employment history etc).
* Sensitive Data
  + Draft planning documents.
  + Internal internet websites.
  + Research data that is NOT identifiable or protected under a Confidentiality Agreement (i.e. identifiers removed).
  + Personal and Demographic Information (marital status, birth date, age, height, weight, email address, PIN ) when NOT aggregated with other personally identifiable information.
  + Employee / Patient Email messages.
  + Employee/ Patient Network usage information.
* Public Data
  + Any information that does not need to be protected to comply with Confidential or Sensitive classification standard.
  + Any information that has been publicly published through official channels.

***3. Stakeholders***

* *Chief Information Security Officer (CISO)* roles and responsibilities are:
  + Establishing and implementing security-related policies
  + Overseeing regulatory compliance
  + Ensuring data privacy
  + Managing the organization's Computer Security Incident Response Team
  + Supervising identity and access management
  + Establish and overseeing the organization's security architecture
  + Conducting electronic discovery and digital forensics investigations
  + Working with other high-level executives to establish disaster recovery and business continuity plans.
* *Security Architect’s* roles and responsibilities are:
  + Building and maintaining the computer and network security infrastructure
  + Develop a compre cents understanding of organizations technology and information needs
  + Develop and test security structures designed to protect the organization's systems
* *Security Director's* roles and responsibilities are:
  + Oversee the implementation of all It security measures throughout an organization.
  + Designing, managing and allocation resources to various security programs within the organization's security department
  + Creating user awareness and security compliance education campaigns
  + Interacting with non-management employees
  + Offering key assistance to law information in the event of a security incident and investigation
* *Security Manager’s* roles and responsibilities are:
  + Managing the organization’s It security Policy
  + Create and execute security strategies based on the input from the Security Director and/or the CISO.
* *Security Engineer* roles and responsibilities are:
  + Responsible for building and maintaining the IT security solutions of the organization
  + Configure firewalls, test new security solutions and investigate intrusion incident, all while reporting to the Security Manager.
* *Incident Responder* roles and responsibilities are:
  + Addresses security incidents, threats, and vulnerabilities that arise
  + Actively monitor the organization's networks for intrusions
  + Perform security audits and penetration testing
  + Conduct malware analysis and reverse engineering
  + Design measures that minimize the damage of a given incident and prevents similars intrusion from reoccurring
* *Security Consultant* is an outside expert who helps an organization implement the best solutions according to their security needs, their roles and responsibilities are:
  + Must be knowledgeable in a wide range of security standards, security systems, and authentication protocols
  + Develop an in-depth picture of the organization which includes:
    - Interview managements and other executives
    - Becoming aware of the organization's corporate policies
  + Implement a set of security tools that correlated with the organization's needs
  + Testing the systems they put in the place and updating them when need (regularly)
* *Malware Analyst's* roles and responsibilities are:
  + Helping an organization understand viruses, worms, bots, Trojans and other malicious software that threaten the organization's network on a daily basis
  + Work with malware analysis and incident responders in the event of an intrusion and/or suspicious computer behavior to help identify computer systems
  + Conducting statics and dynamic analysis of the suspicious code in order the establish signatures of the malwares presces
  + Developing tools that can help protect the organization's network against future intrusions.
* *Security Specialist’s* roles and responsibilities are:
  + Completing a variety of duties designed to strengthen the security of an organization which includes:
    - Analysing the security requirements of an organization's systems
    - Install and configure security solutions on corporate networks
    - Perform vulnerability testing and help train fellow employees in security awareness.
    - Having knowledge in ethical hacking, computer networking, programming and Security Information and Event Management.

***4. Policy***

The development, implementation, and execution of this Healthcare Risk Management and Mitigation Policy is the primary responsibility of the team under the management of the Security Engineer and the Security Specialist. The team are expected to properly facilitate the RMMP for applicable to the service or products they are held accountable. The teams coordinator is further expected to work with the in the development and maintenance of a Security Response Plan. (Sans) This framework takes the Quantitative approach as the need for new software and items being made for scratch will be done without hesitation, assuming the the organization has enough funding to fulfill the needs of the policy. A Quantitative approach is more effective as their are not any recent limitations that you have to work around in order to assess and mitigate a risk.

*Classification (continued)*

* All information should be simple and easy to find by creating an effective data classification app with an algorithm that safely and effectively receives and sends data within the server.
  + The classification software should include the classifications stated in Frameworks Requirements.
* The classification software can either be created by Software Development team in the organization. If a software development team is not available, the use of a third party's system is acceptable (make sure that the software is trusted and secure).
  + Whether or not the software is created by a software development team or acquire via third party, the software should be regularly updated.
* With the classification and risk registry software the employee's role in the organization should correlate with their access to certain items in the server by following the rules of least privilege.
* If there is any risk reported by any employee or found by the risk analysis/scan team should be put into the software by one of the employees appointed with the responsibility by the software Engineer and Security Analyst.

*Risk Assessment & Management*

* The organization's approach to security should be based on risk assessments in the risk registry.
  + On a daily basis the risk registry should be assessed and plans should be made to prevent the risk that was put into the registry from reoccurring.
* Every member of the organization must be knowledgeable of their role and know and control all the information that they have granted control over.
* The organization should continuously (24/7) scan and assess the risk and evaluate the need for protective measures. If cost is a concern for the organization, a scanning and assessment schedule shall be revised based on its budget (and SSAE 16 Report if accessible). Nonetheless scans and risk assessments should at least be done annually.
* The Chief Information Security Office (CISO) must overlook risk assessments which must identify, quantify and prioritize the risks according to relevant criteria for acceptable risks. When changes are made the risk assessment must be change/updated as well.
* The CISO must assess the and effective and suitable consequence to users who violate anything in the policy.
* Risk assessments must be approved by the management of the organization and system owners or the CISO
* If a risk assessment reveals unacceptable risks, measures must be implemented to reduce the risk to an acceptable level as stated previously.
* If a risk has become a threat and has caused severe damage to the organization's security, the organization must follow the rules and policy created by the Security Specialist and Incident responder.

*Risk Mitigation*

Information Security

* + Ensure servers and high-priority documents are protected in password-protected rooms watched 24/7 by security officials and cameras that detect unauthorised movement/access in the room and notifies all security officials in the building. Based on the level data/information within the company the level of concern (LOC) should determine the level of security of that information through assessment.
  + Educate those to not share information with others, not even to fellow peers. If so direct them to a Data Monitoring Committee official if the password has been forgotten or their intentions seems suspicious.
  + Emails and user activity are monitored 24/7 by an assigned data monitoring committee officials along with a learning algorithm that inhibits certains actions and access of the user if a threat is foreseen.
  + Ensure that the server and every account in the server password is reset every 30 days.
  + Any user who request information that is out of their privilege must be directed to the CISO or Data Monitor Committee (DMC).

Natural Disasters

* + In the event that there is a power outage of a natural disaster that threatens the servers, the backup generator automatic power on to ensure that data is restored automatically while running a diagnostic and security test on all of the data in rest in the building to ensure that everything is running smoothly, secure and to assess any loss of data.
* All users in the organization must collaborate with the operational users to create an understanding of the risks and their implications. Such risks can be classified as impacting traditional cost, schedule, and performance parameters.
* Provide users with projections of schedule adjustments needed to reduce risk associated with technology maturity or additional development to improve performance.
* Help control risks by performing analyses of various mitigation options (which are alternative plans/policies created by CSO and/or Data Monitoring Committee and/or software owner.
* Determining the needs of the the different roles/levels of the organization after assessing and revealing a risk/threat.
* Finally create a contingency plan (Plan B) that should be created by the CISO and/or Data Monitoring Committee and/or software owner. Otherwise, assess and scan every back-up until it seems secure.

***4. Report***

The Key Performance Indicators (KPIs) and Key Control Indicators (KCIs) will be defined as:

* The amount of time between a risk being the highest severity
  + The last time that the organization was negatively affected by a risk that was handled by the analysis plan
* The amount of time between creating or updating our policies
  + If the policy has been updated more than often then that implies that the company is adapting, learning, and growing to better face the risks that if faces.
* The happiness and satisfaction of not only the clients/patients but also the employees.

References

Campus Information Technology Security Policy. (2016). Retrieved August 22, 2016,

from <https://security.berkeley.edu/campus-information-technology-security-policy>

<https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en>

The University Policy Manual. (2016). Retrieved August 22, 2016, from

<https://policy.uncg.edu/university-policies/data/>

Secure The Breach | Get Ready For A Security Breach. (n.d.). Retrieved August 30,

2016, from <http://www.securethebreach.com/encryption.html>

Information Security | Washington University in St. Louis. (2016). Retrieved August 22,

2016, from <https://wustl.edu/about/compliance-policies/computers-in>

Risk Mitigation Planning | MITRE (2016). Retrieved October 9,

2016 from <https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring>

UWO. "What Are the Data Classifications." *What Are Data Classifications - Information*

*Security - Western University*. UWO, n.d. Web. 28 Nov. 2016. <<https://security.uwo.ca/information_governance/standards/data_classification/data_classifications.html>>.

HCIN. "Top 5 Security Threats in Healthcare." *Healthcare IT News*. HCIN, 02 Mar. 2012. Web. 28

Nov. 2016. <<http://www.healthcareitnews.com/news/top-5-security-threats-healthcare>>.

Bright Up. "What Is a Risk Register? Explanation & Free Template." *Brighthub Project Management*.

Bright Up, 24 Oct. 2014. Web. 28 Nov. 2016.

<http://www.brighthubpm.com/risk-management/3247-creating-a-risk-register-a-free-excel-template/>.

MITRE. "Risk Mitigation Planning, Implementation, and Progress Monitoring." *The MITRE*

*Corporation*. MITRE, n.d. Web. 28 Nov. 2016. <<https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring>>.

Previous Papers written by Matthew Austin for Information Security CIS 225 were used as references as well.