Risk Management for Healthcare Systems

Lamaris Davis

East Carolina University

07/15/2016

Attract

The responsibility of risk management in healthcare systems falls on multiple individuals within any given organization. It's well known that most hospitals and healthcare systems do not have a completely practicable risk management system that spans across an entire organization and operational structure for the delivery of key services. Ensuring the security of protected health information (PHI) in your health IT system requires that you institute measures to guard against unauthorized use or disclosure of PHI. A risk management plan should have five key parts which are administrative safeguards, technical safeguards, physical safeguards, organizational standards, and policies and procedures. For any single risk, a combination of safeguards may be necessary because there are multiple potential vulnerabilities that exist that could negatively affect healthcare systems, according to the American Society for Healthcare Risk Management (See Reference 1).

Enterprise Risk Management (ERM) should be a part of any healthcare system overall plans for healthcare organizations. A healthcare system ERM plan should address the overall risk that an organization could face from outside or inside the organization. The plan should go over ways of managing risk and the impact of such risks as an overall risk portfolio. Healthcare systems ERM strategy should be viewed from several perspectives which involves Risk avoidance, Risk mitigation/control, risk transfer, and risk opportunity. A full integrated risk management plan should follow a top down approach, starting at the senior level of management working itself down. If the healthcare system ERM program starts from the top going down this will ensure that standards, processes, and procedures are consistent at the entry level and across the rest of the organization.

If the healthcare system follows this top down approach when it comes to their Risk management program, it will help the organization to quickly adapt to disruptions while maintaining continuous business operations and keeping people safe, information assets, and overall organization reputation. The overall idea of risk management techniques as a whole is typically directed toward mitigating financial impact resulting from the misuse or mishandling of information assets within any given healthcare system. Therefore, risk management must be classified as a management function rather than a technical function. It is vital to manage risks within healthcare systems or any system at that. It helps to get a good understanding of risk for healthcare system, and in particular, understanding the possible risks to a system allow that particular system owner to protect the information system according to the information value to the organization.

Risk should be measured by healthcare systems by identifying threats and vulnerabilities, then determining the likelihood and the resulting impact for each possible risk. Risk management is a very complex task for any organization especially for healthcare systems. The healthcare risk manager works very hard to prevent incidents and/or to minimize damages from attacks against healthcare systems. There are healthcare risk managers that focus on event/incident management and emergency readiness to 96-hour mark, which are considered the most critical time after an incident. Emergency management risk managers help to prepare their specific organization for emergency situations by creating ways to keep patients receiving services during critical down times. Emergency risk managers usually do not focus on enterprise business risk and operational impact with a view on mitigating impact or loss before an event occurs. These usually do not focus on returning operations back to normal after a major crisis happen either.

When it comes to the healthcare infrastructure, the healthcare and the public health sector is highly dependent on other sectors to create their continuity of business and service delivery; communications, Energy, Food, IT, transportation systems, water, and drain water system. Therefore, it's very important for healthcare systems to have their own practicable plans to not only respond to specific emergencies, but to continue business as usual for their critical systems until a full recovery can be brought to fruition. If a major hospital was forced to move all of its patients due to a power outage even though it's very possible they will have a backup power available as well as an uninterrupted power source (UPS) to keep the critical systems running, the time of the outage come exceed the limits for the backup systems. If the limits on these backup systems are exceeded, it will put the entire healthcare system at risk for some type of breach.

The emergency team performed their duties correctly, but the facility could have also been a site for medical research which could have put the hospital at a huge financial risk, which isn't largely acceptable. Power outages are definitely considered a risk for a healthcare system. If the healthcare has a useful risk management plan in place, it would have identified critical processes being performed, along with the resources required to keep things running smoothly in case of a critical down situation. A healthcare risk management plan would have also uncovered the threat that the research data had not been in a safe location. A risk management plan could save a healthcare system a great amount of time in lost time and research.

Most organizations, including healthcare systems use quantitative risk assessment which is taken from methodologies used by financial institutions and insurance companies. Most organizations assign values to information assets, systems, business processes, and recovery costs. They use these methodologies so that risk can be measured in terms of direct and indirect costs for that organization. Quantitative risk can be expressed in terms of annualized loss expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being discovered over a period one year. Healthcare systems also consider the SLE which stands for the single loss expectancy which considers a single loss of the information asset, which could be a better way to measure for their systems.

In qualitative risk assessment, it's best not to use numbers when assessing risk for healthcare systems. If numbers are used most senior level management will generally view things as more accurate than the number actually are for that specific system. It's very important to remember that qualitative risk assessments are based on the likelihood and, impact values based directly on the most accurate information available at the time of the assessment.

Healthcare systems must consider the common threat-sources which includes natural disasters like floods, earthquakes, hurricanes, tornados. A healthcare system also must consider human threats which could be both unintentional and deliberate actions. There are environmental threats that must be considered in the risk management plan things like power failure, pollution, chemicals, water damage. The people that understand the healthcare system and the type of systems being used within that organization are the keys to identifying threats. It's very important to gather a list of threats that are present across the healthcare system and use this list as the basis for all risk management activities within the organization. The list should be reviewed with those individuals most knowledgeable about the healthcare system to make sure the system specific risks are covered.

The Risks of free-flowing Private Health Information

Policymakers and Healthcare IT experts are very concerned that healthcare organizations are not dealing adequately with security issues as they develop health IT systems for their organizations. It's very important for healthcare systems and business associates to focus on the security risks that comes with a system that involves increasingly free-flowing private health information. Problems with free-flowing private information are only multiplied when hospitals decide to join their organizations, which usually requires a department to develop some type of IT system for the purpose of setting up information exchanges. Most funds allocated for Healthcare IT systems are used for setting up systems that talk to each other, first and then figuring out risk and security measures last.

As healthcare systems continue to come together and combine their Healthcare IT resources and force the input of information to the edge, with some type of remote monitoring device. This remote monitoring device job will be to collect private patient health information

and bring it back to that particular provider for research and storage. The database storing this private information which is located at the healthcare provider will potentially be exposed to some type of remote access attack.

Defense for these malicious remote access attacks is required at all layers of the OSI model stack; application design layout; switch, and server; and at the firewall. Most organizations combining resources are relatively small innovative organizations, and haven't showed a lot of interest in the security part of their operations. The risks of data breaches extend to businesses hospitals and providers that they contract with to carry out medical coding and billing. These business professionals should also develop their own risk management plans for their Healthcare IT systems and, follow the same standards as the healthcare system they are contracting with.

If any business providing services to healthcare systems have access to private health information (PHI) they are to be held responsible for possible risks and are subject to the same penalties as healthcare providers. Most companies use off-shore resources, but will limit their access to sensitive information, which will overall reduce the risk within their organizations. If a security breach occurs off-shore, and the US based healthcare system allowed the organization to have access to PHI the responsibility will fall on the US based healthcare system generally. It is a great business decision to take risk management seriously when dealing with other organizations.

Continuity of Access for electronic healthcare systems

Data breaches continue to make the news every day, therefore the focus is being put on data security, constant and uninterrupted access to electronic patient data is more crucial to daily healthcare systems and the patient care being given. As hospitals continue to move towards

converting their records into electronic records, they will not be able to function safely without continuous access to patient data. Because healthcare organizations need continuous access to patient's data, it's very important to put together a risk management plan that includes having substantial backups and, disaster recovery systems in place for when there is an interruption in their service.

Healthcare systems are highly depended upon by staff so as mentioned before taking risk management seriously is a great business decision. By looking at this fact as a great business decision it will enhance the benefits of having a great risk management plan in place and will make that organizations healthcare IT systems run better overall. Providers within healthcare systems depend on satisfied patients, and their business associates depend upon satisfied customers. Trust is very important to sustain healthy relationships, and trust will only be achieved by demonstrating privacy is a priority for these healthcare systems.

Five Security Components of Risk Management

There are five security components of Risk management for healthcare systems that should be implemented across all healthcare systems. The five security components are administrative safeguards, physical safeguards, technical safeguards, organizational standards, and policies and procedures. Healthcare systems could try low-cost, highly effective safeguards for their organizations which could be denying requests from staff members to take home office equipment like laptops containing unencrypted information. The staff should never email PHI and organizations should remove hard drives from decommissioned systems before discarded the system. Organizations could also notify office staff that their access to different systems will be monitored randomly and, the server containing electronic health records should be scanned for viruses and malware often.

Organizations could look at implementing administrative safeguards like placing security officers in designated areas. Office staff should have their training begin at the beginning and conducted on a regular basis semi-annually. Physical safeguards for an organization should include building alarm systems and office locks or at least cabinets within the offices that lock. Office staff should also try to use screens to shield their computer screens from wondering eyes or shoulder surfing attacks. Organizations should use technical safeguards which involves users using secure IDs, passwords, and appropriate role-based access should be assigned.

Another component of technical safeguards should include performing routine audits of access and changes to healthcare IT systems. Anti-hacking and anti-malware software should be installed on computers throughout the healthcare systems. Healthcare systems should have organization standards in place which including performing regular reviews of agreements and updates across the system. Policies and procedures are also a crucial part of a risk management plan, written policies and procedures should be put in place and staff should be trained accordingly. Organization should ensure that routine updates are made to document any security measures.

A healthcare system should stick to their plans and by following these plans will reduce security risks and, better protect PHI and the systems holding this information. Healthcare systems should build a culture that values private health information for their patients and actively protect this information. When implementing the risk management plan, the goals consists of protecting private health data through ongoing efforts to identify, access, and manage risks. The security portion of your risk management plan should always follow the five HIPAA security components which are again administrative safeguards, physical safeguards, technical safeguards, organizational standards, and policies and procedures.

Other ways to manage risk for healthcare systems

Risk Transference is the process of allowing another party to accept the risk on behalf of the organization. Risk Transference is used a lot these days for IT systems in general and could be used for Healthcare IT systems, but the obvious downside to this strategy is the fact that it doesn't decrease the likelihood or fix any issues, but it does reduce the overall impact of an incident for that organization. Another strategy that a healthcare system could use when it comes to the managing of risk is to accept the risk altogether. Risk acceptance is the practice of simply allowing the system to operate knowing that there is risk present. If risk acceptance is the practice the healthcare system chooses, there should be some type of criteria followed which should help management to figure out how much risk to accept and what kind of risk.

Many organizations see low risk as acceptable. Risks that present a higher level of risk will normally have extremely high cost to mitigate the risk, which is also usually accepted. If the healthcare system decides to carry out this strategy the organization should ensure that the plan is in wring and accepted by the decision making manager or president of that system. Sometimes risks are accepted that definitely shouldn't have been accepted from the beginning, and then when the organization is under a penetration test, and IT security personnel are held responsible. Typically, business partners or decision making managers, are the only ones authorized to accept risk on behalf of the healthcare system.

Healthcare systems could also deploy the risk avoidance strategy. Risk avoidance is the strategy that removes the vulnerable part of the system or even the system itself in order to get rid of the risk. For instance, during a risk assessment, it was determined that a database wasn't up to date and it's missing the proper patches. When the vulnerable database was discovered management decided to remove the database and use a backup database instead. In this particular

situation, the risk was avoided by removing the system that the vulnerable database resides on. IT staff should be provided with the means to continue their education and provided with the tools to perform their jobs successfully. IT security staff within the healthcare system should provide the guidance needed to employees to ensure that their risk management plan stays effective.

Conclusion

Healthcare system and the IT systems they need to have a risk management plan in place to be able to handle risks. Risks must be communicated within any particular organization. Once the risk is understood, risk and risk management strategies must be clearly communicated to the organizational leadership team within the healthcare system in words easily understandable by the leadership team. Healthcare system managers are just like other managers they are used to managing risk, they perform this duty every day on the job. This reason alone is why it's so important to present risk information in an understandable way. It's also a good idea to try to not use fear, uncertainty and doubt. It's a better idea to present risk in terms of likelihood to happen and the impact that could result from such a risk.

Healthcare systems should focus on managing risks by following the risk management strategies mention in this paper. The risk management strategies are risk mitigation, risk transference, risk acceptance, and risk avoidance. Healthcare systems can significantly reduce their risks by following one or a combination of these strategies. The success of a risk management plan will depend highly on a successful and effective IT security department within the healthcare system. Considering that there are limited resources and a lot of threats to protect organizations against, a reasonable decision has to be made concerning how resources will be used to protect Healthcare systems and the systems they use to conduct their business.

Risk management practices for healthcare systems allow the healthcare system to protect information assets. To make sure that the most is gained from risk management, it must be consistent and repeatable, while still focusing on reducing overall risk. Healthcare systems should establish a high quality risk management process which is based off of the information security activities of the organization in order to create an effective information security program for the healthcare system. Healthcare systems should continue to provide education through seminars and hands on workshops in order to reduce risk overall.

People present the biggest risk to any organization information assets since most people within any given organization have access to sensitive information. Most CNA, nurses, and other hospital staff have direct access to the patient's private health information, therefore education should be ongoing for these employees within the healthcare system. Employees within the healthcare system should also be educated directly on the proper use of the company's computer systems. Shoulder surfing and social engineering should be the leading conversations between healthcare system management and employee since these two types of attacks will more than likely be seen the most. Healthcare systems should stay the course when it comes to risk and their risk management plan.

References

HRSA. Health Information Technology. Security and Privacy Issues.http://www.hrsa.gov/healthit/toolbox/HIVAIDSCaretoolbox/SecurityAndPrivacyIssues/howdoiensuresec.html

Frost and Sullivan. Health Information Technology: The Imperative of Risk and Compliance Management in the HITECH Age. Retrieved from http://www.emc.com/collateral/analyst-reports/fs-health-information-technology-ar.pdf on 07/105/16

*Journal of Healthcare Risk management. Retrieved from http://www.ashrm.org/pubs/journal.dhtml on 07/16/16

Carroll, Roberta. Enterprise Risk Management: A Framework for Success. Retrieved from http://www.ashrm.org/pubs/files/white_papers/ERM-White-Paper-8-29-14-FINAL.pdf on 07/15/16

*American Society for Healthcare Risk Management. Tackling patient safety taxonomy: A must for risk managers. Retrieved from http://www.ashrm.org/pubs/files/white_papers/MonoTaxonomy_1.pdf on 07/14/16

* Zimmerman, Theresa, RN, BSN, JD. Enterprise Risk Management for Hospital Systems: What Counsel Needs to Know. Retrieved from http://media.straffordpub.com/products/enterprise-risk-management-for-hospital-systems-what-counsel-needs-to-know-2012-04-04/presentation.pdf on 07/14/16.

National Institute of Standards and Technology. Risk Management Guide for Information Technology Systems. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf on 07/15/16

SANS Institute InfoSec Reading Room. An introduction to information system risk management. Retrieved from http://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204 on 07/17/16

*[1]Simeone, Cynthia (2015). Business resilience: Reframing healthcare risk management. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/26418138 on 07/14/16

HealthIT. Guide to Privacy and Security of Electronic Health Information. Retrieved from https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf - pg. 45 on 07/16/2016.

Menachemi, Collum T (2011). Benefits and drawbacks of electronic health record systems. Retreived from https://www.dovepress.com/benefits-and-drawbacks-of-electronic-health-record-systems-peer-reviewed-article-RMHP on 07/14/16

OIG website. Security Gaps may threaten Electronic Health Records. Retrieved from https://oig.hhs.gov/newsroom/news-releases/2011/security.asp on 07/12/16