**Company X** is a healthcare company in Rhode Island that manages two of its largest hospitals. They employee over 15,000 people and see an average of 300,000 patients per year. Since it’s part of the healthcare industry, information security regarding personable identifiable information should be a top priority. As I covered in previous posts, the high level of fines regarding data breaches in healthcare only continues to rise, which makes a security awareness program a vital part of mitigating potential attacks.

Based on Section 3.4 in the “Best Practices for Implementing a Security Awareness Program”, I believe the following metrics for Company X should be used:

* Increase in reports of attempted e-mail or phone scams
* Increase in in reporting of security concerns and unusual access
* Reduced system downtime and network or application outages
* Increase in the number of queries from personnel on how to implement secure procedures
* Vulnerabilities are address or mitigated in a timely manner
* Increase in number of employees with privileged access to have received required training

For the metrics I chose, I start with the increased reports of attempted e-email or phone scams because as I’ve seen in my Case Study class, as well as this one, is that phishing and or spear phishing remains the number one-way attackers attempt to gain access to a system. By having this type of metric, it will directly reflect how many people inside the organization are better at recognizing phishing or different kinds of social engineering attempts. Next, I’m recommending the use of increasing the reporting of security concerns and unusual access since it directly correlates with a better understanding by employees of the risks associated with unwarranted access. The more employees Company X has that are aware of unusual access, the better off they will be down the line when an attacker attempts to breach their security networks. Another useful metric I’m recommending for use is tracking the reduced system downtime and network or application outages. By using this metric, Company X can better gauge just how effective all their security policies, and awareness training is regarding employee effectiveness. If Company X sees a greatly reduced amount of downtime in their networks and applications, then they know the policies they’ve been implementing are having an effect. If you don’t measure the overall effectiveness of your approaches, then what’s the point in having them?

Continuing with the theme of ensuring that all personal have better awareness of potential threats, another metric I recommend is to increase the number of queries from personnel on how to implement secure procedures. With this metric Company X will gain a better understanding of just how many employees understand the types of threats the organization is facing. It’s not enough to just give awareness training., The personnel receiving the training should be able to identify potential threats, and this metric give Company X the tool needed to measure that effectively. Another important metric I recommend is tracking how many vulnerabilities are addressed or mitigated in a timely manner. This metric allows Company X to measure the effectiveness of its personnel regarding how they handle potential threats and risks to sensitive information. Since my Company X is involved in the healthcare field, the better the personal can be at understanding and mitigating risks, the better outcomes Company X will have when it comes to avoiding future attacks. Lastly, and perhaps one of the most important metrics I recommend is to measure the increase in personnel with privileged access who have received the adequate security awareness training. As I mentioned earlier, phishing/spear phishing is normally targeted at users who have elevated access inside a company network. Therefore, this metric allows Company X to adequately see just how many of their staff who have privileged access are completing the required training. If the percentage of employees is not up to Company X’s standards, they can enforce disciplinary actions that they see fit to ensure the safety of the sensitive data they hold.

Based on the checklists on page 14-23 in the “Best Practices for Implementing a Security Awareness Program”, I believe the following for Company X should be used:

* Build and Maintain a Secure Network and Systems
* Maintain a Vulnerability Management Program
* Implement Strong Access Control Measures
* Regularly Monitor and Test Networks
* Maintain and Information Security Policy
* Identify methods for creating security awareness materials

The first checklist I recommend is for building and maintaining a secure network and systems. To me this is vital for Company X since they deal in the healthcare industry and securing their networks with things such as firewalls is incredibly important. It would allow them to use the industry standards and best practices with regards to HIPAA and set the standard for not using simple default vendor firewalls. Next, I recommend the checklist for maintaining a vulnerability management program. I chose this for Company X because it’s a way to ensure that they are up to date with system protections such as anti-virus software, and programs used inside the company such as Medicat. Developing and maintaining secure systems and applications is paramount for a company with sensitive patient information. Implementing Strong Access Control Measures is another checklist I recommended because ensuring the principle of least privileged is adhered to is important to thwarting attacks on lower-level employees if there were no access control measures in place. This reduces the attack surface for malicious actors and hardens the overall network to attacks. I also think it’s important that they implement the checklist for Regularly Monitoring and Testing networks because it will help reduce network or system outages, and vulnerabilities can be discovered in a timely manner before an attacker can exploit them. Maintaining an information security policy is another checklist I recommend for Company X because without it, Company X runs the risk of malware infections, phishing attempts, and overall security concerns increasing over time. Having no checklist for maintaining an information security policy is like sailing a boat with no rudder; pointless. Lastly, I went with identify methods for creating security awareness materials because I believe it’s important for any company to continually think of new ways to inform employees in unique ways to help the remember the importance of their role in the security of the company. Company X will only be as strong as it’s weakest link so the more they can do to come up creative ways to keep employees engaged with security awareness over time, the better off the organization will be in the long run.

The checklist that I would not recommend are:

* Protect Cardholder Data
* Identify methods for employees to acknowledge they have read/understood the information security policy at least annually

I chose these two checklists as those I would not recommend because Company X doesn’t really rely on cardholder data for access to sensitive information on their networks or in person nor do I think having employees sign something that denotes there understanding of security would help. For one, cards used at Company X are just for gaining access to location of where you work and doesn’t center around protecting sensitive information. Second, I don’t believe that having employees sign something that says they understand the information proves that they do. I would much rather have quizzes or internal actions taken like fake phishing emails to better gauge employees understanding of security. That way Company X could get a better picture of who is retaining the information they learned instead of just letting employees check a box that says they do.

I do believe that the scale of the organizations matters when it comes to implementing any of these recommendations, because if we’re just talking about a start-up with 10 people, it can be much easier to control networks and systems that they access. However, once you reach the size of Company X, which his 15,000 employees, and holds 300,000 patient records, its essentially mandatory that recommendations like these be put in place to protect the sensitive information. HR in many cases would handle a ton of the employee training and awareness programs, and a human resource department doesn’t usually come into play for companies until they reach a certain number of employees that becomes untenable for the original founders to manage. There are contractors that also handle HR for companies, but when we’re talking about security, I believe that companies should try their best to keep it inhouse, that way they can better control the programs which are tailored to their needs.