2016

Security Awareness Program

SOUTHERN NEW HAMPSHIRE UNIVERSITY
IT-552 HUMAN FACTORS IN SECURITY

CARL B. WADE
HTTP://WWW.CARLBWADE.US

Contents

Statement of Work

1.0 INTRODUCTION

Cyber-attacks are a common occurrence in today's technology driven age. To stay ahead of these attacks, security must be a shared responsibility. Everyone must do their part in the plan since security is no longer set it and forget it. Not only must a plan be in place, but it must also be constantly updated and reviewed.

1.1 SCOPE

To create a security awareness program that will train every employee to be more security minded in the workplace. To mitigate security threats as much as possible through a shared security plan. To create a plan that will patch the security holes that are present in the company.

1.2 GOALS

To overcome the 10 security flaws that were identified and create a program that will mitigate these and other future security flaws. (Listed on page 5)

1.3 TASKS

The security awareness program will be split up into 4 stages: Threat Identification, Data Collection, Training, and Starting of a Continuous Improvement Program. Since the threats have been identified by the CEO, we are now in stage 2. (see page 5) In stage 2 data must be collected to ensure that the threat list is complete, proper tools are in place, and that the training will be properly implemented.

Surveys will be sent out to every employee to get an idea of their current knowledge of security and what they think are the top 5 security threats. Background checks will be performed on all current and future employees. This will give the company an idea on which of our current employees can be trusted and which employees should have more monitoring. This will also prevent any untrustworthy applicants becoming unethical employees.

Data must also be collected on all the current security tools so that the proper tools will be chosen for the workflow. Once the tools are selected, stage 3 will start. Training must be done to ensure the employees know how to use the new tools. Also, training must be done to ensure every employee knows their part in the security plan. The last stage will be starting a continuous improvement program. This will ensure that training programs are updated as needed, input from employees are taken to identify security risks, and that everyone feels like they are part of the solution.

1.4 TECHNICAL REQUIREMENTS

The following tools are needed to overcome current security problems:

- Intrusion detection/prevention system
- Network Logging software
- Encryption and Hashing
- Continuous Improvement tools such as: Root Cause Analysis, 5S, and Key Performance Indicators

1.5 PERSONNEL RESPONSIBILITY

The responsibility of the security program are as follows:

Cyber Security Awareness Training: IT department and HR

Implementation of Intrusion Detection/Prevention System: IT Management and CISO

Logging software, encryption, and other tools: IT Management with IT personal

Continues Improvement Program: CISO

Segregation of Duties and Mandatory Vacation Policies: CEO, CISO, and HR

1.6 SCHEDULE

The following is a 1 year break down of the schedule:

4 Months of data collection.

6 Months of training on the new equipment and cyber security awareness. Training will be done in groups to avoid major work time loss.

2 Months of continuous improvement program implementation. Once the program is in place, monthly cyber security mini training will be done to keep every employee fresh on security risks. Yearly training will also be done to keep everyone up to date on security issues.

1.7 ACCEPTANCE AND APPROVAL

Once the continuous improvement program is in place, data will be collected and analyzed to see if the program is a success or a failure. Security incidents, employee feedback, and vulnerability assessments will be key in the success or the failure of the program. If the number of security incidents goes up, the program is a failure. If the number goes down, the program is a success. By reviewing employee feedback, we can gage employee morale. By reviewing the vulnerability assessments, we can see the program as a success if the number of vulnerabilities goes down. However, if the number stays the same or goes up then we can see the program as a failure. If the program is a failure, then adjustments must be made and reevaluated.

The 10 Identified Security Gaps Within MUSA Corporation

1. No annual cyber security awareness training, which is causing high phishing and social engineering attacks
2. No configuration change management policy (to reduce unintentional threats)
3. No intrusion detection/prevention system
4. Logs are not being collected or analyzed
5. No media access control policy
6. No encryption or hashing to control data flow and unauthorized alteration of data
7. Vulnerability assessment is conducted every three years; unable to assess the security posture status
8. High turnover and low morale among the employees (due to lack of employee readiness programs and work planning strategy)
9. High number of theft reports and security incidents; possible unethical/disgruntled employees
10. No segregation of duties or mandatory vacation policies (to mitigate intentional threats)

Mitigating the Security Gaps

NO ANNUAL CYBER SECURITY AWARENESS TRAINING, WHICH IS CAUSING HIGH PHISHING AND SOCIAL ENGINEERING ATTACKS

This security gap will need to involve a total culture shift to mitigate. The current attitude is either training is a one-time thing, and once it is completed forget about it, or there is no time to complete the training. Either attitude is highly dangerous to have. The only way to mitigate this gap is to just create and roll out a security awareness program in 4 stages: Threat Identification, Data Collection, Training, and Starting of a Continuous Improvement Program.

The program should be started right away because the 4 stages of the security program will take a year to implement. So, the sooner it is started, the sooner this gap can be mitigated. Surveys will be completed for data collection to gage the understanding of security among the employees. The data will be used to tailor the training to meet the security goals. Since phishing and social engineering attacks seem to be the highest level of attacks, a lot of training should be focused on these areas.

Before any training starts, it is important to get everyone in a mindset for change. It is natural for people to resist change and it is important to show everyone that this change is necessary. If everyone is not on board with the change, then it will fail. To get everyone to start thinking about training I suggest that a few quick and short demonstrations be shown to show the importance of training. This will show people that the training is a necessity and not just something that is being forced on them for no reason.

NO CONFIGURATION CHANGE MANAGEMENT POLICY (TO REDUCE UNINTENTIONAL THREATS)

Every employee has different roles and responsibilities within MUSA Corporation. It is important for everyone to understand their responsibilities and the policies involved in their duties. In the current state, it is possible for employees to engage in risky behavior unknowingly. Every project is different and involves different procedures and policies. If they are unaware of the procedures involved in past projects, it is possible that they will obey the same procedures in their current projects.

One procedure might be fine for a past project, but following it for the current project might create a security risk. The way to mitigate this gap is to review the roles and the project for every employee. Based on the information gathered, create documentation that fully outlines everything needed for employees to know what is accepted for each project. This document should be broken down to clearly provide responsibilities, compliance requirements, and overall principles for each role and type of project involved company wide. This documentation should also be readily available to every employee. This will ensure that everyone is on the same page and that acceptable behavior is clearly outlined for everyone; reducing unintentional security risks.

NO INTRUSION DETECTION/PREVENTION SYSTEM

Unfortunately, we do not live in a world without criminals. Having an intrusion detection/prevention system is like having a security system for a house. If the network is not being monitored or protected, then the criminals will attack it. Much like how if a house has open doors the criminals will walk right in.

The first step in implementing an intrusion detection/prevention system is to fully understand system environment. This is because each intrusion detection/prevention system is different, with its own strengths and weakness based on the system it is being installed onto. Without a one size fits all system, installing the incorrect system will create more problems than it will solve. The next step is to create subnets of the network. This will allow for the monitoring to be broken up into smaller chunks and if an attacker is discovered, the attack can be isolated into one subnet. This will prevent the attacker getting too much information.

After the network is broken up into subnets, install the intrusion detection/prevention system in stages. This will allow for the installation to occur without impacting the day-to-day operations. The final step is to fully train the employees who will use the intrusion detection/prevention system. If they do not understand how to use the system, then it will be of no use. This is like installing a security system for a house but if the owner does not know how to turn it on; it offers no protection.

LOGS ARE NOT BEING COLLECTED OR ANALYZED

The logging security gap is linked to the pervious intrusion detection/prevention system gap. Logs can provide vital information to both detect attacks and create defenses against attacks. Information is power in the world of computers. Without complete information that logs provide, total protection is impossible. Before logging can be started, we must know why logs were not collected or analyzed. If the reason was due to a system not being in place to collect the logs, then install the system. If the reason was due to a lack of knowledge, then train everyone on the importance of collecting and analyzing logs. Once the system and training are completed, standard operating procedures must be in place to ensure that logging is not only collected, but also analyzed. If logging is not collected and analyzed after this stage, then dispensary action must be in place to ensure that employees know the importance of the logs. If the requirement has no punishment for non-obedience, then no one will follow the rule.

NO MEDIA ACCESS CONTROL POLICY

Information is power and must be protected. Media access control policies ensures that only authorized people have access to the data they need and nothing else. Like everything in computer security, it is important to fully understand the system you are working with. Each media access control policies have its own set of strengths and weakness.

Mandatory Access Control (MAC) is the most secure but also has the highest overhead requirements. Discretionary Access Control (DAC) gives more control to the content owners but increases the risk of access being given to the wrong people. Role Based Access Control (RBAC) takes more of a real-world approach to structuring access control but it can be limiting when one employee has multiple roles in the company. Rule Based Access Control (RBAC) offers flexibly that Role-Base does not but requires a lot of planning to create an effective control.

Since MUSA Corporation deals a lot with databases, Role Based Access Control (RBAC) should be used. Each employee's role will be examined to determine what rights need to be assigned to each role. Each employee will be assigned a role in the RBAC system. The last step will be to create an auditing system that will be performed periodically to ensure that each employee is correctly assigned to the needed role for day-to-day operations.

NO ENCRYPTION OR HASHING TO CONTROL DATA FLOW AND UNAUTHORIZED ALTERATION OF DATA

Data is one of the most important assets the company has. This data ranges from customer information, company secrets, employee information, usernames and passwords, and more. It is vital that this data is protected from unauthorized personnel. The first line of defense is preventing the data from being accessed. However, sometimes that is not possible and the last line of defense is encryption. All data should be encrypted, no matter what the case might be. This includes all databases and all backups. Usernames and passwords should be hashed with a strong salt to ensure that an attacker cannot just guess their way in or use a brute force attack.

The first stage in selecting an encryption method, is research. There are many encryption, hashing, and salting methods out there. There are right ways and wrong ways of encrypting data and if the encryption is not used correctly, it will fail. Also, some methods offer strong protection while others offer very little. After the encryption method is selected, the next stage involves training. Everyone involved must know how to properly use the encryption method. Otherwise, no protection will be offered. Lastly, there must be policies in place to ensure that the decryption keys and salt does not land in the hands of unauthorized people. Again, this is the last line of defense. If the attacker gets their hands on these keys there will be nothing stopping them from using the data that they have stolen.

VULNERABILITY ASSESSMENT IS CONDUCTED EVERY THREE YEARS; UNABLE TO ASSESS THE SECURITY POSTURE STATUS

Vulnerability assessments are a very critical function in security. Without these assessments, preventative measures cannot be added to stop future attacks. This is where the continuous improvement program will help eliminate this security gap. The program will offer the opportunity for everyone to share in the duty of vulnerability assessments. Through continuous training, everyone will become more aware about security and how to spot insecurities. To further encourage employee participation, a reward program will be in place. If the security vulnerability saves the company $1,000 or more, then that employee will receive a bonus (a percentage of the savings) as a reward. The larger the savings, the larger the reward will be. In addition to the reward program, a quarterly audit will be performed to assess the vulnerability of the network. These audits will be compared to industry vulnerability reports to compare our vulnerably to the industry averages. If our vulnerabilities are higher than the industry averages, then adjustments will be made to the security program to mitigate the risk.

HIGH TURNOVER AND LOW MORALE AMONG THE EMPLOYEES (DUE TO LACK OF EMPLOYEE READINESS PROGRAMS AND WORK PLANNING STRATEGY)

Through the corporate assessment of MUSA Corporation security gaps, the high turnover and low morale are due to a lack of training and planning. To overcome this issue, the best thing to do is create a weekly work planning meeting every Monday. This will ensure that every employee will feel that they not only have an organized plan to accomplish their work, but also feel like they are part of the plan. People who feel like they are part of a goal are more likely to work hard to accomplish them, than those that feel like they are being forced to work. Through the continuous improvement plan, not only will every employee have training that they need to accomplish their work, but will also be given the opportunity to rate their training. Each employee will be given a short survey where they can give feedback on the level of training, any suggestions on improvement, and any other areas they feel that they need more training on. This will be valuable information about the training that can give incite on whether or not the training is effective, and what other areas each employee needs to have training on.

HIGH NUMBER OF THEFT REPORTS AND SECURITY INCIDENTS; POSSIBLE UNETHICAL/DISGRUNTLED EMPLOYEES

The best way to deal with unethical employees is to be proactive. The first step is to assess every employee’s actions through network logs and vulnerability audits. If any employee has been determined to act unethically in ways of theft or repeated policy violations, termination is the only option. If these unethical employees can continue working without any form of punishment, then nothing will stop a good employee from going bad. The next step is to perform background checks on every employee. If anything from their background checks show that they are at a high risk of unethical behavior, then changes to their employment should be made. The high-risk employees should not be allowed to work on projects that require access to highly sensitive data. Also, a closer monitoring should be done on these employees to ensure that they do not participate in unethical behavior. If they do participate in unethical behavior termination should be done immediately.

NO SEGREGATION OF DUTIES OR MANDATORY VACATION POLICIES (TO MITIGATE INTENTIONAL THREATS)

The biggest reason people perform unethical behaviors is because they feel like they can get away with it. It is easy for people to hide their unethical behavior if they are the only ones performing the duty in question.

The first way to prevent this is to segregate key duties to ensure no one can work by themselves and hide their activities. Another way is to have a mandatory vacation policy in place. There is one method that can allow both policies to be set in place. First an assessment on every role and employee must be done. This will show which roles should be segregated and which employees can help in the segregation of key duties.

Next cross train the employees on each key role and rotate them on a schedule. This way not one employee will be able to stay long enough at any key role to preform unethical behavior without detection. Another benefit from the cross training is that when any employee goes on a monitory vacation, it will be easy to find someone to step in to temporality replace the employee on vacation. Once the employee is on vacation, the replacement employee will be able to notice if there are any unethical activities preformed. If any unethical activities are discovered, then the replacement employee will report the security incident immediately.

Continuous Monitoring Plan

This continuous monitoring plan will address three organizational issues within MUSA Corporation. The first will deal with Work Settings: distractions, insufficient resources, poor management systems, and inadequate security practices. The second will deal with Work Planning: job pressure, time factors, task difficulty, change in routine, poor task planning and management practice, and lack of knowledge/skills/abilities. The third will deal with Employee Readiness: inattention, stress and anxiety, fatigue and boredom, illness and injury, drug side effects, values and attitudes, and cognitive factors.

WORK SETTINGS

Having a strong work settings at MUSA Corporation not only helps employee's overall health but will also increase employee retention. Having happy and healthy employees will increase the overall productivity. Distractions, insufficient resources, poor management systems, and inadequate security practices are the obstacles that are preventing MUSA Corporation from having a strong work setting.

Distractions are a big obstacle in strong work setting. Emails, personal phone calls, the internet, and social media are the biggest distractions in MUSA Corporation. According to BusinessCollective, each distraction can be overcome with a few simple steps. Policies can be created with emails to limit when emails are to be checked and having employees respond in batches. "I'd wrap up 12 hours in the office and feel as though I hadn't accomplished a thing. Now, I only check my messages at 10 a.m. and 4 p.m., and batch my responses. As a result, I am more focused, get considerably more done and when I do go into my inbox, I'm highly effective." (BusinessCollective, 2015) The personal phone calls issue can be addressed by creating a policy of forbidding all cell phone use and any personal use of company phones. Personal calls can be permitted during break and lunch times; with emergencies as a case by case situation. The internet and social media issues can be addressed together. There has to be a policy to block all non-work related internet use during working hours; which includes social media. As with personal phone calls, full internet use will be permitted only during lunch breaks.

Resources are used by employees to accomplish their tasks. If employees do not have the needed resources, then being productive is next to impossible. The only way to overcome this issue is to look at every department and analyze each task. Then from that data determine all the resources necessary to accomplish each task. The hardest part is determining which resources are employee wants and which ones are needs. Once the needs are identified, give the employees what they need.

Management systems, like policies, processes and procedures, are the framework of any organization. The most important part of any management system is documentation. After reviewing current policies, processes, and procedures, create a Standard Operating Procedure (SOP) document for everything. I suggest creating a digital SOP that can be accessed by all employees on the network and any changes will be instantaneously distributed. The continuous improvement program will constantly review these SOP documents, update them, and add new ones as necessary.

Security is only as strong as its weakest link and inadequate security practices are weak links. Training is the biggest way to address these issues. Each month every employee will be required to complete training to address a bad security practice. These topics range from bad password management to identifying phishing attacks. However, there are two inadequate security practices that cannot be overcome by training. The first is a lack of intrusion detection/prevention system and the other is a lack in encryption use. I suggest using a Signature-based IDS system that has some anomaly-based features. This will not only ensure that any past attacks will be unsuccessful but also allow for detection of unknown attacks. IDS sensors will be placed at strategic points on the network to allow for sniffing of every packet passing through the network and alerting any unusual activity. I suggest that all data within any database, including backups, be encrypted. Passwords should be not only encrypted but also encrypted with salt. Also, I suggest that all connections should use end-to-end authentication. This will ensure that all data, and connections are only allowed for authorized users.

WORK PLANNING

Planning is a great tool for success in the workforce. Without the proper planning and tools, employees are just aimlessly working. This can cause employees to face pressure, time issues, and difficulties completing tasks.

First thing that I suggest is to evaluate every employee to assess their skills and knowledge. Once we have a baseline to everyone’s current skill and knowledge, we will train anyone who needs extra help to compete tasks. A lack a knowledge can make easy tasks appear to be more difficult, results in the employee facing time factors, and feeling more pressure than necessary. After every current employee has the training they need, I suggest creating a skill assessment test for any future potential new hire. This will ensure that any new hire will have the skills needed to complete any task needed.

With the evaluation of employees, special care should be placed on evaluating management. Having a bad management team can negatively affect the work environment. If there are management members who are unqualified, then training must to given to ensure that they have the skills necessary to effectively lead their departments. The biggest skill needed for any successful management team is effective planning. Each management team will use tools from the continuous improvement program to hold weekly planning meetings. During these meetings, the current week tasks will be planned to create goals that will meet any timelines for the week. Also, previous weeks' goals will be evaluated to see if the goals were met. If the goals were completed, then new goals will be created. If not, then the goals will be evaluated to find the root cause of the failure.

Another factor in unhappy employees is having a lack of change. To overcome this, I suggest cross training every employee with different tasks. Once enough employees are cross trained, rotation of employees can occur to have a change in routine and to enable full coverage when other employees go on vacation.

EMPLOYEE READINESS

Happy and healthy workers are more productive. A 700-person experiment was conducted to see the effects of workers and productivity. "The experiment showed that productivity increased by an average of 12%, and reached as high as 20% above the control group." (Addady, 2015)

To address health issues among MUSA Corporation employees, I suggest creating a wellness program. The first part of the program will consist of free gym memberships to all employees. This will not only benefit the employee's health, but also their stress levels. The Harvard Medical School conducted a study on stress and exercise. Their conclusion was "Regular aerobic exercise will bring remarkable changes to your body, your metabolism, your heart, and your spirits. It has a unique capacity to exhilarate and relax, to provide stimulation and calm, to counter depression and dissipate stress." (Harvard Medical School, 2011)

The second part of the wellness program will consist of classes to help further manage stress and boredom. These classes will include, stress management classes, yoga classes, and other fun classes. The fun classes will be used to reduce boredom. Based on employee interest, these classes can be art classes, cooking classes, or any other non-work related class in order to prevent employees becoming bored.

Creating a Security Culture

Cyber security is not a difficult goal to achieve. If everyone does their part in the Cyber Security Awareness program, the goal can be achieved even by the least tech savvy person. All the technology related tasks will be performed by security specialists. The rest of the employees only have four main tasks to follow in the cyber security awareness program. Those tasks are:

1. Follow all the Rules of Behavior
2. Report any violations/suspicions
3. Complete all the training and ask for any additional needed training
4. Participate in the wellness program

It may seem too simple to succeed, but these tasks will help reduce the number of security gaps. The Rules of Behavior will reduce the risks of unauthorized resource use, help employees create and use strong passwords. The anonymous reporting system and reward program will ensure that if violations do occur, then those violations do not become major security risks. This will also reduce the number of thefts. The training will ensure that every employee will have the knowledge needed to keep the workplace secure. Finally, the wellness program will ensure that every employee is healthy and happy. Healthy and happy employees are not only more productive, but less likely to become an insider threat.

Messaging Strategies for Senior Management

Cyber threats are growing at a rapid pace. We no longer live in a time where anyone can ignore cyber threats and have the "it's not going to happen to me" attitude. According to Forbes contributor, Steve Morgan, "In 2015, the British insurance company Lloyd's estimated that cyber-attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts over the past year put the cybercrime figure as high as $500 billion and more." (Morgan, 2016)

The two most known data breaches are the Target and Home Depot breaches. Both attacks are totaling expenses of more than 500 million. The breach-related expenses included investigation expenses, the costs of providing customers with credit-monitoring and identity-protection services, extra customer service, legal costs, and claims from the card networks on behalf of issuers to cover fraud losses and card re-issuance, as well as network assessments, or fines.

According to USA Today both the Target and Home Depot data breaches were due to stolen log-in credentials. "Hackers used a vendor's stolen log-on credentials to penetrate Home Depot's computer network and install custom-built malware that stole customer payment-card data and e-mail addresses… In January, Target announced that hackers who also used a vendor's sign-in credentials to install malicious software and steal data on 40 million credit and debit cards, in addition to personal data for up to 70 million customers, including e-mail addresses." (Winter, 2014)

The biggest lesson to be learned from these two data breaches is that both could have been avoided by having a strong Cyber Security Awareness program in place. The attack relayed on the stolen credentials; which probably was obtained through a phishing attack. The Awareness program would have prevented the attack through the following:

- Training to identify and prevent phishing and social engineering attacks
- Collecting and analyzing logs to identify unusual activity
- Placing a media access control policy to prevent attackers from gaining total access
- Using encryption and hashing to control data flow
- Conducting vulnerability assessment to identify and patch security gaps

Ultimately the question that needs to be answered is, would the cost of not securing sensitive data outweigh the cost of securing the data? It is true that Information Assurance comes at a cost. However, a cyber security awareness plan should be viewed more as an investment and not an expense. The return on the investment would be:

- More secure work environment
- A better reputation (due to fewer data breaches)
- A more trustworthy staff of employees
- A happier and more productive workforce

References

Addady, M. (2015, October 29). *Study: Being happy at work really makes you more productive*. Retrieved from Fortune: http://fortune.com/2015/10/29/happy-productivity-work/

BusinessCollective. (2015, June 17). *8 Ways to Overcome Your Biggest Distractions*. Retrieved from TIME: http://time.com/3923289/overcome-workplace-distractions/

Harvard Medical School. (2011, Feburary). *Exercising to relax*. Retrieved from Harvard Health Publications: http://www.health.harvard.edu/staying-healthy/exercising-to-relax

Morgan, S. (2016, Jan 17). *Cyber Crime Costs Projected To Reach $2 Trillion by 2019*. Retrieved from Forbes: http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#3f3112ed3bb0

Winter, M. (2014, November 7). *Home Depot hackers used vendor log-on to steal data, e-mails*. Retrieved from USA Today: http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/