Security Awareness Program Proposal

The purpose of this proposal is to make the company and the employees aware of the current vulnerabilities discovered in the network. It is important that these vulnerabilities in the network are addressed to ensure network security and safety. Security awareness is one of the most important aspects in network security. It is vital that employees understand the risk associated with phishing and social engineering and the damages they can do to a network. It is estimated that phishing attacks on large business can collect up to 3.7 million dollars per attack. Small businesses typically have less resources making it easier to attack regularly. As seen in the collected vulnerabilities chart there are many reasons that there is a need for this new security awareness program as well as changes to the overall network security. Having no way to gather data and analyze it creates a risk of improper usage of work tools and network including the risk of malware from unauthorized site access.

Overall the security posture of the organization falls short in many regards. There doesn’t appear to be any accountability for the overall protection of the network. Among the many vulnerabilities found it appears the biggest gaps in the security are setting the company up for many security issues. Among these most important gaps is the lack of intrusion detection or prevention, no encryption or hashing to control data flow, very infrequent vulnerability assessment to ensure the company is following global best practices. Along with the flaws in the network security there are many potential risks associated with the lack of employee awareness and training, including a high number of thefts reported causing low company morale leading to a high turnover rate.

There are also many human factors which are affecting the security climate of the organization. The lack of any cyber security awareness training to go along with the high turnover rate there is a high chance that employees do not understand the dangers of responding to unknown emails or accessing sites or applications they are not meant to access while at work. To go along with this point there is configuration change management policy which helps reduce unintentional threats. This would be important because it helps to plan, evaluate, review and approve any changes to the security policy before implementation leading to added vulnerabilities. Following a plan to the change will make sure that there are no compliance requirements being skipped over or negative effects caused from the changes.

Organizational factors which are contributing to the negative security in the organization is the lack of any encryption or control of data. This is leading to a high potential of unauthorized alteration of data including access of data by users who are not meant to have authorization. Not having any control on media or collection of logs leads to potential of employees gaining access to private information without any way of tracking the changes or information they are gathering from the time using it. This leads to a breach in privacy on potentially vital files which are meant to be accessible only by specific higher ups. Disgruntled employees who may have gained access could do things to have revenge which could be the reason for the high number of theft or security incidents reported.

Overall there are many vulnerabilities that will need to be fixed to raise the organizations security posture and awareness of security risks that the employees can cause unintentionally. Many of these changes to employee readiness and training about network security can significantly improve overall security just by ensuring all employees are continuing to be trained in new risks and how to manage/avoid them before they occur.

Overview:

Network/Cyber security is vital to a network to keep a business functioning while maintaining confidentiality, integrity, and availability. There are many risks out there, with hackers in the world constantly looking to take advantage of unsecured network, or unsuspecting employees.

Purpose: These policies are to help maintain a secure network and the teach the importance of each employee to a networks privacy/security. These rules and requirements are meant to create a well-trained employee base which can spot any risks, or vulnerability before accidentally giving away private or personal information protecting against unintentional and intentional threats.

Scope: This policy applies to all employees, including management of Multiple Unite Security Assurance (MUSA) Corporation. This applies to anyone using the secure network, workstations, or sending/ receiving emails while connected to the work network.

Policy 1: It is the responsibility of every employee to undergo mandatory cyber security awareness training, this will include annual re-trainings, or updates to any current security risks that are found. It is expected that all employees will participate and maintain security after training.

Compliance: The team will demonstrate compliance through mock phishing, social engineering attempts which will test that they are following the proper procedure to ensure the network is protected. Upon failure the employee will be assigned to mandatory retraining, where they will relearn the basics and importance of protecting against phishing, social engineers.

Overview: A Configuration change management policy is an important tool to reduce the risk of unintentional threats to a network. It is one of the top strategies to ensure that changes to the network or configurations do not leave vulnerabilities.

Purpose: The purpose of this policy is to create a path that all changes must go through while also identifying the kind of changes being made ranging from repeatable changes which do not need to follow as many steps, normal changes which should follow the entire path, and emergency changes which need to get pushed through as soon as possible. This will protect the network from a change causing issues with the network by reducing the risk of missing any vulnerabilities that may arise from improper coding or software changes in general.

Scope: This will be mandatory of any person in IT, or any other department which may be making changes to the network, IT systems, policies, or anything that could affect customers and employees.

Policy: Every change made must follow the Change Management policy which includes Planning, evaluation, review, approval, communications, implementation, documentation, and post-change review steps. Every step should be followed and finished before moving on to the next phase to ensure that all aspects of the network change are carefully executed and reviewed. If a change is an emergency and needs to be moved to an urgent list, then it will get reviewed and skip earlier phases and given a longer post-change review period.

Compliance: All employees must follow this policy through all changes being made. Verification will be made through information gathering, business reports, internal audits, and through management. Anyone found violating this policy is subject to disciplinary action including termination

Overview: A company policy with a clear guideline to prepare and react to any intrusion into the company’s network will help to mitigate any damages while also being able to protect any vital or private company or employee information.

Purpose: The purpose of this policy is to establish guidelines which will allow intrusions to be detected quickly. Along with quickly catching any intrusion attempts we will establish procedures to have faster reaction, and counteracting times. It will be an important tool towards mitigating any network intrusions.

Scope: This policy applies to the entire business network, servers, and all employees using devices (personal, workstations) on the company’s network. It also applies to any employee or contractor working to monitor the network and servers or working to resolve any intrusions.

Policy: The policy requires the company to implement and use an intrusion detection/prevention system on the network including on all computers/workstations. There will be constant monitoring on the network to protect against intrusions. Any computer or workstation will be monitored and if an intrusion occurs it must be mitigated by reacting quickly and counteracting any potential damages that can occur.

Compliance: To maintain compliance there will be consistent checks on all workstations by IT personnel. This will ensure that all workstations are running an updated antivirus/malware software including other necessary tools to detect intrusions. There will be monitoring of antivirus software and if you are caught with your software disabled manually you will be subject to discipline including and up to termination. If it is off due to technical issues it will be setup and monitored.

Overview: Many threats come from inside the network through employees either intentionally or unintentionally. It is important to set up a firewall and maintain logs as well as analyzing the data gathered in the logs.

Purpose: The purpose of this policy is to create a guideline and requirements for log collecting. Setting the requirements for what should be logged and for how long. Collecting and analyzing logs will allow us to spot any attempts to breach the network, as well as any attempts to gain access to information not allowed by employees at certain positions. Being able to see who has accessed the network is important to because you can see what everyone is doing inside the network. This allows you to filter and find a security breach that may have occurred.

Scope: This will affect all employees because they need to be aware of the data that will be collected ensuring they do not do anything they aren’t allowed to. It will be most important for the IT group because they will be the ones setting up the log collection and analyzing the data that is collected.

Policy: All attempts to log into the network, access internal applications, make changes to files, policies or organization roles will be collected. It will be mandatory that all data is monitored and audited to continue to provide strong network security. Collected data will be used to pinpoint unauthorized access or attempts to the network. Data will be stored in a separate server only accessible to the group designated to analyze them.

Compliance: Continued monitoring and collecting data is a must. If found to not be gathering information there will be punishment, including training, probation, and continued monitoring by management until compliant. Any unauthorized attempts will be punished with warning/termination.

Overview: Removable media, social media, and unauthorized workstation use for applications can be sources of malware/viruses leading to loss of sensitive information or vulnerabilities to the network.

Purpose: MUSA Corporation aims to minimize the risk of data loss and exposure through internal use. By implementing this policy, we are reducing the likelihood of malware/viruses picked up from unauthorized sites, removable media being used on a work station. Through stricter policy’s we can protect sensitive information which in turn protects the company from fines which could be handed out due to a data breach.

Scope: The policy is to be followed by users on all workstations, laptops, or device connected to the corporate network/servers. This includes any work laptop which may be taken off site.

Policy: All USB devices or other form of removable media must not be used without prior IT management approval. There is to be no use of social media or any other unauthorized website not dedicated to a work task. Correspondence should be kept to internal email/chats only with no emailing for personal use.

Compliance: If caught using unauthorized media you will first be given a final warning, which will be the first and last warning you will receive. Any continued non-compliance will be handled by punishment including suspension, probation and up to termination. To continue monitoring of compliance logs will be kept showing which sites have been accessed by each employee login, and workstations will be checked for media devices plugged in by management.

Overview: Data flow is important for any business. Because of the amount of data that is sent via email between senders and receivers there needs to be a way to protect that data from the possibility of a third party accessing it. It is important that all data being sent via or stored on servers is first encrypted using best practices including hashing.

Purpose: The purpose of this policy is to protect sensitive information being sent over email as well as any information being stored on the servers. If anyone was to gain access to the emails in transit they would only be able to see an encrypted version of the email, which is unusable without having the security keys necessary to authenticate access. This protects the company receiver from getting an email which has been intercepted and altered in transit causing potential damage to the company. Storing encrypted and hashed data on the servers will protect the server incase of a hack/data breach. It will protect that data by making it unusable. In case of a person getting access to the information using stolen verification it is important to also separate connected data such as passwords and email addresses if collected.

Policy: All data being sent and stored will be double hashed before storing in the server. All emails being sent must be sent using shared key encryption using a secure network. There should never be emails sent that are not first encrypted.

Compliance: Because of the importance of data security all emails especially emails with sensitive information is required to be encrypted. If emails are not encrypted it will lead to punishment starting with awareness training, to termination. Security is the primary concern in the company. Compliance will be kept through auditing, and continued training of the importance of data security.

Overview: Keeping up with the current security environment is important in a constant battle to protect networks from vulnerabilities to minimize the risk of a data breach. Vulnerability management and assessment is vital for proper information security. It should consist of assessment, identification, and remediation of any vulnerabilities found.

Purpose: The purpose of this policy is to authorize members of IT or outside security contractors to do vulnerability assessment to find any potential gaps in our network which need to be addressed. Without consistent checks the network will be at risk because of new hacking methods.

Scope: This policy will cover vulnerability assessment to be conducted on every asset of the business network, including products and services.

Policy: There will be a security Operations team which is responsible for the development and execution of vulnerability assessments on a 3-year cycle. This will be over looked by the Chief Security Officer. MUSA employees are expected to cooperate with vulnerability assessment, and any vulnerability scans outside the managed assessment tool must be given authorization by the Security Manager.

Compliance: Any MUSA employee found to have violated policy will be disciplined with potential of termination and legal action. To ensure compliance there will be an assigned security team to run the task overseen by an assigned Operations Security manager and The Chief Security Officer. A full vulnerabilities assessment will be carried out and reviewed every 3 years with smaller checks every year looking to fix newly found exploits from similar companies. The Management and employees overseeing the assessment will be held accountable for the task.

Overview: Employee importance and high morale will increase security in the network by increases employee involvement and willingness to learn and improve. It is important that all employees feel welcome and ready for the tasks assigned to them upon starting, with continued growth training over time. Work planning strategies will give employees focus, priorities, and improve business operations.

Purpose: The purpose of this policy is to reduce the high turnover rate and low morale within the company that we are currently experiencing. By improving employee training, readiness, and giving them help setting up planning strategies we can ensure our employees will be happier in the long run which also provides a more satisfactory level of work contributed by each employee. Increased security awareness, phishing and social engineering training will not only ensure they are doing a good job but improve defense against unintentional treats as well.

Scope: All management will be required to provide proper training to new employees and continue keeping each employee current on new and important information.

Policy: All management will assign and monitor new employee training, readiness, and security training. Continue to implement new methods to keep employee moral high. When an employee’s morale begins to fall the management shall do what is necessary to increase employee happiness by improving relations, training, or planning.

Compliance: Continue compliance will be monitored by upper management reviewing numbers on employee moral surveys and turnover rates. If numbers are not to the standard expected or improving, we will continue implementing ways to continue to improve. Non-compliance to help new employees or personally responsible for hurting morale will lead to punishment including probation, suspension, and up to termination.

Overview: Theft reports and security incidents are currently at a higher number than expected. These issues can be caused by many things including disgruntled employees or even unethical employees.

Purpose: The purpose of this policy is to reduce the total number of theft reports and security incidents. Through improved relations with employees and proper training we can reduce the risk of disgruntled employees, and with added security we can help cut back on theft. These problems will improve the workplace while helping to protect the company.

Scope: Theft policies will apply to all staff with a high standard of compliance with everyone. Reducing security incidents is also meant for all employees, contractors, or visitors in the facility or using the network.

Policy: Background checks will be done before all employees are hired, reducing the likelihood of hiring someone who may be a thief. Security cameras must be setup in the workplace in areas where there are doors to the outside, or shared storage areas. IT will monitor and audit employee work related activities to protect against security incidents caused by disgruntled employees. Training about security importance will be mandatory and used to monitor employees being disgruntled, where we can try to reduce risk caused by them.

Compliance: If theft is caught there will be immediate termination and charges placed against the employee caught. If an employee who is disgruntled leads to a security incident action will be taken including mandatory vacation/suspension without pay, termination and potential lawsuits depending on level and cause of incident. Continued security analysis and reports will be gathered on employees to ensure compliance, with training toward an ethical work place.

Overview: Intentional threats can be controlled within a workplace through proper assignment of duties and training. It is important that no person has control over multiple tasks which are considered incompatible. This will reduce the risk of approving things which may not be authorized.

Purpose: By using proper segregation of duty MUSA will be able to reduce the risk of intentional incidents from an employee using the system for personal gain. By having multiple layers of approval and different departments required to approve tasks it can ensure that there are no internal theft, crime, or other problems which could occur with one person being given to much power. It is also mandatory that the company start handing out mandatory vacations which will help reduce the risk of internal threats as well. By doing mandatory vacations you can track any fraud based on when it occurs and does not occur based on who may be present or on vacation.

Scope: Mandatory vacation will be required by all employees of all levels to ensure fairness, and all levels will be given proper segregation of duties to ensure there are no overlapping job tasks which may cause problems.

Policy: The must be a designated Role Administrator who assigns roles within MUSA to ensure that all employees are given proper roles with no overlap of responsibility. If internal fraud is suspected management will assign mandatory vacations at the end of the year to employees 1 by 1 to reduce the risk of internal fraud.

Compliance: Review of job roles will happen monthly/yearly to ensure no tasks and roles overlap, and management will set up a method for mandatory vacation. If an employee refuses mandatory vacation they may be suspended without pay, or terminated.

Between all these policies I believe that the company will reduce many of the vulnerabilities which have been found in the report. With further employee training we can reduce the risk of intentional and unintentional threats, by ensuring everyone knows the proper security methods to help protect the network. Social Engineering training should be constant with practice attempts taken without employee knowledge to test their awareness and ability to spot social engineering attempts. To protect communication between sender and receiver there will be a shared key which required password authentication which will unlock the encrypted messages being sent. This will allow for a more secure message system protecting from data alteration.

**Introduction**

Continuous monitoring of the organization is an important way to reduce the likelihood of any malicious activities that would harm the network, including both intentional and unintentional threats. By setting up a continuous monitoring plan Multiple Unite Security Assurance (MUSA) Corporation will have guidelines to follow as well as an overall strategy to ensure that the network is secure by planning for all vulnerabilities.

Through research headed by the new chief information security officer it was found that much of the risk to the organizations network, data and access are at risk because of internal factors and threats. Many of these risks come from the side effect of untrained employees, who lack common knowledge and importance of cyber security awareness. Other risks are due to malicious activities which are being done intentionally by employees who may be retaliating or looking to gain profit from the company due to being disgruntled.

There are multiple tools MUSA can incorporate to reduce the threat associated with employees having access to data. Because internal threats require access to authorized user accounts it is important to eliminate threats due to lack of managing access to users. It is also important to find and fix any other security gaps found on the network.

**Tools**

There should be a priority to use a tool which will help secure the network starting with the network’s users. UserLock looks to be a tool which could help with protecting the network from people gaining access to employee’s logins and help reduce non-authorized logins.

UserLock can set restrictions to user accounts including controlling origin of login, time restrictions, session types, and even limit how many logins can be going at a time. If any attempts to log in outside of the regular usage will be detected immediately allowing to quickly block user access. All logins will be quickly auditable allowing you to review any past logins to quickly identify any possible breaches.

UserLock will protect against stolen credentials by limiting where a person can login and how many times the same account can login. It can recognize the user’s normal activities responding to unusual use of the account while quickly reporting those unusual activities to the system administrator. Having control over the network’s user accounts reduces the risks of unintentional threat due to password sharing, lost password, and even phishing by quickly responding to suspicious activity.

Internal threats aren’t the only thing an organization must prepare to defend against. Malware and viruses can due large amounts of damage to a network if the organization is not prepared to mitigate the damage they can do.

Avast Business Antivirus Pro Plus looks to be a great option for a business looking to protect from outside threats. By offering a two-way firewall, virtual private network, data shredder, and a password manager it appears to be a great all in one protection from external threats. Protecting the network from the constant threat of new malware and viruses is important and Avast is dedicated to trying to keep ahead of the new threats. The VPN feature allows any contractors, or employees working offsite to quickly log in through a secure network which encrypts anything done on the connection protecting them from un intentional breaches over an unsecured network. Avast can also protect the network using content filtering which can quickly block potentially dangerous applications, programs and websites. These tools will protect the network from users using inappropriate sites while at work. It will log and collect any data that is being used over the network through the firewall while also encrypting passwords and information being transferred over the network ensuring that all information is protected.

To help reduce the risk of intentional internal threats it is important to implement an employee readiness strategy that targets the employee’s skills, happiness, health, fatigue and boredom. To do this it is important to cut back on work place distractions. Placing employees in appropriate work spaces where privacy is available is important to reduce distractions from other employees. There also needs to be a policy in place that will reduce the use of outside devices like cellphones. We can increase resources towards necessary work needs including annual training to improve the companies over security awareness. This will help to improve all employees understanding of cyber security protocols and the dangers of phishing and social engineering. It is important during these trainings to incorporate fun and interesting methods to improve employee engagement that improves happiness and overall learning.

To help with work planning and control it is important to have policies in place that set out easy to follow methods and guidelines for work tasks. Having simple to follow training documents will allow employees to use free time to look up ways to improve the task they are doing. This will help to reduce the stress of the employee by making them feel less stress and anxiety due to feeling left behind in training. Management should also be knowledgeable in tasks assigned to their employees in case the employees seem to be stressed from task difficulty, allowing them to quickly step in to answer questions and offer help when needed. Knowing how to plan out a task before hand will help set up a realistic timeline while also reducing wasted time. Timelines will also create accountability of management, which creates a need for them to be more interested in the daily work and the quality of work being produced by their direct employees. By working closely with their employees, management can quickly assess the level of skill of the employee and assign trainings to get them caught up if they are beginning to feel behind or stressed from lack of knowledge.

Employee Readiness is important, especially in the day and age of high stress lifestyles, lack of nutrition, and many other issues which can affect the level of work an employee can provide. To combat stress and anxiety in the workplace there will be mandatory breaks that are given to all employees. During this time the company will offer stress relief through an onsite gym, games, healthy food/snack bar, and a bunch of comfortable furniture.

To reduce stress the company will hold employee parties that will give out accomplishment awards and recognition for the hard work of the employees. Small group activities will reduce stress at work while also building upon employee’s interest in work. This will help with fighting boredom by allowing employees to mingle and get to know each other outside of typical work talk. To reduce fatigue, illnesses, and injuries we will have seminars that train employees about the benefits of good nutrition, proper workout techniques, and methods to avoid work related injuries such as back pain or ergonomic pain. Increasing employee happiness and knowledge will begin to allow employees to perform their jobs better, reduce stress related illnesses, and protect the companies most important assets, their employees.

It is important to continuously check on the status of employees and the network, always looking out for any potential vulnerabilities which may arise. Through these methods MUSA will quickly be able to identify and issues which may arise and work to combat it before it becomes a problem, both internal and external.

**Introduction**

Continuous monitoring of the organization is an important way to reduce the likelihood of any malicious activities that would harm the network, including both intentional and unintentional threats. By setting up a continuous monitoring plan Multiple Unite Security Assurance (MUSA) Corporation will have guidelines to follow as well as an overall strategy to ensure that the network is secure by planning for all vulnerabilities.

Through research headed by the new chief information security officer it was found that much of the risk to the organizations network, data and access are at risk because of internal factors and threats. Many of these risks come from the side effect of untrained employees, who lack common knowledge and importance of cyber security awareness. Other risks are due to malicious activities which are being done intentionally by employees who may be retaliating or looking to gain profit from the company due to being disgruntled.

There are multiple tools MUSA can incorporate to reduce the threat associated with employees having access to data. Because internal threats require access to authorized user accounts it is important to eliminate threats due to lack of managing access to users. It is also important to find and fix any other security gaps found on the network.

**Tools**

There should be a priority to use a tool which will help secure the network starting with the network’s users. UserLock looks to be a tool which could help with protecting the network from people gaining access to employee’s logins and help reduce non-authorized logins.

UserLock can set restrictions to user accounts including controlling origin of login, time restrictions, session types, and even limit how many logins can be going at a time. If any attempts to log in outside of the regular usage will be detected immediately allowing to quickly block user access. All logins will be quickly auditable allowing you to review any past logins to quickly identify any possible breaches.

UserLock will protect against stolen credentials by limiting where a person can login and how many times the same account can login. It can recognize the user’s normal activities responding to unusual use of the account while quickly reporting those unusual activities to the system administrator. Having control over the network’s user accounts reduces the risks of unintentional threat due to password sharing, lost password, and even phishing by quickly responding to suspicious activity.

Internal threats aren’t the only thing an organization must prepare to defend against. Malware and viruses can due large amounts of damage to a network if the organization is not prepared to mitigate the damage they can do.

Avast Business Antivirus Pro Plus looks to be a great option for a business looking to protect from outside threats. By offering a two-way firewall, virtual private network, data shredder, and a password manager it appears to be a great all in one protection from external threats. Protecting the network from the constant threat of new malware and viruses is important and Avast is dedicated to trying to keep ahead of the new threats. The VPN feature allows any contractors, or employees working offsite to quickly log in through a secure network which encrypts any thing done on the connection protecting them from un intentional breaches over an unsecured network. Avast can also protect the network using content filtering which can quickly block potentially dangerous applications, programs and websites. These tools will protect the network from users using inappropriate sites while at work. It will log and collect any data that is being used over the network through the firewall while also encrypting passwords and information being transferred over the network ensuring that all information is protected.

To help reduce the risk of intentional internal threats it is important to implement an employee readiness strategy that targets the employee’s skills, happiness, health, fatigue and boredom. To do this it is important to cut back on work place distractions. Placing employees in appropriate work spaces where privacy is available is important to reduce distractions from other employees. There also needs to be a policy in place that will reduce the use of outside devices like cellphones. We can increase resources towards necessary work needs including annual training to improve the companies over security awareness. This will help to improve all employees understanding of cyber security protocols and the dangers of phishing and social engineering. It is important during these trainings to incorporate fun and interesting methods to improve employee engagement that improves happiness and overall learning.

To help with work planning and control it is important to have policies in place that set out easy to follow methods and guidelines for work tasks. Having simple to follow training documents will allow employees to use free time to look up ways to improve the task they are doing. This will help to reduce the stress of the employee by making them feel less stress and anxiety due to feeling left behind in training. Management should also be knowledgeable in tasks assigned to their employees in case the employees seem to be stressed from task difficulty, allowing them to quickly step in to answer questions and offer help when needed. Knowing how to plan out a task before hand will help set up a realistic timeline while also reducing wasted time. Timelines will also create accountability of management, which creates a need for them to be more interested in the daily work and the quality of work being produced by their direct employees. By working closely with their employees, management can quickly assess the level of skill of the employee and assign trainings to get them caught up if they are beginning to feel behind or stressed from lack of knowledge.

Employee Readiness is important, especially in the day and age of high stress lifestyles, lack of nutrition, and many other issues which can affect the level of work an employee can provide. To combat stress and anxiety in the workplace there will be mandatory breaks that are given to all employees. During this time the company will offer stress relief through an onsite gym, games, healthy food/snack bar, and a bunch of comfortable furniture.

To reduce stress the company will hold employee parties that will give out accomplishment awards and recognition for the hard work of the employees. Small group activities will reduce stress at work while also building upon employee’s interest in work. This will help with fighting boredom by allowing employees to mingle and get to know each other outside of typical work talk. To reduce fatigue, illnesses, and injuries we will have seminars that train employees about the benefits of good nutrition, proper workout techniques, and methods to avoid work related injuries such as back pain or ergonomic pain. Increasing employee happiness and knowledge will begin to allow employees to perform their jobs better, reduce stress related illnesses, and protect the companies most important assets, their employees.

It is important to continuously check on the status of employees and the network, always looking out for any potential vulnerabilities which may arise. Through these methods MUSA will quickly be able to identify and issues which may arise and work to combat it before it becomes a problem, both internal and external.

A business that hopes to survive in the modern world must do it’s best to continuously improve upon their security. In a world of ever-changing vulnerabilities and security flaws, there is a need for constant research and implementation of new defenses. No matter how great your defenses are it is important to plan for the potential of an insider attack which can hurt even the most secure network without warning.

This is the reason that every company should implement a security awareness program to help combat any risks that include un-intentional threats and intentional threats. As cybercrime becomes more common it is predicted that cybercrimes will cost businesses around $6 trillion annually by 2021, up from $3 trillion in 2015 (Cybercrime Magazine, 2019). The average cost of a data breach per company in 2013 was about $5.4 (Ponemon Institute, 2013). Even with that amount of money being lost per attack the real damage is done through the damage to a business’s reputation after a breach, especially if it is found that the company was not using a strong posture against cyber security to protect its employees and customers.

Because of the damage a business can go through during and after a security breach it is important to create a great communication plan. Gaining the support of important senior management and stake holders toward implementing a security awareness program should be the priority of the communication plan. The communication plan should be written based on the people you are writing it for. This should allow you to write in a way that is most effective to interest the group and help to gain their support.

There are two major ways to write a communication plan. They can be in a persuasive style where the attempt is to convince the audience of what you want or in a more motivational style where you attempt to inspire the group. I think that a communication plan for improving security should find a way to persuade the group that it is in their best interest to improve the security posture and support changes to security throughout the company.

Security awareness training has many benefits that will help improve the overall security of the company. Education of employees will reduce the likelihood an employee will make a mistake and unintentionally lead to a data breach. A recent study showed that around 80% of breaches are caused by employee carelessness. Training the employees about scams, phishing, emails containing malware and the risk of allowing strangers into secure areas will better prepare them for taking actions to prevent unintentional leaks. Increasing the training doesn’t just enhance security of the company and employees but it helps to increase company morale. An employee who is trained in security and what to do to stay safe can increase job satisfaction and job retention by reducing embarrassment that they may have gotten scammed. Another key reason for needing to improve security awareness is that it will save money and improve compliance. By staying ahead of security vulnerabilities there is less risk of being breached, which tends to take longer than 7 months to recover from and around $955,429 to do upgrades and replacements. Staying compliant with data protection policies that are mandatory will reduce the possibility of lawsuits and fines (Infosec Resources, n.d.).

Adding employee training and readiness is one of the most important ways to protect a company but there is also the threat of intentional attacks. It is important to convey the importance of preparing for both internal and external threats that could cause harm to the company. Senior management and stock holders may be against spending money on something they don’t think is important, so persuading them that the cost of upgrades and training to the network security is an important expense. Show them ways that the company will save money in the long run by using the money as an investment toward protecting itself from future threats.

To convince stakeholders and management that it is important to have a healthy security culture with proper funding we must show them examples of data breaches and the effects they had on companies during and after. Examples like Target and Home Depot who were breached due to an internal leak from a vender who was given access to the network. A few simple trainings about protecting passwords and basic security could have helped these companies save millions including the effort spent trying to avoid lawsuits after the breach. By continuously monitoring our network with firewall logs, access controls, and encryption we can ensure that we are up to date with industry wide best security practices and compliant with cyber laws. If the company is dealing with customers who are based out of the EU, there needs to be precautions taken to protect their personal information to comply with General Data Protection Regulation (GDPR). Encrypting all data being transmitted through email and being stored must be encrypted. By encrypting the data, it makes the information useless without first getting the key to authenticate. This will protect both the sender and the receiver by protecting the data to ensure it has not been tampered with before being received.

By implementing the policies to improve security training, log data, set user controls, improving employee morale, and other practices to improve the security of the company it will ensure that the company is able to be successful for many years to come.

It is important that all employees want to contribute to a healthy security culture within the company and to have the support of the stakeholders too. It is important to make the presentation easy to follow for those who may not have a background in computers, security, or other technical positions. By creating different methods to get the stakeholders interested in the material, as well as getting them involved they will be able to see the importance of creating the best security possible for a company. These methods to get stakeholders involved should include charts, power points, trivia style games, and even competitions between them to keep them interested and wanting to learn more. While trying to gain approval it is important to use real world examples of breaches that relate to the company. Show the stakeholders the importance of being ahead of their updates and vulnerabilities when dealing with security.

Overall it is important that the communication plan is easy to understand and gets the management and stakeholders to back the plan to improve the company’s security. Gain the trust of the stakeholders and management by laying down a plan that they will be able to follow. Setting up a timeline for training, antivirus/malware, firewalls, and access control will give the company a guideline to follow as well as a possible cost estimate to take the steps to improve security.

Cybercrime Magazine. (2019). *Cybercrime Damages $6 Trillion by 2021*. [online] Available at: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>.

Ponemon Institute. (2013, May). 2013 cost of data breach study: Global analysis. Retrieved from <https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf>

Infosec Resources. (n.d.). *7 Benefits of Security Awareness Training [Updated 2019]*. [online] Available at: <https://resources.infosecinstitute.com/7-benefits-of-security-awareness-training/#gref>.

IS Decisions. (2019). *Windows Server Network Software. Secure & Control all Authenticated Users Access.*. [online] Available at: <https://www.isdecisions.com/products/userlock/>.

business.com. (2019). *The Best Antivirus and Internet Security Software Reviews of 2019*. [online] Available at: <https://www.business.com/categories/best-antivirus-and-internet-security/>.

Avast.com. (2019). *Business VPN, Password Protection - AVAST Antivirus Pro Plus*. [online] Available at: <https://www.avast.com/en-us/business/products/business-antivirus-pro-plus>.

Slideshare.net. (n.d.). *Continuous monitoring strategy\_guide\_072712*. [online] Available at: <https://www.slideshare.net/tphan847/continuous-monitoring-strategyguide072712>.

FraudWatch International. (2019). *What is Cyber Security Awareness Training & Why is it so Important?*. [online] Available at: <https://fraudwatchinternational.com/security-awareness/what-is-cyber-security-awareness-training/>.

Is.oregonstate.edu. (2019). [online] Available at: https://is.oregonstate.edu/sites/is.oregonstate.edu/files/projects/change-management-policy.pdf [Accessed 14 Apr. 2019].

Luc.edu. (2019). *Vulnerability Assessment Policy: Information Technology Services: Loyola University Chicago*. [online] Available at: <https://www.luc.edu/its/aboutits/itspoliciesguidelines/vulnerability_assessment_policy_.shtml>.

EC-Council Official Blog. (n.d.). *The Risks of Phishing to Organizations | EC-Council Official Blog*. [online] Available at: https://blog.eccouncil.org/the-risks-of-phishing-to-organizations [Accessed 30 Mar. 2019].