Multiple Unite Security Assurance (MUSA) Corporation:

Security Awareness Program Proposal

Jeremy Willett

**Purpose**:

The goal of this proposal is to establish, explain, and demonstrate the need for a security awareness program at Multiple Unite Security Assurance (MUSA) Corporation. “Security awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches” (Mimecast, 2022). As an information technology and security company, all users in the company use company systems to perform their jobs. With the use of technology and systems comes the risk of cyberattack. “A successful IT security program consists of: 1) developing IT security policy that reflects business needs

tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and 3) establishing processes for monitoring and reviewing the program” (Wilson & Hash, 2003).

Several studies have been performed by various entities to put into perspective the costs that are attributed with failure to secure and protect company systems and networks. “The 2021 "Cost of a Data Breach Report" from IBM and the Ponemon Institute put the average cost of a data breach among the surveyed companies at $4.24 million per incident -- up from the prior year's cost of $3.86 million and the highest cost in 17 years” (Pratt, 2021). The cost of a data breach is substantial but there are more forms of cyber-attacks companies are vulnerable to. “Verizon's "2021 Data Breach Investigations Report" studied 29,307 incidents and reported a total of 5,258 confirmed data breaches had occurred, up from 3,950 confirmed breaches out of 32,002 incidents reported in 2020. The Internet Crime Complaint Center also reported a spike in cyber incidents in its 2020 report. Phishing attacks reportedly jumped from 114,702 in 2019 to 241,342 in 2020, along with 19,369 business email compromise and email account compromise complaints filed with adjusted losses of more than $1.8 billion. According to "The State of Email Security Report" from IT security firm Mimecast, more than 60% of companies surveyed suffered a ransomware attack in 2020. It reported a 64% increase in email threats in 2020, with 79% of organizations claiming lack of cybersecurity preparedness hurt them” (Pratt, 2021).

By implementing a security awareness program, the aim is to provide all users the awareness necessary to understand the need for and responsibility associated with security. The National Institute of Standards and Technology (NIST) defines awareness as “Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly” (Wilson & Hash, 2003). From the baseline of awareness through the company, the program then moves to training and education. “The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues” (Wilson & Hash, 2003). As recommended by the NIST, following a continuum approach to security awareness and training allows for constant advancement and progression in establishing a culture around information security throughout the company. With every staff member on board, the company can implement and maintain a culture of information security.

**Security Posture**:

The MUSA Corporation has multiple security gaps leading to an almost complete lack of security posture. These security gaps range from human caused vulnerabilities to organizational vulnerabilities. “The security posture of a business refers to its overall ability to recognize and react to cyberattacks. It involves looking at all aspects of a business's network and identifying potential weaknesses. This includes all the network components, users, and any stored information that could potentially be stolen. It also involves looking at current security procedures and software and determining their ability to repel attacks” (Nesbo, 2022). Security posture can be compared to company readiness for a cyberattack. Security gaps have been identified that illustrate the lack of preparedness of MUSA Corporation in response to a cyber-attack.

To begin, there is no cyber security awareness training of any kind. This leaves the company open to social engineering attacks such as phishing attempts. Without security awareness training, employees are not taught what to look out for to prevent falling victim to attacks that prey on human weakness and ignorance. The company also has no intrusion detection and prevention system. This amplifies the effects of falling victim to social engineering attacks by having no system in place to detect and respond if the system is accessed without authorization. There is no media access control (MAC) policy in place at the company. Without a MAC policy, anyone can log onto the company network with any device and have no restrictions applied to their access of the network. This is amplified by a lack of log collecting and analysis. Without network log collection, there is no fall back to trace what is happening on the network and by whom. Couple this with the lack of encryption to control data flow and data alteration and the company’s network is effectively a haven for anyone who wants to access, alter, and steal data from the company. These are further amplified by the lack of configuration change management policy. The lack of configuration change management policy means anyone can alter the company network and its protocols. This leaves the company extremely susceptible to ransomware and a complete takeover and lock out of the system. A system vulnerability assessment is conducted once every three years, with the rapid changing environment cyberthreats, the company is not set up to respond to any new attacks and by the time an assessment rolls around, the company has an almost immeasurable vulnerability list to resolve that leaves the company behind on all network and data protections.

The last three security gaps are all related to the culture of the company, and all have an impact on the security posture of the organization. The company has a high turnover rate and low employee morale. The company has no segregation of duties and no mandatory vacation policy for its’ employees. Lastly, the company has a high number of theft reports and security incidents. These three issues are all related to one another. By not creating an environment for employees to thrive and feel welcomed, employee morale falls. As morale falls, sense of responsibility and loyalty to the company fall with it. This results in disgruntled employees and can lead to unethical decisions being made that results in losses for the company.

**Human Factors**:

“Cybersecurity experts generally agree humans tend to be the root cause of most incidents. Many cite a 2014 IBM Security Services report, "Cyber Security Intelligence Index," which found human error was a factor in 95% of successful hacks and security incidents” (Pratt, 2021). The area that creates the biggest issue is not specifically a human factor but is caused by a failure of the organization which contributes to human error. The lack of cyber security awareness training at the company results in employees falling victim to social engineering attacks as evidenced in the risk assessment. By not providing employees with proper awareness, training and education on security responsibilities and risk, the company is setting up their employees to fall victim to these attacks. “An awareness and training program is crucial in that it is the vehicle for disseminating information that users, including managers, need in order to do their jobs. In the case of an IT security program, it is the vehicle to be used to communicate security requirements across the enterprise” (Wilson & Hash, 2003). Human error is the largest unintentional threat to a company. This can come from downloading malware from a corrupted file sent as an email attachment to the strength of passwords used for company logins. Social Engineering is used against company employees to try and get their information by preying on human error. Human error is also used as the vector for attack from intentional threats. Phishing attempts meant to steal employee login credentials are constantly sent to corporate email accounts. Malware attachments are sent to try and coax an employee into clicking on them. The threats to a company can come from within or outside the organization. Failure to prepare employees and arm them with the knowledge necessary to be on guard leaves a company open to attack.

**Organizational Factors**:

Unintentional and intentional threats caused by human error are not the only places a company is vulnerable. Organizational factors play a large role in how vulnerable a company is to cyberthreats. MUSA Corporation’s lack of security posture has created an environment that is easily susceptible to attackers. The list of organizational security gaps is numerous. Starting within the company, data is not encrypted. This results in data flow that can be intercepted and altered without anyone knowing, or outright stolen. The company does not collect or analyze logs of their network traffic. Without the use of logs, data cannot be traced to determine where it is coming from, where it is going, who is accessing it, and who is altering it. The use of logs is important to maintain integrity of data as it flows throughout the network. The company lacks any intrusion detection and prevention system. Without a system in place, anyone who attempts to access the network without authorization can do so without any warning the network admins. This can be the result of human error as previously discussed or it can be done intentionally through a hack or other methods. By not having a media access control policy in place, there is no control over who accesses the network and on what device. The company has no protocols in place that control who has access to information on their network. Effectively, anyone could log on to their network and have free reign over the entire network and all the information and data the company houses. Couple this with the lack of configuration change management policy, and anyone who gets on the network can then change whatever access controls they wish. This leaves the company highly susceptible to ransomware attacks from multiple attack vectors.

The current state of the company is not set up in any way to maintain the confidentiality, integrity and availability of data and information throughout the company. The company fails to uphold the CIA triad and thus, maintains no security culture.

**Information Security and Awareness Training Policy**

All MUSA Corporation employees that use and/or have access to MUSA Corporation information technology resources (including but not limited to computers, smart phones, and supporting technologies) to conduct business, and all employees that transmit data on company networks are required to undergo security awareness training prior to using company systems, when system changes occur, and annually thereafter.

The goal of this training is to educate all employees in understanding their roles and responsibilities in safeguarding company systems and data. Security awareness training will include but is not limited to the following concepts:

1. The concept of separation of duties.
2. Prevention and detection of information security incidents.
3. Proper use of encryption.
4. Access controls, including the use of passwords and confidentiality.
5. Acceptable use.
6. Remote access.
7. Phishing.
8. Social engineering.
9. Least Privilege.

“Research suggests that human error is involved in more than 90% of security breaches. Security awareness training helps to minimize risk thus preventing the loss of PII, IP, money, or brand reputation. An effective awareness training program addresses the cybersecurity mistakes that employees may make when using email, the web and in the physical world such as tailgating or improper document disposal” (Mimecast, 2022). By educating employees in the concepts and implementation of security policy and procedures, the company seeks to limit the affects the risk of intentional and unintentional threats to the organization and its assets.

**Configuration Change Management Policy**

The goal of this policy is to manage any changes made to company systems. These changes are to be well communicated, planned, and performed in a predictable manner. This serves to limit the negative impact to users when performing systems changes, updates, or patches. “The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

1. Information being corrupted and/or destroyed;
2. Computer performance being disrupted and/or degraded;
3. Productivity losses being incurred; and
4. Exposure to reputation risk” (Biswas, 2020).

By implementing and sticking to a formal change control process, the company seeks to limit unintentional threats from occurring during these processes. “The control process will ensure that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored” (Biswas, 2020). Without properly controlling the implementation of system changes, changes made to company systems can negatively impact the business and prevent employees completing their job duties. Failure to the process of change implementation could expose the business to fraudulent activity and limit security measures in place to protect the company and its assets.

**Media Access Control Policy**

MUSA Corporation and its employees have a responsibility to protect all company assets including, but not limited to, devices, networks, and data. To that end, no employee shall knowingly alter any company device. Employees wishing to use removable storage devices shall only use company issued devices and are responsible for the protection and confidentiality of all information stored on the device. The issued device will be tied to the employee and the employee is responsible for maintain the whereabouts of the device to prevent loss and unintentional release of company information. No personal media device shall be connected to a company computer. Any information stored on removable media devices shall adhere to company acceptable use policy and adhere to all access control measures. Sharing information with someone not authorized to view the information is strictly prohibited and tracked as part of company issued storage media. Systems will be configured to automatically encrypt removable storage devices when company data is transferred to them. As a redundancy, the data transferred will also be encrypted to aid in the prevention of unauthorized dissemination of information.

The threat this poses is that of the ease for a small device (such as a flash drive) to be lost or stolen. Therefore, it is critical for employees to maintain the device as they would any other company resource. The prevention of connecting unauthorized devices to company systems is prevent the potential for practices such as baiting. “Baiting involves leaving a device infected with malware on show for someone to be intrigued enough to pick it up and plug it into their own device” (Stokel-Walker, 2022). An example of this is the Stuxnet worm that crippled Iranian nuclear reactors in 2010.

**Network Audit Policy**

This policy is to inform employees of security scanning procedures and precautions used by MUSA Corporation to audit their network and systems. Any person not authorized to do so is prohibited from performing any such audit. Audits are used by the company to:

1. Ensure integrity, confidentiality and availability of information and resources.
2. Investigate possible security incidents to ensure conformance to MUSA Corporation’s security policies.
3. Monitor user or system activity where appropriate.

All actions performed on company systems and networks are tracked on an audit trail. The company frequently performs audit checks to scan the network to ensure compliance with company and governmental policy. This includes scans of any electronic communication and e-mails regardless of by or to whom the communications are sent. While this policy serves to inform employees of the system tracking and auditing in place, this is performed for the safety and protection of the company, its assets, and all its employees. “The primary goals of security audit reports are to improve network performance, strengthen network security, and save expenses. In 2020, the HIPAA Breach Reporting Tool received over 100 reports, affecting millions of patients in doctors' offices and healthcare facilities around the country. Data breaches harm many people's lives and the reputations of the corporations and organizations involved. Following a security event, customers often distrust a company's capacity to secure their data, resulting in a tarnished reputation” (Miner, 2022). By constantly tracking, analyzing, and addressing issues that arise on the company network and its systems, the goal is to protect from the risks associated with potential threats, whether intentional or unintentional.

**Encryption Policy**

MUSA Corporation requires that all information created, stored, transferred, and shared on company systems and networks is to be encrypted using the Advanced Encryption Standard (AES) algorithm. “Advanced Encryption Standard is a symmetric encryption algorithm that encrypts fixed blocks of data (of 128 bits) at a time. The keys used to decipher the text can be 128-, 192-, or 256-bit long. The 256-bit key encrypts the data in 14 rounds, the 192-bit key in 12 rounds, and the 128-bit key in 10 rounds. Each round consists of several steps of substitution, transposition, mixing of plaintext, and more. AES encryption standards are the most commonly used encryption methods today, both for data at rest and data in transit” (Capers, 2021). This encryption method applies to data storage, data transmission (inside or outside the company), and remote access to the company network.

“According to the IBM 2018 Cost of a Data Breach Study, it costs $3.86 million to cover an average data breach. This cost is slated to increase by 6.4% this year with the likelihood of a recurring breach over the next two years, increasing by 27.9%” (RSI Security, 2019). By utilizing encryption methods on data, devices, and network connections, the company seeks to prevent a data breach as much as possible. No threat is completely preventable, however, failing to follow the guidelines set forth in this encryption policy puts the company and its assets at increased risk for exposure and data breach.

Encrypting connections serves to ensure data is not tampered with during transmission. Encryption works to validate and uphold the confidentiality, integrity, and accessibility of data. Preventing unauthorized access and modification of data and connections works to serve this purpose.

**Separation of Duties**

The NIST defines separation of duties as “the principle that no user should be given enough privileges to misuse the system on their own. Separation of duties is a security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud” (National Institute of Standards and Technology, 2017). To this end, MUSA Corporation implements the separation of duties in all departments of the company. This serves the purpose to prevent internal theft as well as unintentional security incidents from arising from someone having too much access and suffering a breach of their identity and credentials within the company.

The separation of duties serves to add an additional layer of security to multiple areas. Any person could find themselves in a situation where they may feel the desire to act unethically in their role. By applying a separation of duty to all job roles and responsibilities, no employee is given access to all functions needed to complete a task. This prevents the temptation to act unethically and commit any fraud against the company.

This policy also addresses unintended consequences associated with falling victim to social engineering tactics. While this is only one measure of defense against social engineering, this policy serves to limit the capability of a user’s account and its privileges in the event someone gains unauthorized access to a user’s account and attempts to act unethically or illegally against the company with the stolen credentials.

**Remote Access Policy**

Today’s computing environments often require out-of-office access to information resources. Remote access refers to the process of connecting to internal resources from an external source (home, hotel, etc.). The ability to connect to business resources securely and reliably from a remote location increases productivity and allows employees to work from in a different environment they may find to be more relaxing. This policy defines standards for employees to connect to the MUSA Corporation network from a remote location. These standards are designed to minimize potential exposures including loss of sensitive information, and limit exposure to security concerns through a consistent and standardized access method.

Employees shall use a company issued computer or smart phone to remotely access the company network. This standard to meant to ensure that devices used to access the company network are set to the standards the company has for devices and control methods are properly installed before the employee receives the device. The device will be preloaded with a Virtual Private Network (VPN) software that is set up to connect to the company network and allow remote access to the employee. Employees will use their work credentials to sign into the VPN and log in to the network. This connection will be encrypted using the AES-128 algorithm. Employees accept full responsibility for the device they are given for work purposes. Employees will ensure that the device is kept secure and logged off when not in use. Employees will prevent any multi-user use and limit the use of the device to themselves only. The employee will take responsibility for any unauthorized use or access to the device.

**Mandatory Vacation Policy**

In an effort to combat employee burnout, promote a healthy work life balance, and protect the companies interests and assets from the potential for internal fraud, MUSA Corporation requires that all employees take mandatory time off for two instances of 5 consecutive days at a time.

“According to the 2021 VMWare Global Incident Response Threat Report, of the 51% of cybersecurity workers who felt extreme stress or burnout during the past 12 months, 65% said they have considered leaving their job because of it” (Gregory, 2021). To promote a healthy work-life balance and focus on overall employee mental health, MUSA Corporation implemented this policy to allow employees time to rest, relax, and rejuvenate with time off from work without the stress of worrying about a paycheck.

The benefits for the company from this policy are that employees feel reduced burnout and are more focused at work. “Many organizations are facing increased cybersecurity attacks and open positions. So, it’s easy for employees to not take vacations. That’s especially true if they perceive that it means long hours before they leave and after they return. However, SHRM found that 78% of managers agree that vacation improves employees’ focus and 81% say time off soothes burnout” (Gregory, 2021). Further, this policy allows the company to detect any potential fraud taking place within the company. “Requiring our employees to take time off is necessary to prevent employee or internal theft. Employees that are required to take vacation are unable to consistently hide their illegal or unethical conduct” (Keng, 2018).

**Vulnerability Assessment Policy**

The purpose of this policy is to grant authorized personnel access to MUSA Corporations networking, computing, and information systems for the purpose of conducting audits to determine vulnerability assessments and penetration testing. This policy will be acted on annually to determine any weaknesses in the security posture of the company. Any identified weaknesses from this assessment will be resolved as fast as possible to resolve the identified weakness in the company’s security. Security audits assess the company’s security stance against an organized listing of security protocols, strategies, and procedures to ensure its IT infrastructure is secure and protected against data breaches.

“Audits may be conducted to:

1. Investigate possible security threats.
2. Test the security of information systems.
3. Make sure that the information is only accessible by the individual who should be able to access it.
4. Make sure system is protected from any unauthorized modification” (WorkForce Central, 2021).

“A vulnerability assessment informs organizations on the weaknesses present in their environment and provides direction on how to reduce the risk those weaknesses cause. The vulnerability assessment process helps to reduce the chances an attacker is able to breach an organization’s IT systems – yielding a better understanding of assets, their vulnerabilities, and the overall risk to an organization” (Hitachi Systems Security, 2017). The feedback and results of this assessment allow the company to stay on the forefront of security and ensures that the company is performing is due diligence in protecting its assets.

**Social Engineering Prevention Policy**

This purpose of this policy is to outline the potential threats that accompany social engineering tactics used by attackers to target unknowing victims. This policy outlines the additional policies that work to help limit this threat to our employees. Social engineering “involves tricking someone into divulging information or enabling access to data networks by taking advantage of human weakness. Put simply, social engineering is the use of deception to manipulate individuals into enabling access or divulging information or data” (Kaspersky, 2022).

MUSA Corporation utilizes spam filtering on its e-mail services to try and limit the number of phishing attempts that get through to our employees. No filter is perfect, and some attempts still get through. Employees are given a report spam option on their e-mail accounts that tags an e-mail, sends it to our IT security staff, and deletes the e-mail for the employee. These types of e-mails can be recognized by coming from unknown senders, including links to click on, and coming from e-mail addresses that are not associated with the claimed sender in the e-mail body.

To further aid in this, MUSA Corporation will keep anti-malware and anti-virus software up to date. System software and firmware will be regularly updated. Passwords are required to be changed every 90 days. Multi-factor authentication is required for all employee accounts and will be set up with the employee during their onboarding process. Finally, the company will hold regular trainings on the prevention of social engineering attacks and post a weekly newsletter with the latest trends for employees to look out for and to stay informed.

**Work Settings**:

A workplace environment comes with many stimuli that affect employees. For MUSA corporation, distractions, insufficient resources, and poor management systems all factor into causing employee undue stress, anxiety, and affect performance and productivity.

In the modern world, every person is surrounded by distractions. Phone calls, email, social media, all these work against an employee to distract them from their work. To combat this, MUSA corporation should combine policies and workplace practices to provide employees with a balance. Phone calls are going to happen and sometimes necessary depending on an employee’s life outside work, those with kids in school for example need to be able to answer their phones. The company should take this into account when creating a policy around phones while on the clock. Personal calls should be kept to an absolute minimum. The company should understand that there are times when personal calls may be necessary and should communicate with employees that they are allowed to answer their phones (i.e., it’s not strictly prohibited) however, excessive use will be monitored and addressed if it becomes a problem. This balances the employee’s needs with the company’s needs. E-mail is a normal part of day-to-day business, but it can become overwhelming and time consuming with the number of emails employees may receive. For this, the company would do well to implement email best practices documentation. This document would recommend that employees save checking emails for set times of day, for example once in the morning and once in the afternoon. This frees employees from being distracted from their tasks during the day. It also allows them time set aside for email purposes, to then focus on their communications and addressing all their emails instead of having to stop every so often as emails arrive. This practice allows employees some structure to their day and establishes a companywide expectation as to when communications can be expected. This same practice can apply to phone call distractions. Doug Bend of Bend Law Group was quoted by business collective as saying, “I get numerous calls a day and would not be able to efficiently complete projects for clients if I was constantly being pulled away and then had to refocus. Instead, I often put my phone on mute and return calls either in between projects or at set points of time during the day when it is not disruptive to completing work” (BusinessCollective, 2015).

Addressing insufficient and inadequate resources comes from the top down in any organization. “Prudent financial management requires companies to closely monitor their bottom line in order to increase profitability for their stakeholders. With this mindset, organizations tend to focus (sometimes exclusively) on the financial burden associated with any expense or investment that employees say that they need. Thus, managers are more likely to cite budgetary and economic restrictions as the primary reason for failing to provide those resources. Budgetary issues ARE real…but, if these resources are crucial for employees to achieve the desired results, then it doesn’t make sense for managers to demand the same outcomes even if they aren’t providing their employees with what they need to achieve them” (Puleo, 2018). This is what needs to be recognized by all levels of management. Once recognized, accountability needs to be taken by leadership and then it needs to be improved for the betterment of the employees. Failing to recognize the issue and correct it will lead to employee frustrations and eventual burnout, low morale, and a high turnover rate as currently experienced by MUSA corporation. The old adage “it takes money, to make money,” certainly applies in this situation and the company should take employee wellbeing as one of their most important elements to improving the workplace and security posture. The more an employee feels heard, the more an employee cares. The more they care, the more vigilant they will be with their work leading to a better security climate.

Continuing, poor management systems need to be addressed at MUSA corp. The establishment of standard operating policies (SOP) is the first step to providing employees a structured work environment. This SOP combined with a continuous improvement plan will allow the company to continue to grow while addressing issues that arise along the way. Without a baseline structure provided by the company, employees have a weak foundation to work from. Establishing an SOP puts everyone on the same page from the very beginning and lays a solid foundation for employees and managers to work from.

**Work Planning**:

In a work environment, employees are going to feel pressure to complete their tasks, time constraints are going to add to stress, poor planning and task difficulty will pile onto what an employee is already feeling and can push them to a point of stress and anxiety overload. To address this, leadership needs to change the culture around how they treat and interact with their employees. Specifically, leaders should remember that we are all human. With that, compassion can play a key role in understanding and helping your employees overcome their difficulties and be more productive. “Displaying compassion to our fellow workers, subordinates, and managers requires an acceptance of our innate humanity. In other words, compassion brings the “human” back into the workplace. In an age in which innovation, collaboration, client customization, and adaptability are critical to organizational sustainability, there is an urgent demand for “bigger, better, and faster” – regardless of the goals’ reasonableness or achievability. As burnout runs rampant in many organizations and employees choose to leave their employers (rather than continuously strive toward the achievement of these unreasonable demands), organizations must rethink their attitudes toward urgency. By instead rethinking organizational policies and processes in terms of their level of compassion toward workers, companies can reap the benefits of an engaged, energized, and loyal workforce” (Puleo, The Compassionate Workplace: What It Is, Why It’s Missing, and How It Contributes to Organizational Success, 2018). This has been backed by research. “In a study by Jonathan Haidt of New York University, leaders who interacted with their subordinates in ways that were perceived as fair and self-sacrificing were rewarded with employees who were more loyal, committed, and collaborative in working to find solutions to problems. Fowler and Christakis found that generous, compassionate, and kind actions created a chain reaction in workplaces – thus creating a cultural change toward compassion. Workplace compassion creates a culture of cooperation and trust. Rather than a culture of competition, organizational cultures that exhibit and support compassion tend to have lower health care utilization rates, greater employee engagement, less turnover, and a culture of trust that supports learning and innovation” (Puleo, The Compassionate Workplace: What It Is, Why It’s Missing, and How It Contributes to Organizational Success, 2018).

When it comes to addressing an employee’s lack of knowledge, skills, or abilities, there a few key factors. Everyone may learn differently, but how that learning is presented is vital to the employee retaining and growing from the training. When teaching employees, they need to be supported, there will be times when they fail, and they need a leader next to them encouraging them and reminding them that they can do it and the leader believes in them. Constructive criticism and discussion over failures needs to occur. An employee can just simply be corrected but teaching them why something failed allows them to learn the fundamentals of the issue for them to remember in the future and not repeat. To aid in employee learning, leaders responsible for training should find new ways to teach lessons and train skills. Regardless of the area of training, presenting the training material in a relaxed and approachable way will prove to be received most often by employees. “Above all else, the key to finding and closing knowledge gaps is to ensure that learning and evaluation are done on a continuous basis. The challenge in training is that as soon as a learning event ends, information retention immediately begins to degrade, unless it can be continually reinforced until used. Interval Reinforcement is a way to make it continuous” (Axonify, 2012).

**Employee Readiness**:

Employee readiness and wellness is an area of concern for every business regardless of size. With any job, employees are going to experience anxiety, fatigue, and boredom. This is something business owners and managers should expect to happen. How these feelings present themselves will vary depending on the individual employee. To address this, an employer needs to offer a wide variety of wellness programs to combat these feelings and support their employee’s overall health and wellness. In doing so, the employer will see benefits in employee retention, employee engagement, and employee productivity. Some ideas for ways to manage and reduce these feelings from employees are:

1. Set Attainable Goals – “Employers need to set realistic goals. For example, if an organization has attainable goals, it’ll be easier for employees to perform better without too much pressure, resulting in stress and anxiety. The employer also gains a lot of popularity. When setting goals, you should ensure that they’re in line with the organization’s objectives and they’re SMART” ( Declutter The Mind at Work team, 2022).
2. Provide employees with areas at work they can escape – Workdays can be filled with stresses. Giving employees an area, they can escape to during their break times allows employees time to refresh themselves throughout the day. An example could be a breakroom with games such as ping pong and air hockey. Things they can do to take get a break from work and come back in a better mindset to finish the day productively.

Employee wellness is vital to employee productivity. It doesn’t matter where the stresses come from. Employees are human beings and we all experience stress from all sorts of areas in our lives. Whether it be a bad experience on the way to work, troubles at home, or overwhelming feelings of anxiety associated with a hectic day at work. Employee wellness programs can be used to help employees escape and decompress from these experiences and recenter themselves to be able to focus on work. A workplace that provides these shows an employee they care about their wellbeing and in turn instills a desire to fulfill duties by the employee.

**Messaging Strategies**:

When trying to ensure that stakeholders and employees buy into a company sponsored program, it is important that the goal of the company is clearly communicated with consistent methods that relay the importance of the program to the company and how it affects everyone involved. Consistency is vital to the success of the program and utilizing multiple ways to deliver the message to stakeholders and employees allows for delivering the importance of the message to get stakeholders to buy in to its importance. One of the best ways of doing this is to utilize visuals in any area possible. “The first rule of engagement is all about sharing information in a purposeful and consistent way. All key stakeholders need to know the organization’s core purpose. External stakeholders need to understand why the organization exists and what value it provides for its customers, vendors, and the market. Internal stakeholders need to know where the organization is going so, they can align their work with those goal(s) and direction. To make sure this happens, use all communication means available – newsletters, electronic messaging, e-mail, meetings, posters, payroll inserts, etc. Be consistent in the messages and use them to show employees how they fit into the plan and how their contributions have helped shape the choices made. Share the results they have achieved and coach them toward strategic performance” (Posey, 2022). Utilizing these forms of communication constantly reiterates the importance of the program and acts as a constant reminder of the messages that have been delivered from leadership and those driving the campaign. This applies to any program but serves the purpose well for a security awareness program as it keeps the importance of security and the idea that security is everyone’s responsibility at the forefront of every employee’s mind as they are constantly presented with it. These visuals also serve to act on the subconscious, as posters placed throughout the company are something that everyone will see even if they do not specifically focus their attention on them. When developing messages to deliver to stakeholders and employees, consistency is key. “Make sure to remain consistent in what you say and how often you communicate. As the project leader, your responsibility is to provide guidance and consistency throughout every stage of the project. Stakeholders need to know you are always there, always approachable, and consistent. This provides stakeholders with the much-needed stability necessary to remain vested” (Alexander, 2018).

The next important strategy needed when communicating with stakeholders is the need to educate them. Stakeholders can come from inside or outside the company. Different departments may interact, and external business may partner together throughout daily business. When working with a security awareness program, it cannot be expected that other departments are going to know much about security and how their actions affect the businesses overall security vulnerability. “Many organizations have the opinion that the security department is responsible for security. Sustainable security culture requires that everyone in the organization is all in. Everyone must feel like a security person. This is security culture for everyone. Security belongs to everyone, from the executive staff to the lobby ambassadors. Everyone owns a piece of the company’s security solution and security culture” (Romeo, 2022). Therefore, education is key. “Security awareness is the process of teaching your entire team the basic lessons about security. You must level set each person’s ability to judge threats before asking them to understand the depth of the threats. Security awareness has gotten a bad rap because of the mechanisms used to deliver it. Posters and in-person reviews can be boring, but they do not have to be. Add some creativity into your awareness efforts” (Romeo, 2022). By adding consistent training and education opportunities, security becomes a part of everyone’s day-to-day activities. Supplementing the visuals placed throughout the company with continuing education e-mails and newsletters, the company can begin to establish a culture around security by delivering to stakeholders and employees the importance of security, how it effects everyone daily, and how everyone has a role to play with some responsibility.

**Security Culture**:

The overall goal of a security awareness program is to change a company’s culture around security. Through education and awareness, a company wants every level of employee to buy in to the idea that security is everyone’s responsibility, and it is important to every person in the company. “You can achieve this “all in” mentality by incorporating security at the highest levels into your vision and mission. People look to these things to understand what they should focus on. Update your vision or organizational objective to clearly articulate that security is non-negotiable. Speak about the importance of security from the highest levels. This does not mean just the people who have security in their title (CISO, CSO), but also from other C-level execs all the way down to individual managers” (Romeo, 2022). The approach to security must adapt to a company’s employees if a company wants their program to be successful and the culture in the workplace to change. “Some companies are beginning to get it. They are moving beyond tactical, episodic approaches to security and recognizing that effective enterprise-wide security requires a strategic, long-term approach, focusing more on communication and culture than exhortations from IT and an ongoing stream of new policy mandates” (Carpenter, 2021).

As technology has changed, and the understanding of the importance of security and the vulnerabilities companies carry in the modern world have been brought to light, employees have become confused with what needs to be done to be “compliant”. But a company seeks to move past compliance into a realm of second nature when it comes to security. The problem his presents is that years of security mandates and “best practices” have seemed to change every few years. “It’s not surprising that there is so much confusion among employees about what they should and shouldn’t be doing to protect company information. Even something as seemingly simple as using effective passwords has historically been a mishmash of contradictory and changing communications” (Carpenter, 2021). To combat this, companies need to stay consistent in their messaging and when something changes that was once acceptable, companies should take the opportunity to teach their employees what they have learned and why the former “best practice” is no longer valid and needs to be changed. “The key to building strong security behaviors is building a strong security culture. That means an ongoing process that is driven not from the IT department but from the top of the organization down. A process that is fueled by a relentless — and consistent — drumbeat to help employees understand exactly how their daily behaviors have the potential to protect or threaten corporate data” (Carpenter, 2021).

To further the transformation from a security awareness program to a companywide security minded culture, a company needs to ensure their workforce buys in by incorporating them in the development to foster the change in culture and usher it towards the desired security-minded nature. “Nothing helps to build cultural change more than involving employees in the process and solution. If the workforce understands the threat and helps with the solution, then the culture has a good foothold to grow into a standard operating procedure. Once security professionals have employees invested, they must create training programs. Although a robust cybersecurity training program requires labor-intensive work, it proves invaluable in engendering the culture. Thirty-seven percent of organizations’ staff cite insufficient cybersecurity training in the workplace. Training warrants more than one workshop or online course. An efficacious training program needs to repeat key concepts more than once a year. For example, some enterprises publish monthly IT newsletters to facilitate communication with other divisions. These newsletters cover various security topics, and each month, IT team members discuss these topics with their colleagues outside of IT. Some even require employees to add the monthly topic to their internal email tagline to reinforce it. This may help persuade colleagues to recognize cybersecurity as a serious matter” (Frenken, 2020). By making the entire organization apart of security and the development of security strategies, the company puts every employee on the same page and makes it clear that security is an important goal for the entire organization. With all employees on the same page, the culture at the company begins to change as everyone is participating.

# Works Cited

Declutter The Mind at Work team. (2022, May 18). *Employee Wellness Program Ideas: 11 Ideas to Proactively Support Employees*. Retrieved from Declutter The Mind at Work: https://declutterthemind.com/work/resources/employee-wellness-program-ideas/

Alexander, M. (2018, April 12). *6 ways to increase buy-in from project stakeholders*. Retrieved from TechRepublic: https://www.techrepublic.com/article/6-ways-to-increase-buy-in-from-project-stakeholders/

Biswas, P. (2020, February 1). *Example of Change Management Policy and Procedure.* Retrieved from Pretesh Biswas: https://preteshbiswas.com/2020/02/01/example-of-change-management-policy-and-procedure/

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

Capers, Z. (2021, July 22). *4 Common Encryption Methods to Shield Sensitive Data From Prying Eyes*. Retrieved from GetApp: https://www.getapp.com/resources/common-encryption-methods/

Carpenter, P. (2021, May 27). *The Importance Of A Strong Security Culture And How To Build One*. Retrieved from Forbes: https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/?sh=7d9dd1c16d49

Frenken, P. (2020, August 28). *Building a Culture of Security*. Retrieved from ISACA: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security

Gregory, J. (2021, October 29). *7 Ways to Improve Your Cybersecurity Team’s Employee Satisfaction*. Retrieved from Security Intelligence: https://securityintelligence.com/articles/jennifer-gregory/

Hitachi Systems Security. (2017, July 4). *The Benefits Of A Vulnerability Assessment.* Retrieved from Hitachi Systems Security: https://hitachi-systems-security.com/the-benefits-of-a-vulnerability-assessment/

Kaspersky. (2022). *Ways to avoid social engineering attacks.* Retrieved from Kaspersky: https://usa.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks

Keng, C. (2018, September 29). *Forced Vacation Prevents Employee Theft*. Retrieved from Forbes: https://www.forbes.com/sites/cameronkeng/2018/09/29/forced-vacation-prevents-employee-theft/?sh=399bb9d445bd

Mimecast. (2022). *What Is Security Awareness Training And Why Is It Important?* Retrieved from Mimecast: https://www.mimecast.com/content/what-is-security-awareness-training/

Miner, M. (2022, April 12). *Why Are More Companies Taking Network Security Audits?* Retrieved from SSI: https://insider.ssi-net.com/insights/why-are-more-companies-taking-network-security-audits

National Institute of Standards and Technology. (2017, June). *Separation of Duty (SOD)*. Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-192.pdf

Nesbo, E. (2022, June 10). *What Is Security Posture and Why Is It Important?* Retrieved from Make Use Of: https://www.makeuseof.com/what-is-security-posture/

Posey, P. A. (2022). *Stakeholder Engagement for Strategic Planning*. Retrieved from Everett Community College: https://www.everettcc.edu/ccec/enewsletters/stakeholder-engagement-strategic-planning

Pratt, M. K. (2021, December). *Security Awareness Training*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/security-awareness-training#:~:text=Why%20is%20security%20awareness%20training,significantly%20harm%20its%20brand%20reputation.

Puleo, G. (2018, July 24). *Inadequate Resources, Poor Performance, and Employee Burnout: Are Managers to Blame?* Retrieved from Change Management Solutions: https://changewithoutburnout.com/2018/07/24/inadequate-resources-poor-performance-and-employee-burnout-are-managers-to-blame/

Puleo, G. (2018, June 26). *The Compassionate Workplace: What It Is, Why It’s Missing, and How It Contributes to Organizational Success.* Retrieved from Change Management Solutions: https://changewithoutburnout.com/2018/07/26/the-compassionate-workplace-what-it-is-why-its-missing-and-how-it-contributes-to-organizational-success/

Romeo, C. (2022). *6 ways to develop a security culture from top to bottom*. Retrieved from TechBeacon: https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom

RSI Security. (2019, September 19). *Importance of Encryption in the Business World*. Retrieved from RSI Security: https://blog.rsisecurity.com/importance-of-encryption-in-the-business-world/

Stokel-Walker, C. (2022, April 6). *What are the safety risks of removable media?* Retrieved from Cybernews: https://cybernews.com/privacy/what-are-the-safety-risks-of-removable-media/

Wilson, M., & Hash, J. (2003, October). *Building an Information Technology Security Awareness and Training Program*. Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

WorkForce Central. (2021, April 9). *IT Vulnerability Assessment Policy.* Retrieved from WorkForce Central: https://workforce-central.org/wp-content/uploads/2021/04/it-vulnerability-assessment-policy.pdf