9-1 Final Project Submission: Security Awareness Program Proposal

Ivan V Santos

SNHU IT-552

Abstract

This document outlines the final project security awareness program proposal. The prompt is as follows: “You were just hired as the new chief information security officer for a large corporation whose security posture is low. The first thing your chief executive officer tells you is that he has recently seen a presentation by one of the information security team members emphasizing the importance of having a security awareness program. As a result, you have been asked to develop a security awareness program based on the specific needs of the organization. To that end, you will make recommendations for enhancing security policies, practices, and processes that are currently contributing to a dysfunctional security culture. Your chief goal is to build a program that will foster a healthy security culture and ensure continuous improvement. Your final project is to create a **security awareness program proposal** that addresses the needs of this case.” (SNHU, n.d.) Milestone reports 1-4 have been edited and compiled to create this final document.

TABLE OF CONTENTS

9-1 Final Project Submission: Security Awareness Program Proposal

1. **Introduction**

   a. **Purpose**:

This security awareness program will help to reinforce our user compliance with security policies and help reduce risks posed by threats. Information security awareness programs help educate users about emerging threats such as techniques attackers are currently using, acceptable use policies, and policies related to social networking sites. Attacks that deal with data loss in business enterprise are growing faster every day. As technology continues to improve, so does the amount of malicious attacks and loss of confidential data. An information security awareness program will add direct value to the company by educating staff, promoting best practices, and ensuring that confidentiality, integrity, and availability are executed properly throughout the organization. We can see the trend of breaches growing from the Verizon 2016 Data Breach Report (*most companies that partook in this data are large companies, >1000 employees*):

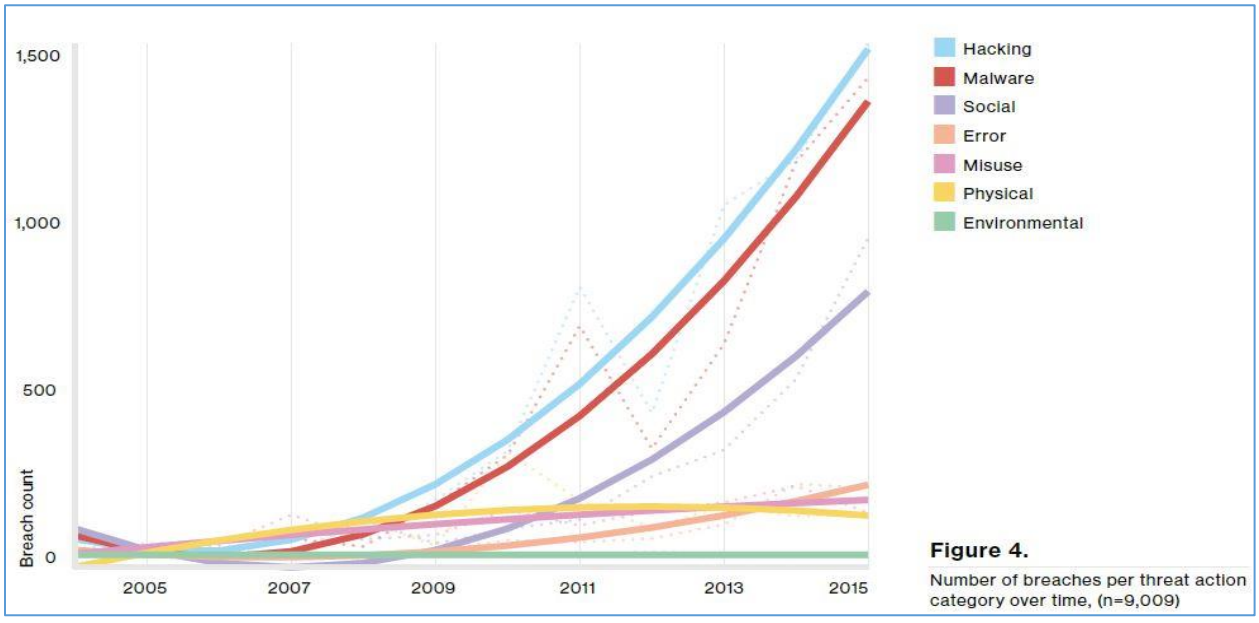


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

b. Scope:

The security awareness program directly deals with the company's major assets: the people and data. The policies, controls, and procedures will have an impact on every single user in all departments. There are 3 key roles within the company that will each have a responsibility. The roles and responsibilities are broken down below:

Specialized Roles
• Recognize their accountabilities • Recommend secure practices • Handle processes securely
Management
• Encourage security awareness in staff • Re-enforce security messages to staff • Address security-related issues with staff • Set security expectations
All Personnel
• Recognize threats • Recognize security as benficial • Report potential security threats • Make security a habit

The 3 different roles, eventually, will be the ambassadors of information security best-practices for their respective jobs/groups. The IT team (mainly the information security team) will spearhead the security initiates and coordinate the training to increase consistent awareness throughout the company. Training will be done annually and be part of every employee onboarding process. Training is broken down for the different roles below with the main goal being to add value to the company by increasing information security on all fronts.:

(PCI DSS, n.d.)

c. Security Posture:

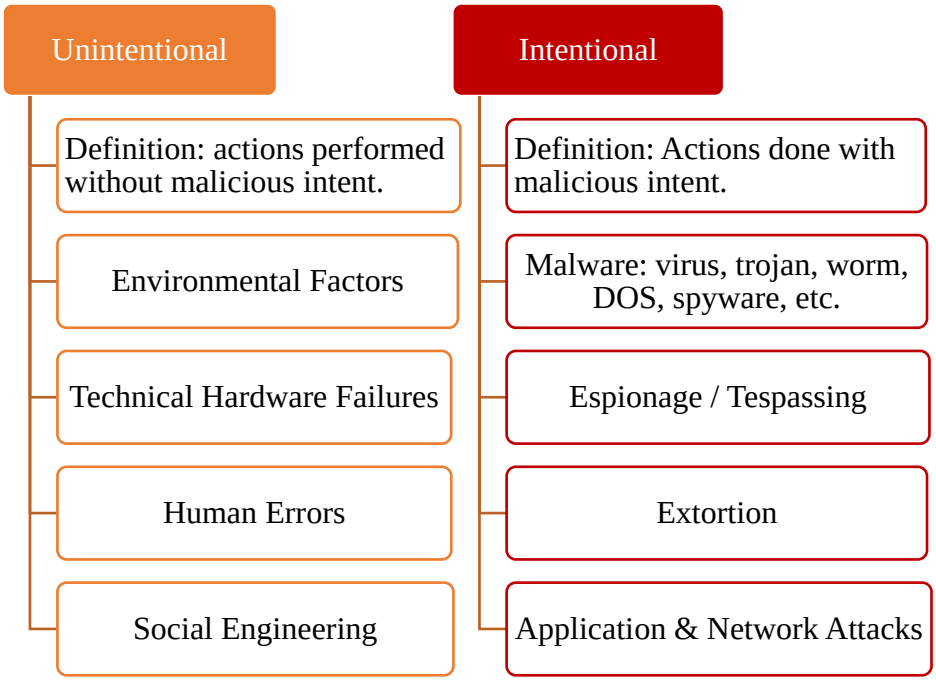
Currently, the security posture is very poor and must be improved if the company wants to grow properly. The security awareness program will be accompanied by the information security policy, continuous monitoring plan, and communication plan to help mitigate these high-impact risks throughout the company. Per the current scenario, this is a high-level risk break down of the current security posture:

Risk	Impact
No information security awareness training	HIGH: causes phishing and social engineering attacks.
No change management policy	HIGH: change management processes help prevent outages from configuration changes, directly affects availability.
No IDS/IPS system	HIGH: very poor network defense.
No logs being collected	HIGH: reduces ability to mitigate and respond to security incidents.
No media access control policy	HIGH: no device governance.
No encryption or hashing	HIGH: compromises confidentiality and integrity of data.

Vulnerability assessment is every 3 years	HIGH: very poor network defense.
High turnover, low employee morale	HIGH: too much money spent on hiring new employees so frequently.
High amount of security incidents	HIGH: Every security incident is a potential data loss.
No separation of duties or mandatory vacation	HIGH: compromises integrity.

d. Types of Threats (intentional & unintentional):

A basic breakdown of intentional and unintentional threats is broken down below:



Our controls, procedures, and plans for threat mitigation are all outlined in the Proposal section.

e. High-level Objectives:

Objectives and goals are further addressed in the stakeholder section. At a very high-level, the key objectives for the security awareness program will be to create a security-aware culture and implement official information security policies and procedures that will include:

- Acceptable use policy (AUP): defines the proper system usage for users.
- Mandatory vacation policies: these policies help to reduce fraud and discover malicious activities by employees.
- Separation of duties policy: separates individual tasks of an overall function between different entities or different people, and helps to deter fraud.
- Clean desk policies: require users to organize their desks and surrounding areas to reduce the risk of possible data theft and password compromise.
- Account policies: require administrators to have two accounts to prevent privilege escalation and other attacks. Account disablement policies ensure that inactive accounts are disabled.
- Change management: define the process for making changes, and provide the accounting structure or method to document the changes. Change management helps reduce unintended outages from changes.
- Third-party agreements: include a non-disclosure agreement requiring all parties to recognize who owns the data and prohibiting unauthorized sharing of data.
- Service level agreement (SLA): an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.
- Interconnection security agreement (ISA): specifies technical and security requirements for connections and ensures data confidentiality while data is in transit.
- Information classification practices: help protect sensitive data by ensuring users understand the value of data.
- Sanitization procedures: ensure data is removed from decommissioned systems.

- Storage and retention policies: identify how long data is retained. This can limit a company's exposure to legal proceedings and reduce the amount of labor required to respond to court orders.
- Personally identifiable information (PII) policies: PII requires special handling and policies for data retention. Many laws mandate the protection of PII, and require informing individuals when an attack results in the compromise of PII.
- Privacy Policy: identifies what data is collected from users on a web site.

f. Metrics:

Metrics will be based on the service level agreements set in place (SLAs). All metrics will be measured on how well we meet the SLAs and core objectives:

- Limit immediate incident impact to customers and business partners;
- Recover from the incident;
- Determine how the incident occurred;
- Find out how to avoid further exploitation of the same vulnerability;
- Avoid escalation and further incidents;
- Assess the impact and damage in terms of financial impact and loss of image;
- Update company policies, standards, procedures, and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

2. **Proposal**

Below are the main deliverables of the security awareness program: the training curriculum, security policies, incident response plan, data classification, forensics plan, and continuous monitoring plan. The plans were all developed with the high-level objectives in mind. Once again, the main goals are to create a better security culture while maximizing the security

of all company assets: people and data. Proper execution of these deliverables will help get us there.

a. Security Awareness Training Curriculum:

User awareness is essential to ensuring a more secure environment. A basic training overview of policies and end-user computer best practices will be part of the onboarding process for all new employees. This training will also be made mandatory once a year for all employees to keep everyone filled in on the current best information security practices and threat. The curriculum is broken down below:

(REFER TO ATTACHED POWERPOINT PRESENTATION FOR TRAINING MATERIAL)

Each topic can be designed to be either basic, intermediate, or advanced depending on the end user / audience. IT would be receiving intermediate through advanced awareness training. The company will be better protected as more employees understand and adhere to the information

security policies and best practices. The possibilities of training help increase the potential for better confidentiality, integrity, and availability throughout the company.

b. Security Policies & Rules of Behavior

Rules for internal users:

1. User should only process data that pertains to official business and is authorized to be processed on the system.
2. You should log-off, lock the computer, or use a password-protected screen saver whenever the workstation is left unattended.
3. Do not connect any personal devices to workstations, including phones.
4. Report all security incidents or suspected incidents to the IT department.
5. Discontinue use of any system resources that show signs of being infected by a virus or another malware and report the suspected incident.
6. You must use only the data for which you have been granted authorization.
7. You must notify your manager if access to system resources is beyond that which is required to perform your job.
8. Do not download anything unless preapproved by your manager. Manager must notify IT of the download to gain approval. Pirating will not be tolerated; you will be held accountable.
9. Do not install unapproved software onto the system. Only designated personnel are authorized to load software.
10. Do not add additional hardware or peripheral devices to the system. Only designated personnel can direct the installation of hardware on the system.
11. Do not store any customer information on systems, unless authorized to do so.

12. Do not remove any information technology resources from the facility without proper approval.
13. Question any unfamiliar presence in your work area. Contact your manager, HR, or security.
14. Protect and handle computer resources with care.
15. All user should understand that any person who obtains information from a computer connected to the Internet in violation of their employer's computer-use restrictions is in violation of the Computer Fraud and Abuse Act.

Security Policies Overview:

Written security policies are basically management controls that will identify the overall organized security plan for a company and help in reducing the overall risk. Other security controls enforce security policies. Security policies cover many areas of security including human resource policies, business policies, certificate policies, and incident-response policies. The security policies will be able to mitigate risks, threats, and incidents. Below is a breakdown of 10 of the company's security policies:

1. **Remote Access:** Remotes access for users is an important requirement. In the world we live in today, we are increasingly mobile. We will utilize encryption technologies to maintain confidentiality and keep everything private (encryption discussed in #2). For remote users, we will use RADIUS for authentication. RADIUS (Remote Authentication Dial-in User Service) is an authentication protocol for almost everything. It is a very common authentication, authorization, and accounting (AAA) service that deals with modems, routers, switches, firewalls, etc. It is also a common authentication method for 802.1X Secure authentication, and it sends passwords as a hash. Remote access logs will

constantly be audited. Telnet will not be used, instead only Secure Shell (SSH) will be used for any type of remote administration. Our virtual private network (VPN) will be the connection point for remote users. While on the VPN, the traffic is encrypted across the Internet and decrypted on the internal private network.

2. **Encryption & Hashing:** We will provide data integrity with hashing. Hashing verifies the integrity of data, such as downloaded files and email messages. A hash (sometimes called a checksum) is a fixed-size string of numbers or hexadecimal characters. Hashing algorithms are one-way functions used to create a hash. By doing this, you cannot reverse the process to re-create the original data. The passwords will be stored as hashed instead of the actual password. “Salting” the password thwarts many password attacks. We will incorporate a mixture of hashing algorithms such as secure hash algorithm (SHA), Message Digest 5 (MD5), and Hash-based Message Authentication Code (HMAC). We will provide the Encryption and confidentiality of data, including data at rest (any type of data stored on disk) and data in transit (any type of transmitted data). Our transport encryption methods will be to utilize IPsec, TLS, and SSL. RADIUS will use symmetric encryption, where the same key is used to encrypt and decrypt data. We will utilize digital signatures. A digital signature provides authentication (verified identification) of the sender, non-repudiation, and integrity of the message. We will use a public key infrastructure (PKI) for our certificate management. A public key infrastructure (PKI) is a group of technologies used to request, create, manage, store, distribute, and revoke digital certificates. The PKI will allow two entities to privately share symmetric keys without any prior communication. We will utilize a key escrow and a recovery agent to prevent losing our initial private keys.

3. **Auditing Network Accounts:** Identification, authentication, and access control will be monitored, audited, and analyzed regularly. Identification associates a user with an action, while authentication proves that a user is who they claim to be. The access control process consists of being able to prove a user is who they say they are, and proving that a user performed an action. Authorization will only be granted on a least privilege model; user will only have access to what they need to do their jobs. Role-based access control (RBAC) will be utilized. Role-based access control is broken down as follows: access is based on the role of the user; rights are gained implicitly instead of explicitly. There will be some time of day restrictions for access certain servers that will only be available during working hours. There will be no shared accounts as this practice breaks non-repudiation. We will utilize Group Policy, joined with our Active Directory (AD), for program and desktop security administration. All network accounts must have a password with a length of at least 8 characters that are alphanumeric with a special character. User passwords expire and must be changed every 90 days. All actions will be logged and monitored via our Solar Winds Log Event Manager (LEM) tool. Logs will be analyzed by the security team daily.
4. **Configuration Change Management:** Change management documentation will be managed through our information technology service management (ITSM) tool. All changes will be logged (upgrade software, hardware configurations, patches, etc.) change documentation that must be completed and accounted for include frequency, duration, installation process, and fallback procedures. The ITSM change module will be configured in such a way to recognize legitimate activity and stop any unapproved

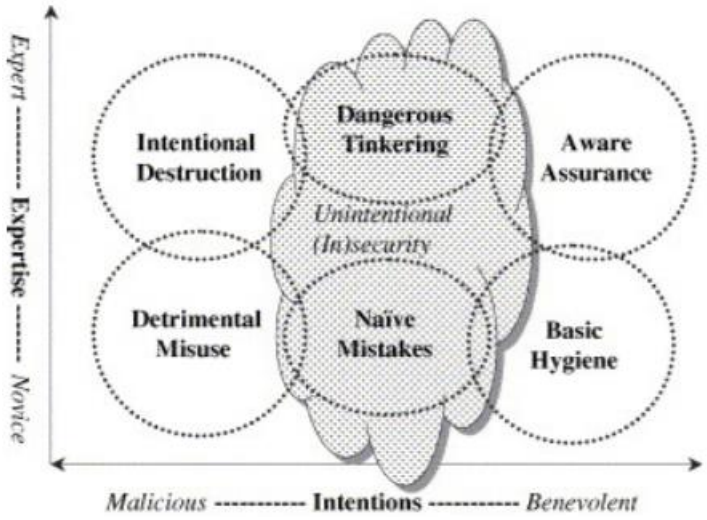
activity/unapproved changes. Changes will only happen once the appropriate leaders sign off on the "change request" form in the ITSM tool.

5. **Segregation of Duties:** Separation of individual tasks of an overall function between different entities or different people, and helps to deter fraud. For example, a single person shouldn't be able to approve bills and pay them, or print checks and then sign them. HR and IT will collaborate to determine user roles. The ITSM tool will automate most of this once users have been set up properly.
6. **Mandatory Vacation:** We will require employees to take time away from their job. These policies help to reduce fraud and discover malicious activities by employees. Security team will coordinate with HR to audit vacationing employees.
7. **Personal Identifiable Information:** Personal Identifiable Information (PII) is data that is used to personally identify an individual. Examples include the full name, birth date, address, and medical information of a person. A privacy policy identifies what data is collected from users on a web site, our privacy policy states that no credit card information will be stored or collected via the PCI DSS compliance. PII will be treated as confidential information.
8. **Media:** Bring your own device (BYOD) is not permitted. The next generation firewalls (NGFWs) should be configured to automatically block external removable media from user systems via group policies. Users are also required to organize their desks and surrounding areas to reduce the risk of possible data theft and password compromise. All data on mobile devices will be protected with encryption, screen locks, and remote wipe capabilities (Remote wiping removes all the data from a lost phone). We will use mobile device management (MDM) tools to ensure that all mobile devices meet patch

requirements, and if not, network access will be blocked until requirements are met. Virtual local area networks (VLANs) will be used to isolate mobile device traffic from the primary network. We will utilize a trusted platform module (TPM) and hardware security module (HSM) for laptops and portable devices. TPMs have a storage root key used to generate and protect other encryption keys. An HSM generates and stores RSA encryption keys and can be integrated with servers to provide hardware encryption.

9. **Social Engineering:** Our security baselines will be used and measured against by the monitoring and audit teams. The logs from the LEM and NGFWs will also be reported on and analyzed. All onboarded employees will undergo basic security awareness training that covers social engineering, physical, and operational security. Security training is mandatory once a year for all non-IT employees (IT will have more). Our NGFWs should be configured to enforce blacklisting and whitelisting for emails, as well as spam filtering. We have gated security and security traps in place to prevent tailgating, as well as video surveillance. All devices are set up with antivirus (AV) software, pop-up blockers, anti-spam software, anti-spyware, and an SCCM agent in which our LEM will track all logs for forensic and analysis.
10. **Integrating Systems & Data with Third-Parties:** A non-disclosure agreement will be used that will require all parties to recognize who owns the data and prohibit unauthorized sharing of data. An interconnection security agreement (ISA) will be used, which specifies technical and security requirements for connections and ensures data confidentiality while data is in transit. A service level agreement (SLA) will be used; an agreement between a company and a vendor that outlines performance expectations, such as minimum uptime and maximum downtime levels.

These 10 policies describe the ways the company would mitigate and reduce nonintentional threats, intentional threats, and secure data flow. The combination of physical and technical controls (NGFWs, LEM, ITSM tools, etc.) will mitigate a variety of threats, both intentional and unintentional. Operational controls, such as the clean desk policy, vacation policy, segregation of duties, etc. will help to create a culture that incorporates security into the normal workflow. Data flow will be handled with a combination of physical, technical, and operational controls as described in policies 1,2,3,8,9, and 10. The policies in place are written to cover each of the risk areas outlined in the image below:



(Stanton et al., 2005)

According to IBM's 2014 CSI Report, "95% of all security incidents involve human error." The active controls: physical, operational, and technical, will continue to evolve over time as technology improves and people change. The security policies must be enforced and known throughout the company. Pairing the policies with sound leadership that promotes awareness and best practices is key to a successful information security program.

c. Data Classification:

Classification	DATA CLASSIFICATION DESCRIPTION	
Restricted	Definition	Restricted information is highly-valuable, highly-sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Impact	· SIGNIFICANT DAMAGE would occur if Restricted information were to become available to unauthorized parties either internal or external. Impact could include negatively affecting competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
Confidential	Definition	Confidential information is highly-valuable, sensitive business information and the level of protection is dictated internally.
	Impact	· MODERATE DAMAGE would occur if Confidential information were to become available to unauthorized parties either internal or external. Impact could include negatively affecting competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.

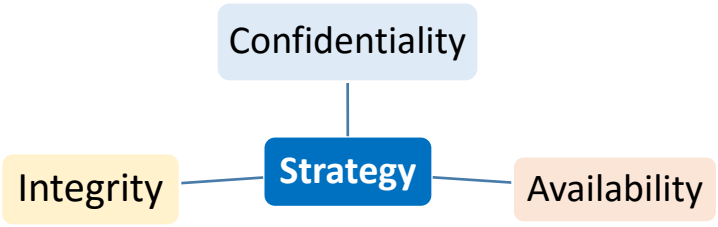
Internal Use	Definition	Internal Use information is information originated or owned by the company, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Impact	· MINIMAL or NO DAMAGE would occur if Internal Use information were to become available to unauthorized parties either internal or external. Impact could include damaging the company's reputation and violating contractual requirements.
Public	Definition	Public information is information that has been approved for release to the general public and is freely sharable both internally and externally.
	Impact	· NO DAMAGE would occur if Public information were to become available to parties either internal or external to. Impact would not be damaging or a risk to business operations.

d. Incident Response Plan:

The team has created the incident response plan (IRP) in alignment to the security program objectives. The main objective is to protect company data and systems. The IT team will lead the effort in protecting all the company's data and the information systems that function to collect, process, and maintain this data. Proper security of systems must contain the controls and safeguards to deal with any possible threats, and mainly the controls must be able to ensure

availability, integrity, and confidentiality of the data. Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of company data and information systems. This also includes against accidental loss or destruction.

The incident response plan (IRP) will be the framework that the company will follow to efficiently handle any information security incidents that could compromise confidentiality, integrity, or availability. This IRP is necessary to support the guidance and management of risks in day-to-day operations. All strategy will focus on creating and maintaining confidentiality, integrity, and availability.



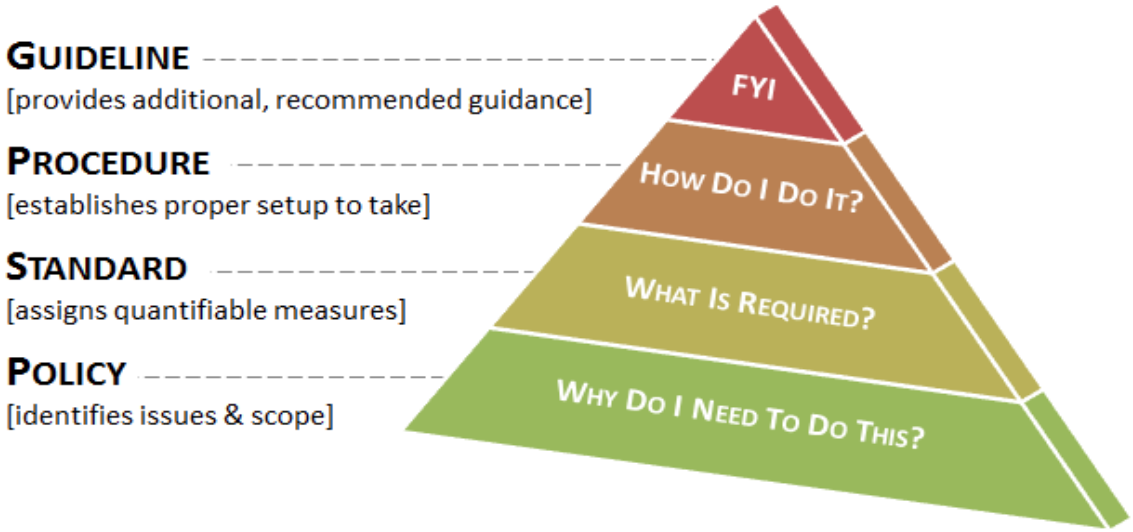
Key Terms:

- Asset Custodian: a person or entity with the responsibility to assure that the assets are properly maintained, to assure that the assets are used for the purposes intended, and assure that information regarding the equipment is properly documented.
- Contract Owner: a person or entity that has been given formal responsibility for entering and managing legal contracts with service providers. Contract owners are formally responsible for making sure due care and due diligence is performed with service providers.
- Control: any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help IT accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

- Data: an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies. (Data classification covered in communications section).
- Data Owner: a person or entity that has been given formal responsibility for the security of an asset, asset category, or the data hosted on the asset.
- Information System: an asset; a system or network that can be defined, scoped, and managed.
- Policy: formally established requirement to guide decisions and achieve rational outcomes.
- Service Provider: includes companies that provide services that control or could impact the security of data.

Organizational Approach to Incident Response:

The IRP is comprised of four main parts: a core policy; measurable standards used to quantify the policy; procedures that must be followed; and guidelines that are recommended, but not mandatory (PCI DSS, n.d.).



(Made in VISIO)

The IRP focuses on IT security management and IT-related risks. The main governing driver of this plan is that the IRP should be able to stay effective and efficient for the long-term visions and goals. It must be able to adapt to changes within the organization and environment. In accordance with ISO/IEC 27001, the IRP incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming Cycle, approach (ISO, n.d.):

- Plan: This phase involves designing the ISMS, assessing IT-related risks, and selecting appropriate controls.
- Do: This phase involves implementing and operating the appropriate security controls.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: This has involves making changes, where necessary, to bring the ISMS back to optimal performance.

Communications:

It is important to understand each team member's role and recognize the correct avenue for communication to maximize response time and efficiency. The roles are broken down below:

Role	Description
Information Security Officer (ISO)	The ISO is accountable to the organization's senior management for the development and implementation of the information security program. The ISO will be the central point of contact for setting the day-to-day direction of the information security program and its overall goals, objectives, responsibilities, and priorities

Asset Owners	Business or department manager with budgetary authority over the system(s) with responsibility for the basic operation and maintenance of the system(s).
Asset Custodians	Under the direction of the ISO, asset custodians (e.g., system & network administrators) are responsible for the technical implementation and management of the PCI DSS Information Security Policy. Party responsible for certain aspects of system security, such as adding and deleting user accounts, as authorized by the asset owner, as well as normal operations of the system in keeping with job requirements.
End Users	All employees (and contractors) are considered both custodians and users of the information systems and data on their issued information systems and are required to uphold all applicable PCI DSS Information Security Policy policies, procedures, standards, and guidelines.
IT Company Management	▪ Oversee and approve the company's information security program; ▪ Appoint, in writing, an Information Security Officer (ISO) to implement the information security program; ▪ Ensure an appropriate level of protection for all company owned or maintained information resources; whether retained in-house or under the control of contractors; ▪ Ensure that funding and resources are programmed for staffing, training, and support of the information security program and for implementation of system safeguards, as required;

▪ Ensure that persons working in an information security role are properly trained, and supported with the appropriate resources.

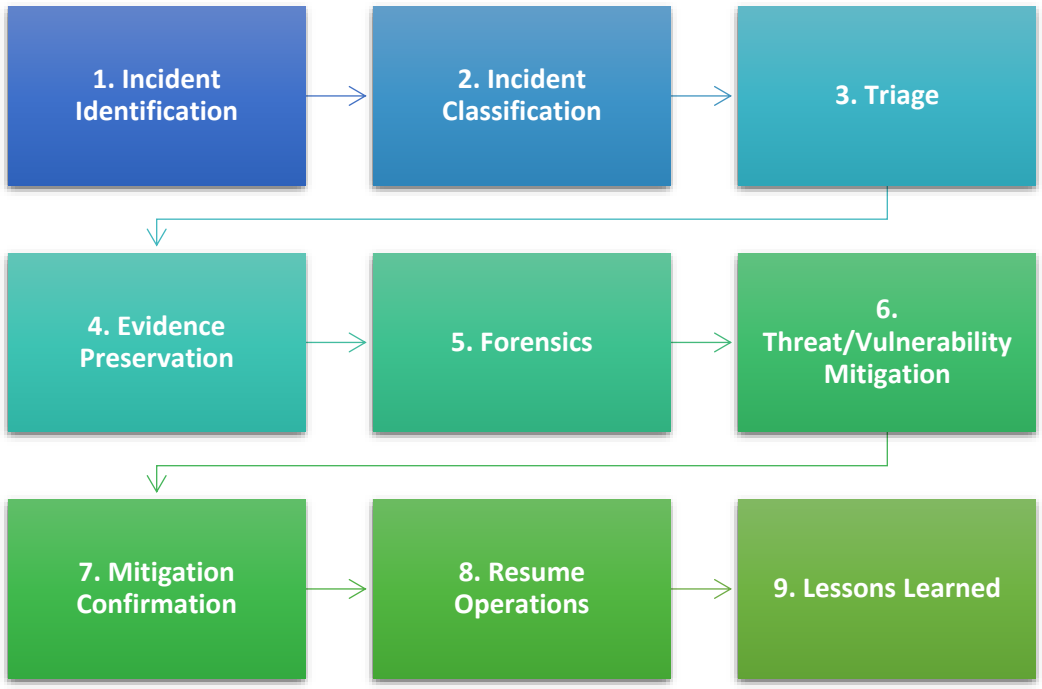
A basic breakdown of internal communication is shown below:

Communication with outside parties that interface with any will always include a role from the IRP team present. The team will document all contacts and communications with outside parties for liability and evidentiary purposes. The company may communicate with several types of outside parties, as depicted in Figure 2-1. The double-headed arrows indicate that either party may initiate communications:

Figure 2-1. Communications with Outside Parties

(NIST, n.d.)

i. Incident Handling Roadmap:



1. The team must identify the problem and analyze if it is an incident. An incident is anything that can comprise the C.I.A. of the company.
2. The data roadmap will be referenced when classifying incidents to establish priority and scope.
3. During triage, the team will form the "game plan" and do all the prep necessary to resolve the incident.
4. Evidence will be persevered; priority will be from the most volatile to the least volatile.
5. Computer forensics will be done to further obtain evidence and information that would help with mitigation (capturing system hashes, logs, chain of custody, etc.)
6. During mitigation, the team will:
    a. Determine the attacker

b. Analyze controls and security logs and make necessary changes (passwords, firewall ACLs, port configurations, etc.)

c. Communicate and notify all affected people (PII may require additional notifications).

d. Prevent the spread of damage.

e. Document everything!

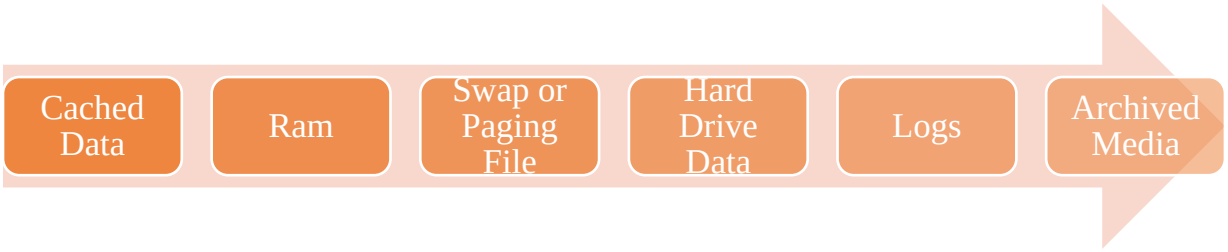
7. It is vital to do proper analysis that all threats have been successfully mitigated. The team will also finish documentation.
8. Operations will resume once the ISO reports to management and management approves.
9. All documentation is finalized. Additional analysis may be done to develop strategic plans for hardening security. All lessons learned will also be documented.

e. Forensics Procedures:

The team will conduct forensics to determine anything that was done to impact confidentiality, integrity, or availability. Some of the forensic procedures that would take place are shown below:

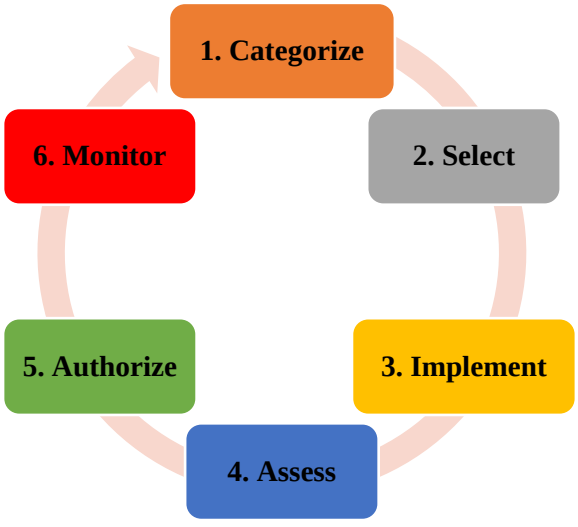
Depending on the scope of the data in the device, we might completely rebuild the system, including applying all updates and patches. Before anything is done to the device, the team must capture an image of the data before analysis to preserve the original and maintain its usability as

evidence. The culprit will be determined by active monitoring and proper execution of the forensics plan. Collaboration with the police will also be considered should the need arise, since it is a federally owned device with very confidential personal identifiable information on it. All data will be handled by the order of volatility (most to least), which is shown below:



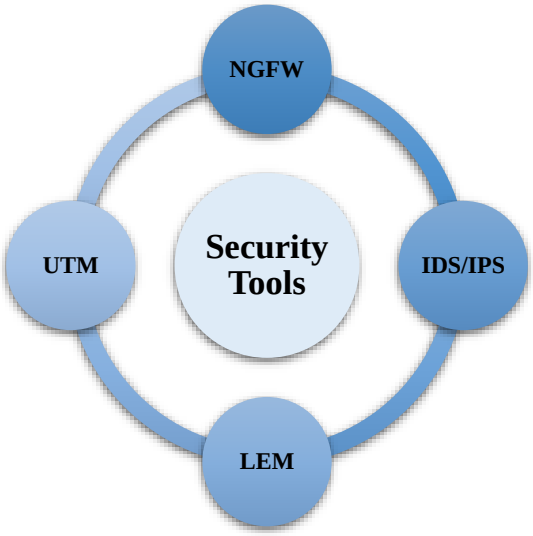
f. Continuous Monitoring Plan:

We will use continuous monitoring alongside our policies, IRP, and forensics plan to further harden our company defenses. The team will utilize our data classification to help categorize and quantify the risks/threats and determine the proper control. “Continuous monitoring enables information security professionals and others to see a continuous stream of near real-time snapshots of the state of risk to their security, data, the network, end points, and even cloud devices and applications.” (SANS Institute, n.d.) We will be utilizing the process that stems from the Information System Continuous Monitoring (ISCM) methodology and Risk Management Framework (RMF):



1. Categorize Information Systems: Criticality and sensitivity will be defined for systems based on the impact of their potential worst-case scenarios.
2. Select Security Controls: Baseline security controls will be chosen that reflect a proper risk assessment.
3. Implement Security Controls: Technical, managerial, and operational controls will be implemented throughout the business.
4. Assess Security Controls: Analyze the effectiveness of security controls and ensure they meet the correct standards for security.
5. Authorize the Information System: Identify key organizational risks for operations and assets. If the risk is acceptable, the system will proceed to go-live.
6. Monitor the Security State: This is where continuous monitoring happens. All changes to the information system that can affect security controls will be monitored.

Effectiveness of security controls will always be analyzed as well. We will utilize this framework to create and implement proper controls that address our policies, and the continuous monitoring team will use the framework to measure against any changes in the environment. The security tools that the company will be using are shown below:

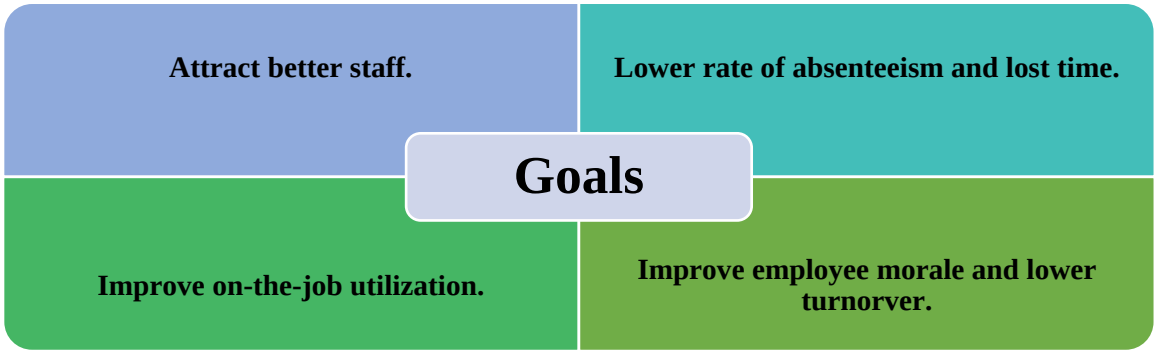


- Next Generation Firewalls (NGFW): The greatest benefit of a NGFW is the ability to protect at the application layer. Access control lists (ACLs) can also be configured to reflect company policies. Once implemented, IT can report on most activity with a NGFWs GUI, like the Palo Alto Panorama.
- Unified Threat Management (UTM): A UTM is security appliance that includes multiple layers of protection, such as URL filters, content inspection, and malware inspection. This appliance will help protect the network perimeter and analyze any perimeter activity.
- IDS/IPS: Intrusion detection systems (IDS) and intrusion prevention systems (IPS) inspect network traffic like a protocol analyzer would. An IDS will detect attacks, based on the inspected traffic, on the network. An IPS will not only detect attacks, but it can act to stop attacks as well. IDS will utilize signatures for detecting threats. Signatures must always be updated! An IPS can be utilized to actively monitor data streams, detect malicious content, and mitigate the effect of malicious activity. IDS/IPS are part of vulnerability management, and a tool like Nexpose can be utilized to create proper reports and metrics for vulnerability assessment and management.
- LEM: Log Event Monitoring (LEM) provides the ability to aggregate all activity into a centralized system. Solar Winds Log Event Manager is an example of a seamless and user-friendly tool that provides active log monitoring with strong reporting capabilities. The tool utilizes SCCM agents on devices which enables the active monitoring. This tool will also interface with all security appliances to create the executive reports. Log monitoring, analysis, and reporting are all essential for strong continuous monitoring.

By pairing the framework with the right tools, the company will be able to start continuous monitoring on the systems to ensure that all assets are being treated with confidentiality, integrity, and availability.

g. Work Settings, Work Planning, Employee Readiness plans:

We will be collaborating with human resources (HR) to create strategies that deal with bettering employees themselves and the workplace. These plans and policies will have an impact on the company culture, so HR will be invested alongside the IT leadership to properly create and execute the strategies throughout the company. The goals of these strategies are outlined below:



(Lisa Welshhons, n.d.)

Improving the work settings in a company is something that will not be done hastily. Management will conduct a proper audit/screening of work to fully understand the work setting conditions. Once an assessment is made, the team will strategize based on the quantitative and qualitative measures of the audit. Work planning and employee readiness strategies will also be planned methodically and properly to maximize the potential of positive change. A very basic approach we will use as a starting point is broken down below:

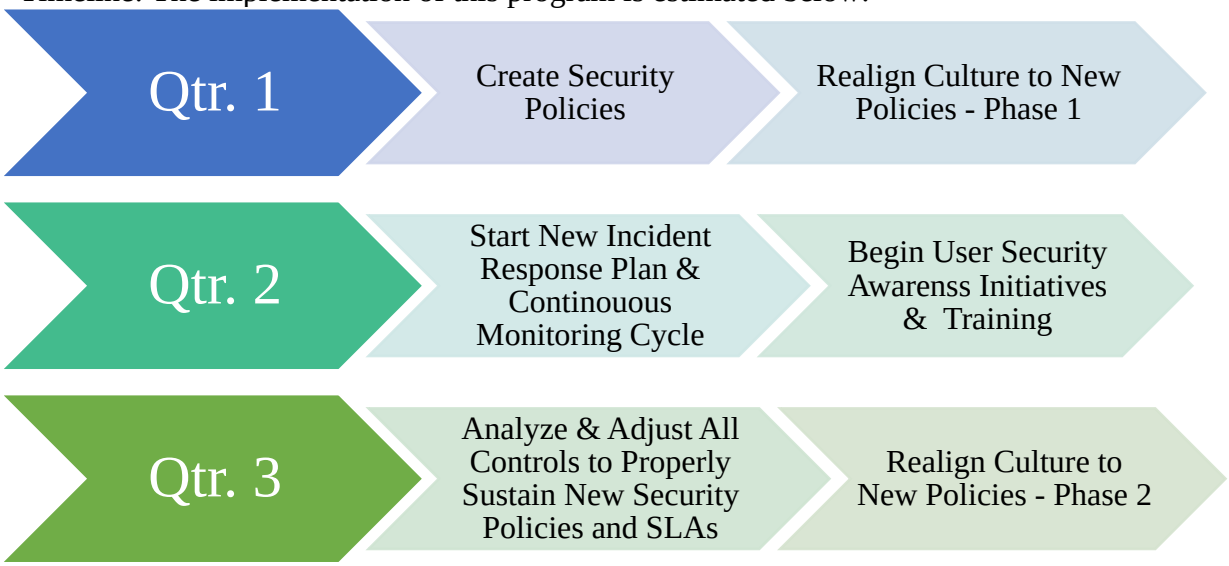
1. Promote health and wellness: a wellness program will only be successful if the company organizational culture promotes the benefits. The work environment itself must promote

healthy lifestyles in their food, break areas, proper work space lighting/air quality, ergonomic furniture, noise levels, etc. Leadership will create company policies that enhance employee health.

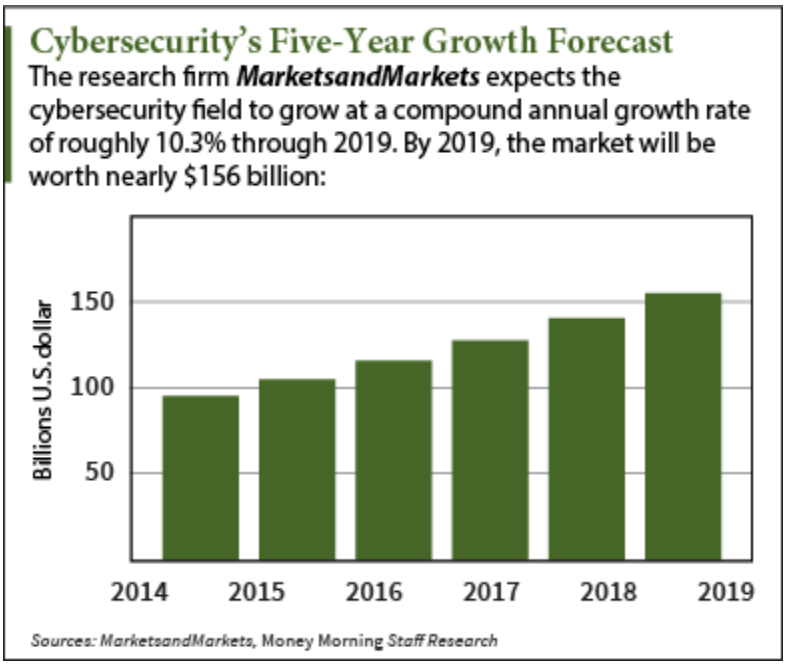
2. Incentives to motivate employees: There needs to be incentives in place that will drive employee participation and motivation. Other than financial incentives, there needs to be some thought on how to continuously keep employee morale high and reduce stress, fatigue, bas practices, etc. Possible options can be department employee of the month, frequent team outings, appointing the "bubbly" person in the department as an encourager for the rest of the team, etc.
3. Training for growth and development: I believe the way to go in terms of general training and development is a learning management system (LMS) like Lynda. An LMS tool will enable management to track employee progression, and it will also give management the ability to create incentives that promote training. Training is important because you want the people you hire to grow in time to maintain or increase their value. If employees prefer a "live session", departments could have team training sessions using the LMS and the leader can commentate as necessary. (This is training apart from the security awareness training)

3. **Executive & Stakeholder Overview**

- Purpose: The purpose of the security awareness program is to create and maintain a company culture that “lives and breathes” the best practices for modern information security.
- Scope: The security awareness program directly deals with the company’s major assets: the people and data.
- Objectives: We want to ensure that confidentiality, integrity, and availability remain consistent with all assets in the company.
- Timeline: The implementation of this program is estimated below:

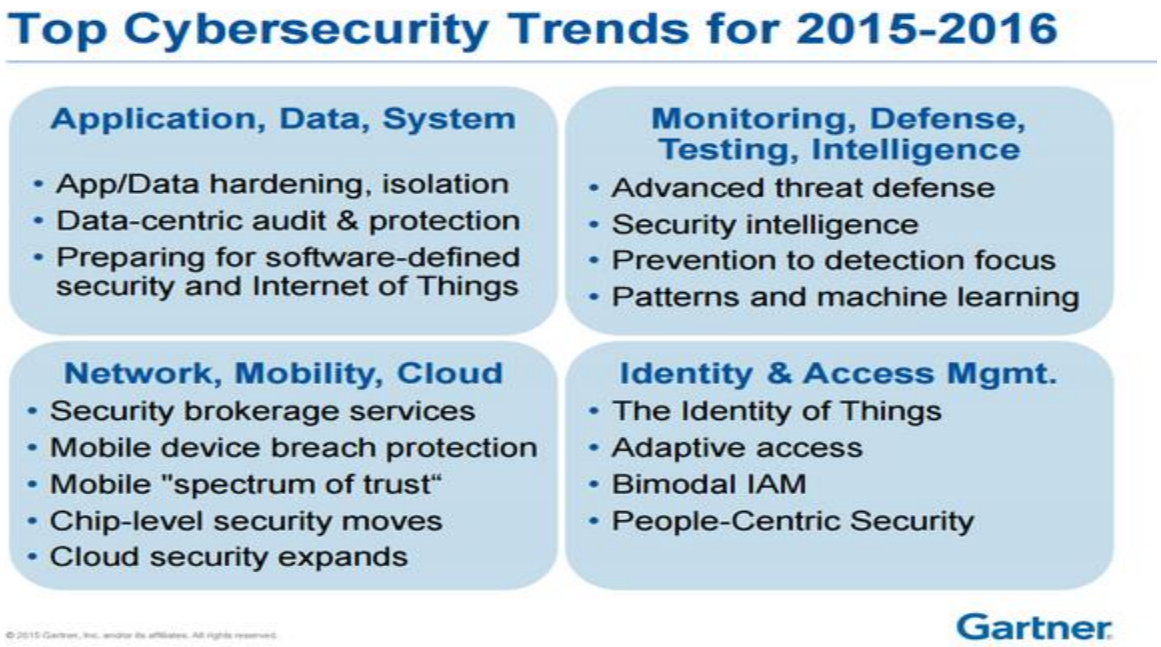


- Stats & Trends: Due to the rise in numbers of attacks and data breaches, cybersecurity has started to “boom” in the market. Companies are realizing the importance or properly securing their assets and are taking the necessary action to promote security best practices. Below is a market forecast analysis that speaks to this point:



(Gilani, Baldwin, Wyckoff, & Anderson, 2016)

Below are the top security trends per Gartner analysis (Panetta, 2016):



As technology grows and is further adopted into business enterprise processes, security challenges will continue to arise. Below is Intel's analysis (Rosenquist, 2014):

Below is IBMs 2015-2016 Analysis (Hirani, 2016):

Our purpose, scope, objectives, and timeline were all strategically created for the company to address some of the trends and stats shown above. Costs and breach/attack statistics are shown above to educate and emphasize the point that securing company assets should always be part of the company strategy. Our information security awareness program will help the company adapt to a security culture while also improving the information security infrastructure along the way. Security awareness and training programs in general will help to reinforce user compliance with security policies and help reduce risks posed by users throughout the company.

Broad & Diverse Communication Strategy:

Apart from the internal stakeholders, our team will also be communicating outward to others we do business with to inform them of the new positive changes. We need to understand external stakeholder influence and attitudes, and assess positive and negative attitudes and behaviors. Once strategy we will use is to create surveys and measure responses to our objectives and metrics. Some questions to consider while planning to send out surveys to stakeholders are shown in the table below:

What do they value most?
How will their commitment to the program and the work be measured?
What authority do they have to effect the required change?
Have they clearly communicated their needs and requirements?
What areas/stakeholders are in conflict?
Are they willing to take ownership upon program completion?
Who will have the most influence, impact on program success?
How do you handle the stakeholder that gets the short end of the stick?

Planning and knowing the audience is key, so we will utilize the SMART criteria when communicating with all stakeholders:

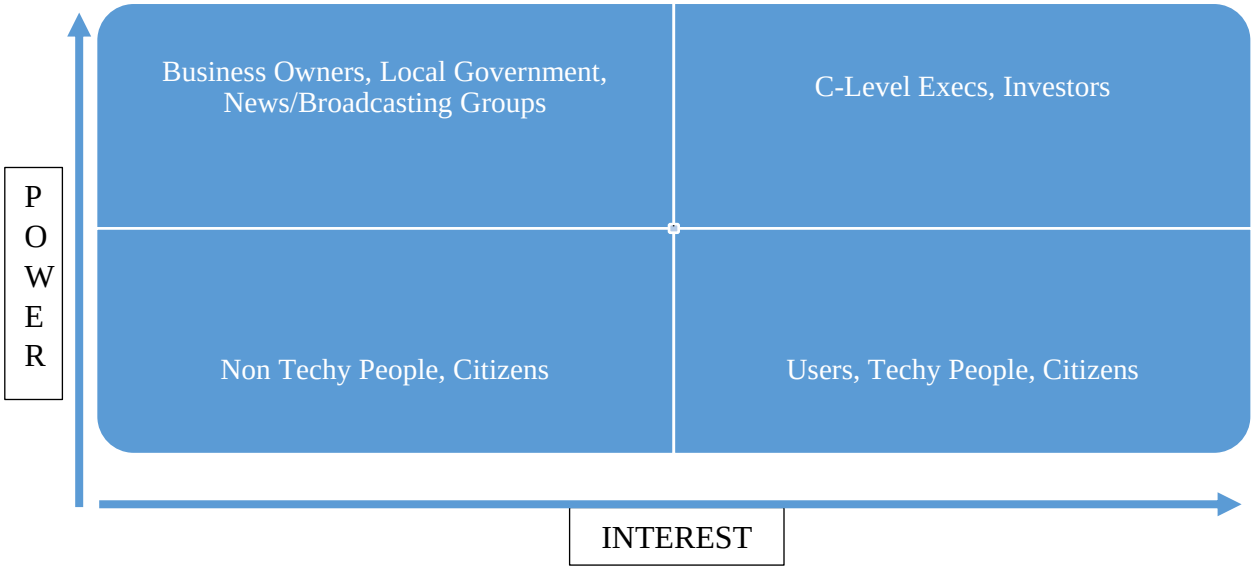
- **Specific –**wording is clear and concise.
- **Measurable –**the program has criteria that can be tested.
- **Achievable –**the program can be successfully implemented in the environment.

- **Realistic –**the program is appropriate to the company scope and resources.
- **Traceable –**the program can be associated with a stakeholder, process, system, model, test document.

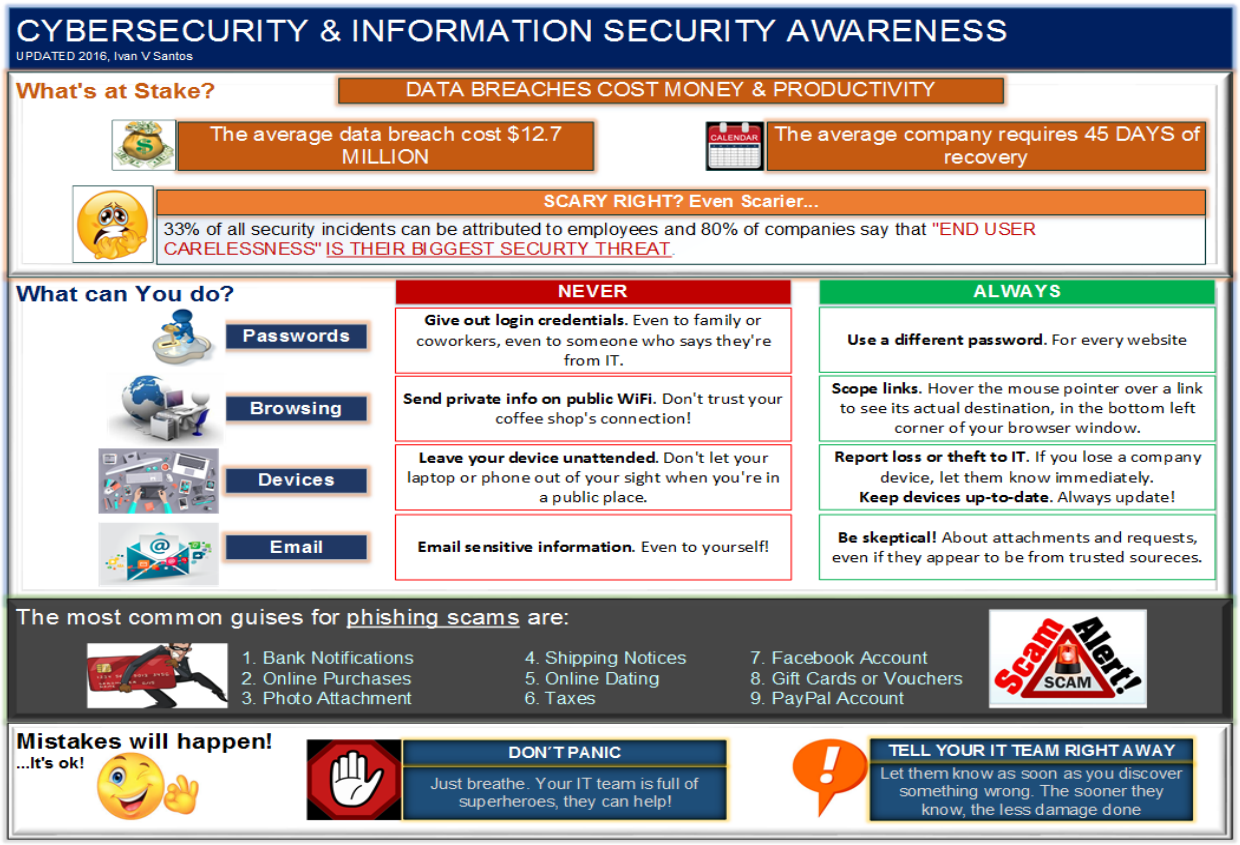
Interaction is essential when promoting any culture change. For a security culture change, some of these interaction type meetings will be held by the "culture ambassadors" to help facilitate positive promotion (with end users and/or managers and up):

- **Interviewing** – eliciting detailed information from individuals and educating them on new changes.
- **Brainstorming** – group technique that provides broad spectrum of ideas and information and helps derives themes for further analysis.
- **Observing a job** – assessing a role or process from a user's interaction perspective to gain insight, and provide feedback as it relates to the new changes.
- **Surveying** – a way to elicit information from many people in a short amount of time. Use these to measure metrics for objectives and strategy.

A visual strategy for planning that we will use is creating a basic power vs interest matrix as shown below (chart will vary based on targeted audience):



A chart like this can be very helpful when planning the presentation and the language that will be used for communication. All the strategies above will help in communication efforts for promoting the security awareness program. Probably the best strategy for external buy-in is just to be a positive ambassador for the security awareness program: consistently find genuine opportunities to share information about the program and utilize your relationships throughout the company to further promote the positive change. The best way to make it "real" to someone is make them aware of the current day security issues, then pinpoint an experience they might have had dealing with security. The security awareness program is beneficial for both work lie and personal life because the users will get best practice training on current information/cyber security. We have also created a basic 1-pager infographic in VISIO that will be issued out to all users as a guide for best practices (ALSO SENT SEPARATE ATTACHMENT):



The communication plan is an essential step to achieving a successful information security awareness program. We can obtain buy-ins by conducting research to understand the audience, thoroughly preparing and executing a SMART presentation, and continuously be a positive ambassador for the project. Communication doesn't start at the presentation; it starts on the day-to-day work life. The stakeholders, users, and the company should be able to see excitement and positivity from those driving the security initiatives. By incorporating all the said techniques and key points, the security awareness program will indeed have a bright outlook.

4. **Approval**

Approval is to be signed by the company leadership involved in decision making.

_____

Name, title Date

_____

Name, title Date

_____

Name, title Date

References

Gilani, S., Baldwin, G., Wyckoff, J., & Anderson, K. (2016, December 19). The best type of Cybersecurity companies to invest in now Retrieved from http://moneymorning.com/2015/02/27/the-best-type-of-cybersecurity-companies-to-invest-in-now/

Hirani, S. (2016, September 28). SCET explains — Cybersecurity - UC Berkeley Sutardja center. Retrieved December 18, 2016, from CSEC, http://scet.berkeley.edu/scet-explains-cybersecurity/

ISO. Information Security Management. Retrieved from www.ISO.org, http://www.iso.org/iso/iso27001

Lisa Welshhons. How Employee Wellness Programs Can Generate Savings for Your Company. Retrieved December 4, 2016, from http://web.archive.org/web/20160403011918/http://meritresources.com/userdocs/materials/Employee_Wellness_Initiatives_Merit.pdf

NIST. Retrieved December 12, 2016, from nvlpubs.nist.org, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Panetta, K. (2016, June 15). Gartner's top 10 security predictions 2016 - smarter with Gartner. Retrieved December 18, 2016, from IT, http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/

Rosenquist, M. (2014, February 13). Jinho Joo. Retrieved December 18, 2016, from Intel, http://www.slideshare.net/MatthewRosenquist/cyberstrat14-helsinki-matthew-rosenquist-2014-public

PCI DSS. Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. (n.d.). Retrieved November, 2016, from https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

SANS Institute. Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It. Retrieved December 4, 2016, from SANS, https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-is-needed-35030

Security, I. (2016, September 28). IBM Cyber security intelligence index - United States. Retrieved November 12, 2016, from http://www-03.ibm.com/security/data-breach/cyber-security-index.html?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

SNHU. Retrieved December 21, 2016, from https://bb.snhu.edu/bbcswebdav/pid-13660544-dt-content-rid-38036283_1/courses/IT-552-16TW1-MASTER/IT-552%20Student%20Documents/IT%20552%20Final%20Project%20Document.pdf

Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviours. Computers and Security, 24, 124-133.

Verizon's 2016 Data Breach Investigations Report. (n.d.). Retrieved November, 2016, from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/