
SECURITY AWARENESS TRAINING PROGRAM EXECUTION PLAN

Tim Larkin
IT VOLUNTEER

Table of Contents

<u>EXECUTIVE SUMMARY</u>	<u>3</u>
<u>ORGANIZATIONAL STRUCTURE AND STAKEHOLDERS</u>	<u>4</u>
MANAGEMENT SUPPORT MATRIX	4
STEERING COMMITTEE MATRIX	5
<u>TARGET AUDIENCE</u>	<u>6</u>
TARGET GROUPS	6
<u>AWARENESS PROGRAM TARGET AREAS</u>	<u>8</u>
RISK ASSESSMENT	8
SELECTED TRAINING TOPICS	9
TRAINING REQUIREMENTS BY TARGET GROUP	10
<u>DELIVERY/COMMUNICATION METHODS</u>	<u>11</u>
CULTURAL REQUIREMENTS	11
LANGUAGE REQUIREMENTS	11
TRAINING DETAILS	11
DELIVERY SCHEDULE	13
<u>PROGRAM UPDATES</u>	<u>14</u>
REVIEW AND UPDATE PROCEDURES	14
WHO WILL UPDATE	14
<u>PROGRAM EFFECTIVENESS METRICS</u>	<u>15</u>
<u>LEARNING OBJECTIVES</u>	<u>ERROR! BOOKMARK NOT DEFINED.</u>

Executive Summary

This organization is a shelter for victims of domestic violence. The organization maintains two physical locations; the first is an administrative office with a publicly known physical address that hosts board meetings, administrative staff, and serves as a donation drop-off site. The second location is the shelter for victims of domestic violence and is not publicly known. This is to help provide physically security to the victims and their families that we serve.

To date the organization has made minimal investment in personnel, processes, or technology with respect to Security Awareness or Information Security. Through volunteer efforts some technology-based risk mitigation strategies have been donated, configured, and deployed. These include a firewall, Microsoft domain controller and WSUS, and a domain wide backup solution. While technical controls continue to be updated and upgraded within the scope of the limited budget, the organization has made no effort thus far to address the risks that can be mitigated through a Security Awareness Program.

The goal of this program is to secure peoples' behaviors to prevent unintended or unlawful disclosure of sensitive information that could catastrophically result in the physical or emotionally harm of the people we serve. In addition, any type of security incident could expose our organization to reputational or legal damage, ultimately causing us to be shut down. The Board of Directors and the Executive Director understand the need for cultural change and increased awareness. This Security Awareness Program is the first step toward these goals.

Organizational Structure and Stakeholders

Management Support Matrix

The organization enjoys extensive management support and interest in establishing a security awareness program. This, however, does not equal extensive financial support to provide a budget for the program. In light of this, the organization expects no trouble receiving senior leader buy-in. The Executive Director will serve as the project champion. As with most efforts within this organization, it will be supported with what volunteer labor and free, publicly available materials are available. The senior leaders identified in the table below have been identified as having key roles in ensuring the effectiveness of this security plan.

Name	Current Commitment Level	Target Commitment Level	Engagement Strategies
President of the Board	High	High	Keep briefings short and to the point; concentrate on value to organization.
Executive Director	High	High	Show value of project, compliance, and project management; keep briefings and communications short and efficient.
Director of Program Services	High	High	Interested mainly in keeping the subject matter and presentation simple and easy for staff to understand.
Director of Development and Marketing	High	High	Coordinate with marketing early to ensure we are following the organizational communication policy.
Director of Finance	High	High	Explain that we understand that there is little to no Security Awareness budget and we can work within that scope.
Shelter and Volunteer Coordinator	High	High	Coordinate ahead of time, get her on the Steering Committee, as she will be the primary interface between employees and any security-related questions or reporting.

Advisory Board Matrix

The Advisory Board provides the awareness program's important stakeholder input. The committee will also assist with overall organizational buy-in. The members of the Advisory Board will be solicited for input in all training materials, scheduling, and major decision points and will meet in person, initially. Follow-on meetings will be held as needed, but most communication is expected to take place via organizational email.

Name	Department	Reason for Being on Steering Committee
Executive Director	Executive	Champion of the awareness program. Sits in on Steering Committee to provide any executive assistance and support. In addition, this individual provides direct communications to the Board of Directors.
Marketing Director	Marketing	Assists with developing and communicating our core messages. Also enables us to use the organization's internal communication mechanisms and better understand any communication limitations or requirements.
Shelter Coordinator	Shelter Staff	An excellent resource for better understanding our organization's culture. She can also help coordinate awareness training for new hires and assist with any enforcement issues.
Director of Program	User Representative	Director of Program is a power user and has visibility over the responsibilities of all members of the shelter staff. Her input will be invaluable.
Volunteer Rep	Volunteer	This volunteer is a long-time volunteer at the shelter and will provide valuable feedback from the volunteer perspective.
Legal Advisor	Executive / Legal	Board member with legal expertise.

Target Audience

The first step in building a mature security awareness program is to identify whose behaviors we want to change. Different target groups have different risks, roles and data that they handle. As a result, the level, frequency and methods of training will vary between the targeted groups. For our program, we have identified three target groups, described below.

Target Groups

Target	Description	Why	Location	Unique Requirements
Board of Directors	Volunteer group of business people / community leaders infrequently at either physical location. Each member's individual reputation and information security posture is a significant factor in the overall reputation and security posture of the organization.	Board members are key stakeholders that can influence budget, buy-in, and priority. Board members work almost exclusively with personal devices and a compromise of any board member would dramatically affect the reputation of the organization as well as put a significant amount of sensitive data at risk.	Admin Office and Remote	Rarely in the same place at the same time. Remote training may be the only way.
Staff	Staff includes the administrative staff of the Executive Director, Finance personnel, Marketing, and administrative assistant. The shelter staff and volunteers include personnel who provide for the daily upkeep of the shelter, therapists and counselors, volunteers who	Personnel who store and process critical information for the back-end of the organization or sensitive client information. These personnel are required to interact directly with clients/victims and may have specific requirements (e.g. therapists and HIPAA) for their data.	Admin office and shelter	Lack of IT expertise means that IT Security must be easily implemented and clearly presented.

	<p>receive hotline phone calls and record data of current and future clients or victims. These personnel use organizational IT resources as well as personal smart phones and laptops to process and store data.</p>			
Clients	<p>Victims of domestic violence and their dependents receiving shelter or assistance from the organization. This target group is received into the shelter program with no notice, provided shelter for a period of approximately 90 days, and who then move out of the shelter once safe and stable lodging is acquired.</p>	<p>The clients of the organization are victims of domestic violence who are temporarily dependent on the organization for life sustaining shelter, physical and mental healthcare, food, and safety. As physical harm has already occurred, it is imperative that we communicate the principles of Security Awareness to the adults and children in this target group, as appropriate, in order to help the clients maintain a safe and secure life.</p>	Shelter	<p>Interacting directly with victims of domestic violence requires special training and techniques and must be done in accordance with the guidance of the shelter coordinator. Further, the shelter's stated policy of anonymity and non-disclosure must be adhered to strictly when interacting with the clients.</p>

Awareness Program Target Areas

Risk Assessment

Our goal is to focus on the smallest number of topics (human risks) possible that represent the greatest risk to our organization. The fewer human risks we focus on, the more likely we effectively change the required behaviors and manage human risk to our organization. We identified the top human risks by completing a human risk analysis of our organization. The following risk assessment examines the probability and impact of a given risk which may negatively impact the organization. Likelihood was ranked on a five-category scale to include very low, low, medium, high and very high based off previous events and subjective analysis of future probability. Impact was ranked on the same five-category scale but focused on a qualitative and quantitative analysis of the operational environment and associated processes when the given risk is introduced.

Data considered for this assessment included a trend analysis of perceived security related events and incidents either observed by or reported to the IT volunteer, current status and trend analysis of the patch management (WSUS) effort and vulnerability management report, and the status of organizational compliance of data storage and processing requirements mandated by grantors. The total score accounts for the likelihood and impact. This risk assessment must be revisited in future updates of the awareness program to ensure continued risk accuracy.

Risk	Likelihood/Probability	Impact	Total Score
Social Engineering	Very High	Very High	High
Mobile Device Security	Very High	High	High
Data Security	Medium	Very High	High
Social Networking	Very High	Very High	High
Email and Messaging	Very High	Low	Medium
Browsing	Very High	Low	Medium
Targeted Attacks	Low	High	Medium
Passwords	Medium	Low	Low
Malware	Medium	Low	Low
Working Remotely	Very High	Very Low	Low
Cloud	Low	Low	Low
Physical Assault	Low	Low	Low

The total score column above was calculated using the following criteria. Once the likelihood and impact were calculated, the table below derived the overall total risk score:

Probability	Very High	Low	Medium	High	High	High
	High	Low	Medium	Medium	High	High
	Medium	Low	Low	Medium	High	High
	Low	Low	Low	Medium	Medium	High
	Very Low	Low	Low	Low	Medium	High
		Very Low	Low	Medium	High	Very High
		Impact				

Selected Training Topics

The following four human risks were selected as the priority efforts based on the “high” risk assessment in the table above. While every risk identified in the assessment above is important and will eventually be addressed by the security awareness program the constraints of volunteer staff availability and lack of budget make it necessary that the program begins by first addressing the topics assessed as high risk. The table below outlines the risk topics, why the topic was selected and why the topic reduces overall risk.

Top Human Risks/Topics	Why Selected	How Risk is Reduced
Social Engineering	The organization is on the receiving end of Social Engineering attacks every day. These attacks can manifest in the form of email, phone calls, and face-to-face interactions. As many of the clients are literally hiding from known abusers who intend to do them physical harm, it is paramount that staff be aware of social engineering attacks.	This risk is reduced through awareness and through social engineering exercises intended to teach staff members how to recognize and react to perceived social engineering attacks.
Mobile Device Security	The organization relies heavily on BYOD with little to no oversight, user education, or risk management. As mobile devices (laptops / phones) are routinely used by staff to process and store organizational	This topic will educate users on encryption, authentication, screen-locks, remote wiping, etc. as well as impressing upon the users what steps are required when a device is lost or stolen. It is important that all

	data, it is important that this risk be mitigated as best as possible.	users understand the risk involved with the use of mobile devices.
Data Security	The organization routinely processes two types of very sensitive data: victim abuse reports / personal histories and back-end organizational data akin to human resources and financial records.	This risk is mitigated through user education and the proper implementation of processing, storing, transmitting, and destruction of sensitive data.
Social Networking	Social Networking is a primary method of both organizational communication and attackers targeting this organization.	Educating the Board of Directors and Staff on common Social Networking attacks and proper security settings in social network sites will help to reduce the attack surface of the organization.

Training Requirements by Target Group

Training Module / Target Group	Initial Training	Online CBT	Interim Communications		
	Board of Directors and Staff	All Target Groups	Board of Directors	Staff	Clients
Social Engineering	X	X	X	X	X
Mobile Device Security	X	X	X	X	X
Data Security	X	O	X	X	X
Social Networking	X	X	X	X	X

Delivery/Communication Methods

Cultural Requirements

The organization operates in two locations within the metropolitan area, and all board members and staff live locally. Clients are primarily from the southeast quadrant of the United States.

An analysis of Board of Directors and Staff by generation:

1. Baby Boomers (1945 – 1964): 80%
2. Generation X (1961-1981): 10%
3. Generation Y or Millennial (1975-1995): 5%
4. Generation Z (1995 – 2015): 5%

An analysis of 2017 Clients by generation:

1. Baby Boomers (1945 – 1964): 10%
2. Generation X (1961-1981): 30%
3. Generation Y or Millennial (1975-1995): 30%
4. Generation Z (1995 – 2015): 30%

Language Requirements

English is the primary language of employees and staff. However two of our employees are fluent in Spanish as well. This is due to twenty per cent of our clients are native Spanish speakers who speak English as a second language, or not at all. As such, all electronic and printed materials will be provided in Spanish and English. A bi-lingual staff member will be present for all Client training sessions if necessary.

Training Overview

We understand and recognize that training people once a year is not enough to change their behaviors. As a result, we continuously reinforce key behaviors using a variety of different training methods and modalities. In addition, due to our almost non-existent budget we have to rely on and leverage free resources whenever possible. The target groups for this Security Awareness Program are the Board of Directors, Staff, and Clients. In all cases, this program will utilize a combination of face-to-face interactive training sessions, online computer based training, handouts and digital communications such as email and newsletters. These delivery methods are scalable due to the small size of the organization.

Initial / Primary Training

Interactive training sessions will be delivered for the Administrative Staff and the Board of Directors at the Administrative Office location. The initial training for the Board of Directors and Staff target groups will consist of a one hour block of interactive instruction and question and answer session. The initial training for both the Board of Directors and the Staff will have an identical outline. It is likely that

Questions and Answers will differ greatly between the two target groups due to different work functions and focus.

Due to the transient nature of the Client target group, there will be no opportunity for a coordinated initial training session. Instead Clients will receive initial awareness training during their onboarding process from staff that are onboarding them. This will include staff giving the clients a quick-tips fact sheet and a verbal overview of key behaviors, such as protecting the location of the shelter.

Follow-on / Reinforcement Training

Additional training sessions will be delivered at the shelter location for all Staff and Clients, but in separate sessions for each target group. Initial training for the Staff will consist of a one hour interactive training session followed by a question and answer period. Follow-on training will consist of 30-minute interactive training sessions each quarter with electronic communications in the interim. Follow-on training will be tailored to each location as applicable. Each training session will identify the learning objectives for that session and participants will take part in a verbal discussion to include checks-on-learning to verify that the objectives have been met. Attendance sheets for each session will record which staff members were present.

Additional reinforcement will include electronic communications via email and text messaging, to include materials such as fact-sheets and newsletters. Each method of communication will have a Security Awareness trivia question or challenge for staffers to respond to. All correct answers will be entered into a drawing for a reward to be determined by the Executive Director. Response levels to these messages will be tracked for effectiveness.

Free Security Awareness Resources

- National Cyber Security Alliance – <https://staysafeonline.org/cybersecure-business/>
- OUCH! Monthly Newsletter - <https://www.sans.org/security-awareness-training/ouch-newsletter>
- Microsoft Safety - <https://www.microsoft.com/en-us/safety/pc-security/default.aspx>

Delivery Schedule

Upon initial approval, the first training session will be conducted at the Administrative Office coinciding with the next meeting of the Board of Directors. Quarterly sessions not exceeding 30 minutes will follow to coincide with the meetings of the Board of Directors. One week after the initial session with the Board of Directors, the initial session for the shelter location will be held to coincide with an already scheduled weekly staff meeting. Quarterly sessions not exceeding one- hour will follow scheduled on the same week as the Board of Directors quarterly sessions. The online computer based training will be made available to all employees. The training will be available continuously and employees will have a suggested module per quarter. Interim communications will be delivered in the interim months by email and text message.

Q1	JAN	FEB	MAR
	Social Engineering Interactive Session	Social Engineering Email	Social Engineering Text
Q2	APR	MAY	JUN
	Mobile Device Security Interactive Session	Mobile Device Security Email	Mobile Device Security Text
Q3	JUL	AUG	SEP
	Data Security Interactive Session	Data Security Email	Data Security Text
Q4	OCT	NOV	DEC
	Social Networking Interactive Session	Social Networking Email	Social Networking Text

Program Updates

Review and Update Procedures

The organization's Security Awareness Plan will be reviewed and updated annually. Any feedback received and changes requested will be considered by the Steering Committee for inclusion or changes. Measured effectiveness will be provided to the Executive Director and the Board of Directors so that senior leadership can review effectiveness of all or part of the program.

Who Will Update

The comprehensive awareness plan will be updated by the volunteer IT staff member before the January meeting of the Board of Directors each year.

Program Effectiveness Metrics

What is Measured	Metric	Metric Owner	How	Frequency	Type
Initial Training – Face to Face	Number of Employees present at the session	IT Volunteer	Attendance sheet	Annual	Compliance
Initial Training – Onboarding Client	Number of Clients training on security basics	IT Volunteer	In person by staff	As part of onboarding	Compliance
Mobile Device Screenlocks	Percentage of individuals who have screenlocks enabled.	IT Volunteer	Survey individuals	Monthly	Impact
Mobile Device Geolocation	Percentage of individuals who have geolocation disabled	IT Volunteer	Survey individuals	Monthly	Impact
Social Engineering	Percentage of employees and staff that can identify key clues of a social engineering attack	IT Volunteer	Assess workforce	Monthly	Impact