

README

The organization chosen for this assignment is a technology startup in the financial technology sector. The organization's name, locations, and any other identifying information have been changed to limit legal liability. The organization, which shall be called Dauntless for this assignment, was chosen due to the authors familiarity with both the sector and industry they are in. The organization was founded less than 4 years ago and is currently seeking to become the next technology unicorn with a \$5 billion IPO planned for next summer. As such, all focus within the organization is on bottom line revenue and removing any obstacles on the public offering path.

Dauntless is in the financial business and seeks to cross open source intelligence, regional statistics, and other disparate sources of information with traditional financial algorithms through artificial intelligence to provide customers with a distinct competitive advantage. Dauntless has multiple offices located across the US and currently employs about 200 employees across each of the offices.

There are currently limited cybersecurity functions performed within the Dauntless organization. Dauntless management has been informed that the bank underwriters will look negatively on this and it will adversely impact their initial offering price. In response, Dauntless has hired the author to come in and build the cybersecurity components required for compliance starting with security awareness. This security awareness project plan is the author's proposal to build a program that goes beyond compliance and helps to secure the organization.

Due to the nature of this assignment, this project plan is a hybrid of what would be submitted and what was required in the grading rubric for this assignment. Certain sections such as the Executive Summary, Project Charter, and first part of the Engagement Strategy section would be submitted as part of an actual project plan with a few modifications. Other sections such as the rest of the Engagement Strategy and the Appendix would be significantly rewritten or omitted completely. As such, certain terms which would be understood by executive management within this organization, such as KPIs and KRIs, have not been explained and elaborated upon. Information about the risk assessment, described in the problem section of the executive summary, which drives the need for this plan has also not been expanded upon outside of this README document.



DAUNTLESS CYBERSECURITY AWARENESS PROJECT PLAN

FEARLESS CYBERSECURITY

This document is a mock awareness project plan written for a SANS graduate course, ISE 5300, and should not be utilized outside of this medium. The Author is not responsible for Career Limiting Events (CLEs) that may result from the unintended use and distribution of this document....



Table of Contents

Executive Summary.....	3
Problem.....	3
Solution	3
Cost	3
Project Charter.....	4
Engagement/Training Strategies	5
Organizational Culture	5
Communication and Modalities.....	6
Reinforcement	7
Branding.....	7
Metrics	8
Phase 1: Compliance Focused Metrics	8
Phase 2: Behavior Change Metrics	8
Phase 3: Sustainment Metrics	9
Appendix	10
Learning Objectives.....	10



Executive Summary

Problem

The lack of a cybersecurity awareness program will hinder our initial public offering valuation. During our last cybersecurity assessment, security awareness was identified as one of the critical deficiencies in our cybersecurity program. The lack of this program poses immediate regulatory risk as it is required for compliance with 23 NYCRR 500 and exposes us to long-term risk through lack of mitigating controls for the top cause of cybersecurity breaches in small and medium-sized businesses.

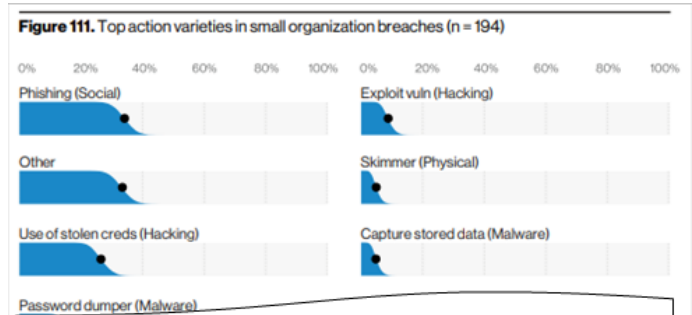


Figure 1: Root Cause of Breaches for SMBs
Source: 2020 Verizon Data Breach Investigations Report

Solution

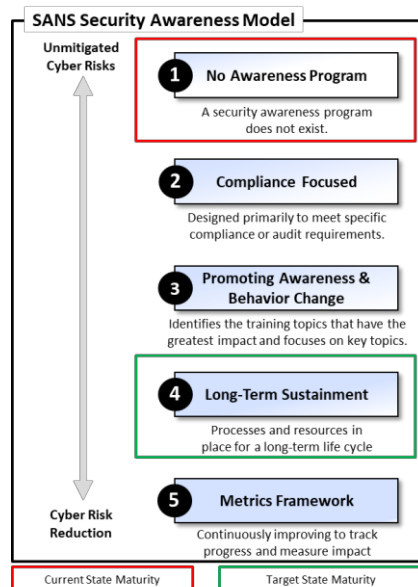


Figure 2: The SANS Security Awareness Model

Security awareness is the knowledge and attitude members of an organization possess regarding the protection of physical and digital assets. Formal programs around security awareness aim to train individual users on behaviors and actions which reduce cybersecurity risk. A common method of gauging security awareness across differing organizations is the SANS Security Awareness Model. As an awareness program matures, it becomes able to influence meaningful and measurable behavior changes within the organization. As it further matures, these behavioral changes become sustainable and systematic. The goal of our program is to provide evidence to the underwriters beyond a shadow of a doubt that we are in regulatory compliance and to quantifiability reduce cybersecurity risk throughout the lifecycle of the program.

Cost

The estimated initial cost to build the project is \$65,000 with a run cost of \$40,000 after the foundational elements are in place. Build costs are primarily capital expenditures to fulfill technology gaps required for project competition. The build duration is estimated at 12 months with ongoing operations continuing indefinitely. Initial staffing requirements can be met with existing personnel with a final FTE count of 3 (2 additional FTEs in twelve months) required for run.

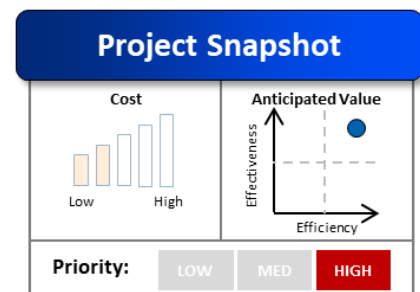


Figure 3: Project Charter Summary



Engagement/Training Strategies

Creation of an effectiveness and sustainable security awareness program will occur in three specific phases aligned to progression through the SANS Security Awareness model. The first phase will be designed to bring the organization into compliance with regulatory standards. In the next phase will be specialized activities designed to identify and mitigate cyber risk specific to Dauntless. In the final phase, activities will focus on reinforcement and integration of security awareness as a part of the Dauntless culture.

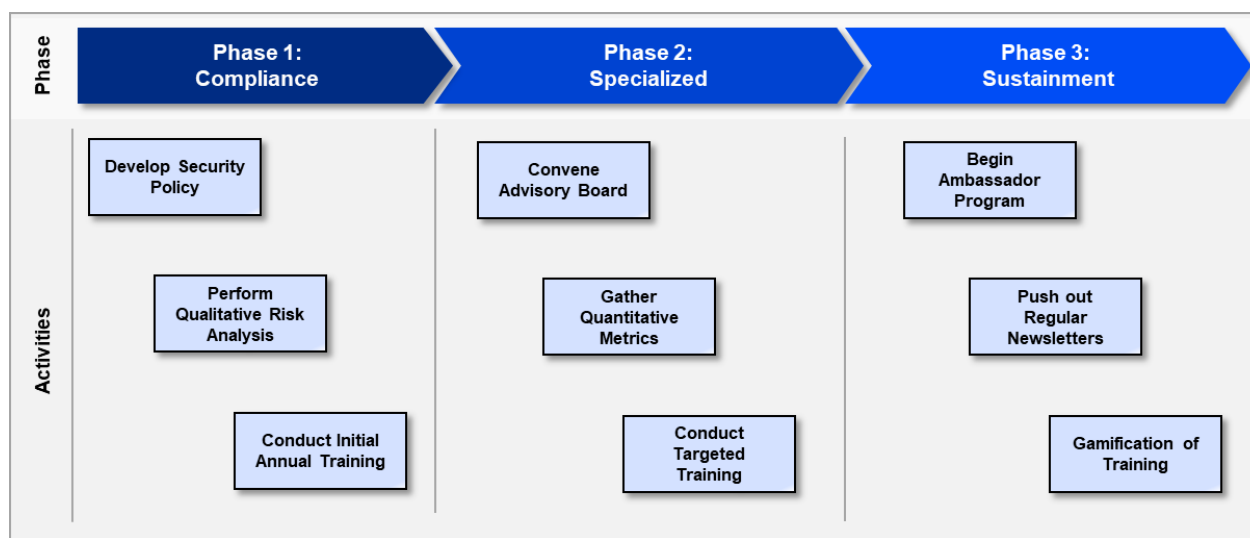


Figure 4: Project Build Phases

The success of the program will hinge on tailoring these activities around distant concepts across build phases.

Organizational Culture

Integrating security awareness into organizational culture is critical for a program that strives beyond regulatory compliance. To achieve long term sustainable behavioral change, the program must change the security beliefs, values, and perceptions of those involved.

The culture at Dauntless empowers all employees towards cybersecurity innovation, fearlessly capturing the financial insurance market and boldly pushing services to the next level. This desire permeates everything employees do and is further empowered by the Silicon Valley startup culture. Hand in hand with this outgoing culture is a competitive nature among business units and teams. It is not uncommon to find intercompany sporting events taken to the next level with mutually agreed upon fun wagers between business unit teams. This boldness also leads to throwing caution to the wind in favor of results in the realm of cybersecurity.

Alignment with our culture is critical for the success of the proposed security awareness program. This alignment will occur in two distinct areas. The entire company will be introduced to external cyber threat adversaries in the initial training proposed in Phase 1 of the build plan. The intention with this inclusion will be to bring the broader cybersecurity program



in line with our organizational culture by highlighting the fight between well organized and funded external cyber adversaries against up-and-coming small and medium business such as ourselves. This will ignite the competitive fires of our employees and motivate them to put on their game faces with regards to cybersecurity. Alignment will also occur in Phase 3 through the proposed gamification of training. This gamification of security awareness will create a leaderboard which ranks individuals in the organization, as well as their subsequent business unit teams, against each other on specific security awareness categories.

Communication and Modalities

How security awareness content is delivered to a user is as important as the content itself. Not only does this have a direct correlation with how receptive the user will be to the content, it also enables or limits subsequent security awareness activities

The delivery method for security awareness content will vary across each of the build phases to take advantage of individual strengths in each approach. In Phase 1, initial training of users will be instructor led. Instructor-Led Training (ILT) minimizes the upfront costs in the initial phase and allows us to customize the training in real time with relevant examples, stories, and demonstrations based on the reaction of the audience. These customizations will be critical in establishing that initial interest in taking up the cybersecurity fight, aligning the overall security awareness program with our organizational culture. This also enables us to customize that initial training to be more receptive in each locale. To lead this training, we will evaluate members of the internal security team before looking at outside industry subject matter experts to ensure maximum impact, optimal results, and minimal costs.

In Phase 2, we will switch to utilization of computer-based training (CBT) to deployed targeted content modules as well and ongoing annual training content. There are three primary benefits to CBT in this phase: it enables gathering of quantitative metrics around content, provides convenient attendance options for users, and enables activities around gamification in Phase 3. Quantitative metrics gathered from security awareness content delivery will allow us to measure residual cybersecurity risk. These metrics will be augmented with monthly simulated Red Team exercises to develop a content roadmap with prioritization by impact. The ease of consumption for this modality minimizes the demands on users' time and frees them to continue the great work they are doing. Finally, CBT laid the groundwork for the gamification of security awareness which is a pivotal aspect to long term sustainment in Dauntless.

In Phase 3, we will also begin pushing out monthly security awareness newsletters in addition to the ongoing CBT. These newsletters will focus on a specific cybersecurity concept or story that is relevant to Dauntless with the purpose of generating user interest in subsequent newsletters. Custom templates that utilize company branding will be developed and usage metrics will be tracked as part of qualitative metrics activities. While this activity is primarily intended to reinforce security awareness concepts and content, it will also tie into gamification efforts in the form of trivia questions.



Reinforcement

With the information overload in our digital age, secure awareness must continually be brought to the forefront of thought to ensure continued effectiveness. This is one of the most difficult aspects of security awareness as continued effectiveness also depends on the user being receptive to the reinforcement method.

Given the importance of reinforcement to achieving the target level of maturity for our security awareness program, we will pursue a three-pronged reinforcement approach focusing on negative, neutral, and positive activities. Negative reinforcement will occur through quarterly phishing campaigns in Phase 2, identifying users who fall victim to campaigns and mandating additional OnDemand CBT for those users. This type of primary reinforcement directly addresses cybersecurity risk from this threat vector. Neutral reinforcement will occur in Phase 3 through monthly cybersecurity newsletters which are covered in greater detail in the “Communication and Modalities” section.

Positive reinforcement will be conducted through gamification of the security awareness program developed in Phase 3 and which integrates numerous activities across different phases. This gamification will fuel the fire kindled in the initial awareness training of Phase 1 and provide a catalyst for ongoing sustainment. Gamification topics will be driven by both the qualitative risk analysis and quantitative metrics findings before being signed off on by the advisory board. Regular phishing exercises resulting from targeted training in Phase 2 and the monthly newsletters in Phase 3 will serve as potential inputs into the gamification program as opportunities to earn points. The leaderboard for the security awareness gamification program will be published on the information technology security intranet site. Ambassadors can use this to stir up friendly competition in security awareness between individual business units. As additional positive reinforcement, monthly top-ranking individuals and teams will be awarded “Cybeer”, the custom brewed and bottled beer of our internal IT security team.



Figure 5: Cybeer, Consumable Bragging Rights

Branding

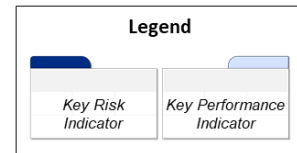
Creation of emotional bonds through mascots, logos, and taglines can assist with retention of interconnected cybersecurity elements. This also helps to distinguish the organization's security awareness program from other aspects of cybersecurity in different domains of life.

All company branding elements will be utilized for both build and run phases of the security awareness program. This intimately links the security awareness program with the Dauntless culture, upon which the program was designed around. Derivatives of the corporate tagline “Fearless Innovation” may be explored in Phase 1 to highlight the threat adversary risk and in Phase 3 to highlight the internal competition elements of the security awareness program.



Metrics

Measurable metrics are the only reliable method of measuring the residual risk and progress of the security awareness program through maturity levels. While differing metrics will be gathered across the life cycle of the project, they will be grouped into two distinct categories. Key Risk Indicators (KPIs) will measure the direct impact of the program against identified risks also known as the program's effectiveness over time. Key Performance Indicators (KPIs) will measure the success of the security awareness program in achieving its objectives over time also known as the program's efficiency. These two categories will be measured across each build phase to demonstrate the impact of the security awareness program within Dauntless.



Phase 1: Compliance Focused Metrics

Training Attendance			Reported Sec Events		
Description <i>This is the number of employees who have attended or completed mandatory ILT or CBT.</i>			Description <i>The number of potential security events reported to the information security team through email, phone, or in person.</i>		
Who Collects	Collection Frequency	How Measured	Who Collects	Collection Frequency	How Measured
Security Awareness Officer	Annually	# of Employees Completing Training	Information Security Manager	Monthly	# of Security Events Reported
Why Collected This metric will be used to prove we are following any mandated compliance requirements and directly addresses risk of non-compliance.			Why Collected This metric will be used to evaluate if the initial security training resonated with employees by measuring if employees are acting on the information.		

Phase 2: Behavior Change Metrics

Phishing Test Victims			Reported Phish Emails		
Description <i>The number of users who fall victim to red team phishing exercises conducted on a monthly basis.</i>			Description <i>The number of users who successfully identify and report phishing emails to the information security team.</i>		
Who Collects	Collection Frequency	How Measured	Who Collects	Collection Frequency	How Measured
Information Security Manager	Monthly	# of User Opening Attachments or Links	Information Security Manager	Monthly	# of Positive User Reports per Campaign
Why Collected This metric will be used to evaluate business and operational risks associated with the most common initial attack vector for SMB breaches.			Why Collected True positive user submissions per campaign will enable measurement of targeted behavioral changes which directly mitigate risk.		



Phase 3: Sustainment Metrics

Newsletter Downloads		
Description <i>The number of times the monthly security awareness newsletter and linked resources have been downloaded from the intranet.</i>		
Who Collects	Collection Frequency	How Measured
Security Awareness Officer	Monthly	# of Downloads per Resource
Why Collected This metric will be used to evaluate neutral reinforcement activities across the employee population.		

Gamification Traffic		
Description <i>The volume of user traffic to the intranet site hosting gamification activities</i>		
Who Collects	Collection Frequency	How Measured
Security Awareness Officer	Monthly	# of Unique Visitors per Day
Why Collected This metric will measure user interest in gamification activities which is a prerequisite for user participation		



Appendix

Learning Objectives

To ensure specific and measurable outcomes from security awareness activities, learning objectives are developed to ensure high risk topics are address and lead to user behavior changes.

Email Security		
Target Audience All employees, vendors, and contractors who require provisioning of a user account in our system.	Learning Objective 1 System users describe the different types of phishing attacks employed	<i>Individual Metric</i> System users correctly match the 5 most common types of phishing attacks with their definitions
Background Email is a critical communications medium for all network users and the primary attack vector threat actors use against SMBs.		<i>Organizational Metric</i> N/A
Applicable Human Risk Humans over rely on visual cues when dealing with mundane or frequent tasks such as reading and responding to emails.	Learning Objective 2 System users identify common methods attackers employ to execute phishing attacks	<i>Individual Metric</i> System users identify malicious or suspicious indicators within 9 out of 10 emails
Goal All system users will be familiar with the terminology and methodology used in the common malicious and spoofed email message.		<i>Organizational Metric</i> Less than 10% of users fall victim to quarterly red team phishing exercises.
Intended Outcome Reduce the number of users falling victim to phishing attacks and increase the number of user who report suspicious email messages.	Learning Objective 3 System users list the reporting steps to take when a phishing attack has been identified	<i>Individual Metric</i> System users can correctly recall the proper location to forward malicious emails.
		<i>Organizational Metric</i> The number of users who report red team phishing exercises is greater than or equal to 25%

