TABLE OF CONTENTS

[README 2](#_Toc32609709)

[CHARTER 3](#_Toc32609710)

[ADVISORY BOARD MATRIX 5](#_Toc32609711)

[PROJECT PLAN 6](#_Toc32609712)

[1.0 Executive Summary 7](#_Toc32609713)

[2.0 Target Audience (WHO) 9](#_Toc32609714)

[3.0 Risks (WHAT) 11](#_Toc32609715)

[3.1 Purpose 11](#_Toc32609716)

[3.2 Process 11](#_Toc32609717)

[3.3 Top Risks (and scores) 12](#_Toc32609718)

[3.4 Selected Topics 13](#_Toc32609719)

[4.0 Engagement Strategies (HOW) 14](#_Toc32609720)

[4.1 Overall Strategy 14](#_Toc32609721)

[4.2 Organizational Culture 14](#_Toc32609722)

[4.3 Branding and Imagery 15](#_Toc32609723)

[4.4 Localization 15](#_Toc32609724)

[4.5 Training Methods 15](#_Toc32609725)

[4.6 Reinforcement Training 16](#_Toc32609726)

[5.0 Metrics 18](#_Toc32609727)

[LEARNING OBJECTIVES 19](#_Toc32609728)

[RACI MATRIX 21](#_Toc32609729)

[Security Awareness Program Enhancements - Project Status Report 22](file:///C:\Users\riggy1999\Desktop\SANS%20MSISE%20program\ISE%205300%20Paper%20-%20Stephen%20Brown%20(final%20draft).docx#_Toc32609730)

# README

The focus of my Security Awareness Program is a US-based commercial insurance carrier with approximately 400 employees and 50 full-time IT contractors. More than 90% of the employees work out of the company’s home office in Chicago, Illinois. The remaining employees work in branch offices in ten other major US cities. Only five of the IT contractors work remotely. The remainder work at the Chicago office.

This company profile resembles my current employer. To protect its sensitive information, I’ve modified the company’s attributes and replaced people’s names with those of famous astronauts and other people. In this paper, I’ll refer to my company as US Insurance.

Of the 400 employees, roughly 100 have worked at US Insurance for more than 15 years, 100 for between 5 and 15 years, and the remaining 200 employees have started within the past five years. Within the most recently hired group, there’s an even mix of people who’ve had previous work experience in insurance and those who are new to the industry.

US Insurance currently has a Security Awareness Program focused on compliance requirements such as the cybersecurity regulations published by the New York Department of Financial Services. KnowBe4 software is the delivery method for the annual security awareness and phishing training provided to every employee and contractor. No other formal security awareness training exists.

The primary goal of this proposed project is to increase the workforce’s overall interest in security. Without significant security incidents to justify spending more time and money, the project will focus on motivating people to seek out additional security training opportunities on their own. Loosely explained from an economics perspective, we will concentrate on growing the demand for security training rather than merely increasing supply.

I chose US Insurance because the Information Security group has discussed enhancing the Security Awareness Program for the past three years, but has not found the time to do so. They’ve realized emphasis placed on technical security controls has far exceeded attention to workforce education, even though readily-available information highlights the risk posed by social engineering and other human-centric threat vectors. In my actual role at US Insurance, I will be able to pitch these Security Awareness Program enhancements directly to the CISO.

For extra credit, at the end of this file, I’ve included two exhibits. The RACI matrix summarizes the roles and responsibilities of the people listed in the project artifacts. The status report is an at-a-glance view of the significant aspects of the project and can work for multiple audiences, from executives to team members. It will be essential to manage the expectations of the project’s stakeholders.

# CHARTER

|  |  |
| --- | --- |
| **Security Awareness Program Enhancements – Project Charter** | |
| **Project Title:** | Security Awareness Program Enhancements |
| **Owner:** | The Chief Information Security Officer (CISO) is the project sponsor. The Deputy CISO is responsible for building, maintaining, and measuring the Security Awareness Program. The Deputy CISO reports directly to the CISO. |
| **Estimated Costs:** | Per company protocol, personnel costs for this project are employee FTE (full-time equivalent) units and hours. These hours are in the People Requirements section below. No other new spend exists. |
| **People Requirements:** | * The Deputy CISO and CISO will partner to administer the Security Awareness Program as additional duties (requiring 0.25 FTE from each individual). They will reevaluate additional staffing for the next company budget cycle. * The Corporate Communications Manager will be assigned at 0.25 FTE to aid with the design and marketing of training material. The Communications Department’s resource plan already includes an allocation for “Enterprise Project Support.” * An estimated 720 hours of user time (employees + contractors collectively) are needed to complete the proposed training program. * Reinforcement training will require 2-4 additional hours per person annually. * The Advisory Board will meet for 60 minutes monthly. |
| **Project Start Date:** | February 22, 2020 |
| **Project End Date:** | October 15, 2020 |
| **Scope:** | All company employees and contractors with access to the company network. |
| **Description:** | This project’s focus is to enhance the existing Security Awareness Program, which is currently at the “Compliance” level of the Security Awareness Maturity Model. At this level, specific compliance and audit requirements drive training. Employees, as a result, exhibit limited engagement. At the next level of maturity, “Promoting Awareness and Behavior Change,” training aligns with the company mission, promotes employee engagement, and provides continual reinforcement throughout the year. Company personnel are more aware of security policies and actively recognize, prevent, and report incidents, leading to an overall reduction of risk to the company. |
| **Goals:** | The Security Awareness Program enhancements proposed in this project focus on increasing workforce engagement, inspiring people to improve their security-related behaviors, and encouraging people to actively seeking additional security training. In doing so, the Security Awareness Program will transition from a compliance focus to also promoting security awareness and behavior change. |
| **Objectives:** | 1. Ensure employees and contractors understand where to locate security policies, procedures, and standards. |
| 2. Identify three top human risks to the company and manage these risks by changing employee and contractor behavior. |
| 3. Identify three groups to receive audience-specific training. |
| 4. Improve data security by providing data classification training and ways to avoid common causes of data loss. |
| 5. Ensure employees and contractors understand the risks and mitigations associated with Social Engineering. |
| 6. Ensure employees and contractors understand the risks and mitigation associated with Social Networking. |
| 7. Implement a metrics program to track and report on the impact of the Security Awareness Program. |
| 8. Build and maintain leadership support for any follow-on projects to further enhance the Security Awareness Program. |
| 9. Create a security-aware culture where people actively seek to improve their security knowledge and behavior. |
| **Justification:** | Corresponding with US Insurance’s recent company growth, measurable cyber risk is also increasing at US Insurance. In the past two years, the number of network intrusion attempts has risen by 35%. Phishing attempts have increased at an even higher rate of 50%. While our security solutions have detected and prevented these potential attacks, sooner or later, without significantly enhancing our approach, an attacker will be successful.  To combat the attacks, we need more than just technology. Humans, not technology, are typically the weakest link in security. Whether from active attacks (e.g., phishing and social engineering) or inadvertently sharing sensitive information with an unauthorized party, deficient security behaviors are leading causes of cyber loss. To promote positive security behaviors and thereby reduce the risk for US Insurance, we propose enhancing US Insurance’s Security Awareness Program. |
| **Milestones:** | Select and build Security Awareness Advisory Board. |
| Meet with the Corporate Communications Manager to identify program branding. |
| Complete any updates to the Security Awareness Plan. |
| Gain approval of plan/budget by senior leadership. |
| Conduct training kickoff meetings. |
| Conduct security assessments to measure the awareness level(s) of the training groups. |
| Create and execute three-month training cycles for each of the training groups. |
| Provide training results to the Advisory Board, senior leadership, and the training groups. |
| Communicate expectations and timing for Reinforcement Training. |
| Decide whether to propose a follow-on project. |
| **Assumptions and Constraints:** | **Assumptions:** |
| The project will have support from the Communications Department. |
| The work proposed in this project creates meaningful benefits for the company. However, follow-on work will be needed to extend the benefits across the workforce. |
| **Constraints:** |
| Employees and contractors have limited time available for training. |
| The CISO and Deputy CISO will staff this project above and beyond their regular responsibilities. Long-term program support may require a dedicated resource or to transition a portion of their current workload. |
| **Critical Success Factors:** | Support from senior leadership. |
| The project requires at least 0.25 FTE support from the Communications Department for branding and overall messaging. |
| Support from the department heads of the trainees |
| **Go/No-Go** | **Approved/Rejected** |
| **Comments:** |  |

|  |
| --- |
| ADVISORY BOARD MATRIX |
| As an enterprise effort, the Security Awareness Program needs input from a representative cross-section of the company to generate acceptance and enthusiasm. The Security Awareness Advisory Board, consisting of volunteers and led by the CISO and Deputy CISO, assists with identifying trainees and material while championing security across the company. Each Advisory Board member has pledged to advocate for security awareness actively. |
| |  |  |  | | --- | --- | --- | | **Name** | **Role / Department** | **Reason for Being on Advisory Board** | | **Alan Shepard** | **Corporate Communications Manager / Communications** | Assists with branding, development of visual aids, and communicating program themes. | | **John Glenn** | **Director of Learning and Development / HR** | Consults on training themes to ensure alignment with corporate culture and standards. | | **Neil Armstrong** | **Assistant Department Head / Claims** | Fraud detection and prevention is a high priority in the Claims department, and Neil has already approached the Information Security group for additional training. Neil is outgoing and has indicated he will promote customized security training throughout his department. | | **Sally Ride** | **Technical Writer / IT** | Sally has a long tenure at the company and has written procedures and training manuals for many of the departments. Her work is known for its quality and usability. She understands how to write in a manner received well by the company’s workforce. Leveraging this knowledge for the Security Awareness Program will increase the likelihood of communicating successfully. | | **Roberta Bondar** | **Vice President of IT Compliance and Risk Management / IT** | Roberta educates IT and business personnel on good email practices as the administrator of the Phishing Awareness Program. She has developed points of contact throughout the company that we can leverage for communicating additional security awareness topics. | | **Buzz Aldrin** | **Vice President / Sales** | Buzz routinely fields questions from commercial clients regarding the company’s internal security practices. He will provide insight into the unique needs of customer-facing personnel. | | **Mae Jemison** | **Staff Counsel / Legal** | Legal will review training included in the Security Awareness Program to ensure it meets any requirements contained in applicable laws and regulations. | | **Ellen Baker** | **Information Security Manager / IT** | Ellen is responsible for technical operations within the Security Group. She is the primary liaison to the IT Developer and infrastructure teams. Her knowledge of the personalities within those groups will greatly help when crafting specialized training. Viewed as a technical expert, she helps generate buy-in for the program from the technical personnel. | | **Kathryn Sullivan** | **President / Executive** | Sponsor of the Security Awareness Program. Kathryn has long been a vocal advocate for enhancing security capabilities at the company. Having an executive presence on the Advisory Board will directly reinforce the importance of the program with members. | | **Eileen Collins** | **Chief Risk Officer / Enterprise Risk Management** | Eileen works closely with the Information Security group to assess company risk. Her most recent annual risk assessment is the basis for the first three training groups. | | |

# PROJECT PLAN

**SECURITY AWARENESS PROGRAM ENHANCEMENTS**

***US Insurance***

***\*****although information included in this plan loosely resembles that of a real company, individual names and specific company details were changed – this is for the academic exercise specified in SANS ISE 5300.*

## Executive Summary

US Insurance provides commercial insurance products to many Fortune 500 companies and other comparably large clients in the public sector. Cyber insurance is one of the new and strategically essential product offerings provided by US Insurance. As an insurance carrier, US Insurance stores considerable amounts of sensitive data, from its clients’ financial and accident history to detailed personal information of claimants, such as social security numbers and medical records. US Insurance’s executive management has prioritized avoiding data loss (e.g., data breaches) as critically important for the growth of the cyber insurance product and the company in general. They’ve determined it would be challenging to market cyber insurance if US Insurance itself has to disclose significant security incidents. Overall, the company’s risk tolerance for security incidents has decreased significantly over the past two years.

On the surface, the current state of security is quite good. The cybersecurity program follows industry-standard frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) Controls. The security approach is defense-in-depth and includes best-of-breed anti-malware, data loss prevention, network segmentation, encryption, identity and access management, and multi-factor authentication solutions, to name just a few. Third-party auditing firms perform annual penetration tests with minor or no findings. No reportable security incidents have occurred in the past five years.

From a business perspective, US Insurance is in a period of significant transition. In the past five years, US Insurance has added 50% to its workforce. The company’s five-year plan calls for continued growth at a rate of 40 new employees per year going forward. To address the rapid growth of personnel, the company has committed to significantly increasing its IT capabilities, including: (1) in-progress projects to replace two of its core enterprise software platforms with cloud-based solutions; (2) the recent purchase of several new cloud-based software solutions to service new business units; (3) a plan to double the size of the internal IT Developer teams from 40 to 80 contractors over the next two years; and (4) a project starting later this year to provide clients with access to insurance policies and claims records directly through an online portal.

The company’s transition brings with it multiple challenges, along with numerous benefits. First, by significantly increasing the workforce, many new people are added with uncertain security knowledge. Whereas longer-tenured employees have received security awareness training from US Insurance and their understanding is relatively clear, we are unsure of the level of security training previously received by the new personnel. Second, as part of the company’s growth strategy, it’s targeting increasing the use of digital communications to reach its clients. In doing so, risks from social media, mobile apps, and other modern communications channels have increased. Despite the increased risk, security awareness and phishing training are still delivered to company personnel using a “one size fits all” approach with no customization based on job role or risk to the company. Lastly, technical security knowledge exists primarily in the Information Security group. Scaling security to implement the previously-listed new capabilities will require knowledge transfer to the IT Developer group.

Measurable cyber risk is already increasing at US Insurance. In the past two years, the number of network intrusion attempts has risen by 35%. Phishing attempts have increased at an even higher rate of 50%. Although our security solutions have detected and prevented these potential attacks thus far, without significantly enhancing our approach, an attacker will likely be successful.

Whether from attackers actively targeting someone through social engineering or an employee’s unintentional negligent behavior, many instances of cyber loss are attributable to someone failing to follow an organizational security policy or cybersecurity best practice. Rather than waiting for such an attack to be successful at US Insurance, this plan offers a proactive approach, in the form of enhancements to the company’s existing Security Awareness Program, for continuing to provide the level of security the company expects.

A Security Awareness Program is a formal program to train a company’s workforce on threats to the company’s assets and how to avoid putting those assets at risk. The program focuses on human behavior rather than technical controls. In information security, people are typically the weakest link.

In concert with continuing to invest in technical solutions, this plan proposes expanding the company’s existing Security Awareness Program to (1) provide specialized training to staff based on their baseline security knowledge customized to their job role, (2) measure the training’s impact, and (3) consider the results for future training. The plan covered in this document focuses on the three highest risk groups identified in the recently completed risk assessment from the Enterprise Risk Management department: (1) IT Developers, (2) Claims department personnel; and (3) Sales department personnel As a part of this project, we may propose additional program enhancements in separate projects.

## Target Audience (WHO)

This Security Awareness Program plan provides a scalable framework for customized training. The program emphasizes inspiring trainees to improve their security-related behaviors and delivering the minimum training for the maximum benefit. Everyone should not receive the same training, as people have different awareness levels, needs based on their jobs, and learning styles.

Since everyone is already busy with their main jobs, and because the Security Awareness Program does not have unlimited funding, we will target specific groups to train at different times. For each group in this plan, we will analyze for learning style, interest areas, and risks to US Insurance. In doing so, people will be more receptive to training, retain more of the training material longer, and change security behaviors to most benefit US Insurance.

Initially, three groups will receive customized training: (1) IT Developers, (2) Claims department personnel; and (3) Sales department personnel. While other groups will eventually warrant customized training, these three groups pose the most significant risk to the company, as identified by the Enterprise Risk Management (ERM) department in their annual assessment of organizational risk.

Limiting this plan to three groups provides the opportunity to demonstrate the approach is practical and creates value before committing more company resources to enhance the program. Successful experiences with these groups will also generate word-of-mouth excitement throughout the company. After training these groups, the Advisory Board will help to identify which new groups would benefit from a similar approach.

IT Developers will receive the first training for the reasons listed below.

* The ERM department’s study identified this group as posing the most risk to US Insurance.
* As noted in the company’s five-year plan, IT Developer staffing and responsibility will significantly increase over the next two years.
* By the number of personnel, the IT Developer group is the largest in the company. Currently, it consists of 20 employees and 40 full-time contractors.
* Within two years, the group will increase in size to 30 employees and 80 full-time contractors.
* The IT Developer group is responsible for creating and maintaining secure software to support the company’s operations and process its sensitive data.

The Claims department, with their access to millions of claimants’ personal information, will receive training next. This priority is also consistent with the ERM study.

Of the Training Groups, the Sales department will receive training last. Although their use of IT while traveling presents unique considerations, per the ERM study of organization risk, the Sales department accounts for less risk to the company than either the developers or Claims personnel.

The following table contains details for the IT Developers group. These details are highlighted since IT Developers is the first and riskiest group. Details for the other two groups will be shared with the Advisory Board for their input before beginning training.

**Training Group 1 – IT Developers (60 people)**

|  |  |
| --- | --- |
| **IT DEVELOPERS** | |
| **Description** | IT Developers primarily create internally-created applications for internal company use. They are beginning to develop web applications offered for customer use. Additionally, they are responsible for managing a significant amount of third-party software, both internally-hosted and cloud-based. |
| **Group Size** | Currently, there are 40 full-time contractors and 20 full-time employees. Of the employees, three are managers, and two are architects. |
| **Profile** | Most developers have between three and ten years of experience, but roughly 25% have 20+ years of experience. More than 75% of the group has been with US Insurance for less than two years. Men outnumber women at roughly a 4:1 ratio. |
| **Unique Requirements** | IT Developers are the most critical group because of their involvement in building and maintaining the software used to process the company’s sensitive data and support its business operations.   1. This group responds well when a perceived technical expert delivers the training. 2. Most members of the group prefer online training over in-person training 3. Most members of the group are familiar with .NET programming languages, while 10 of the contractors and two of the employees specialize in Java. |
| **Remote Access** | Employees can connect to the corporate network via VPN on their company-managed laptop. Only contractors who regularly work remotely receive remote access privileges. They connect using Virtual Desktop Infrastructure (VDI) rather than VPN. |
| **Travel Frequency** | Most employees travel once annually to training or seminars that last no more than one week. One of the development managers travels 3-4 times a year to branch office locations. |
| **Access to Sensitive Information** | This group only receives access to the Development and Test environments. They have no access to the Production environment. IT obfuscates sensitive Personal Information such as names and social security numbers and Personal Health Information in all non-Production systems. |
| **Level of IS Access** | Per company policy, IT Developers cannot receive privileged access. Both employees and contractors receive company-managed laptops. IT strictly enforces Separation of Duties. External Audit verifies this annually. |

## Risks (WHAT)

### Purpose

Not only are there limits on the Security Awareness Program in terms of time and money, but the workforce receiving training also has very little time to spend on activities outside their jobs. Therefore, to create the most value to US Insurance and the highest likelihood of future interest in training, it’s imperative to select the most important topics and deliver the training most engagingly. Accordingly, the risk-based approach outlined below describes the training subjects that produce the highest return. Training priority results from analyzing the probability and impact of security incidents. The largest risks are the subjects of this plan, whereas lower risks may be in future training.

### Process

Risk prioritization followed a qualitative method. Leveraging existing organizational infrastructure, the Tactical Operations Group (TOG) assessed each of the human risk categories listed below to determine an overall risk score. The TOG was the appropriate group to assess risks because it consists of 25 mid and senior-level managers representing each of the company’s 16 departments, and it already receives a bi-annual security briefing. Overall, this group was a great choice based on its collective expertise and familiarity with security. Each member of the TOG received a questionnaire asking them to score ten categories of human risk based on probability and impact (*see the table below)*. Participants also had the opportunity to write in custom responses for future consideration.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Targeted Attacks | Email and Messaging | Internet Browsing | Social Networking | Mobile Devices |
| Social Engineering | Passwords | Data Security | Cloud | Hacking |

***Scoring followed these standard criteria:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Probability**  (of an event occurring in the next 12 months) | |  | **Impact**  (in terms of human, financial, or reputational harm to the company) | |
| **Very High (5)** | 95% or greater chance of happening in the next six months. |  | **Very High (5)** | 1. Loss of life or permanent loss from work. 2. Financial loss of $10 million or more. 3. Executive leadership must report to congress for public hearings. 4. Permanent negative reputational damage. 5. Shutdown of operations for more than five days. |
| **High (4)** | 80–95% chance of happening in the next six months. |  | **High (4)** | 1. Critical employee injury, one month or more loss from work. 2. Financial loss of $1 million – $10 million. 3. Leadership directly involved in legal proceedings. 4. Long-term negative reputational impact and public exposure. 5. Shutdown of operations for 1–5 days. |
| **Medium (3)** | 20–80% chance of happening in the next six months. |  | **Medium (3)** | 1. Severe employee injury, one week to one month time lost from work. 2. Financial loss of $100,000 – $1 million 3. Leadership directly involved in legal proceedings. 4. Serious negative reputational impact and public exposure. 5. Shutdown of operations for one day. |
| **Low (2)** | 5–20% chance of happening in the next six months. |  | **Low (2)** | 1. Employee injury, one week or less time lost from work. 2. Financial loss of $10,000 – $100,000. 3. Management supporting some legal proceedings. 4. Some negative reputational impact and public exposure. 5. Shutdown of operations for less than 24 hours. |
| **Very Low (1)** | 5% or less chance of happening in the next six months. |  | **Very Low (1)** | 1. Minor employee injury, no time lost from work. 2. Financial loss of $10,000 or less 3. Minimal to no legal involvement. 4. Minimal to no negative reputational impact and public exposure. 5. Shutdown of operations for less than an hour. |

### Top Risks (and scores)

The following table summarizes the aggregate average probability, impact, and risk score results from the 25 TOG members. After totaling the scores, we worked with the TOG to match training groups with applicable risks. Those results are included in the table as well.

|  |  |
| --- | --- |
| **Risk Score** | **Overall Risk** |
| >20.0 | **Very High** |
| 15.1-20.0 | **High** |
| 10.0 -15.0 | **Medium** |
| <10.0 | **Low** |
| **Risk** | **Description** | | **Target Group(s) Applicable to** | **Probability** | **Impact** | **Risk Score** | **Overall Risk** |
| **Data Security** | The treatment of sensitive information including (1) data classification, (2) restrictions on transfer or sharing, and (3) secure disposal. | | IT Developers;  Claims Dept.;  Sales Dept. | **4.3** | **4.8** | **20.6** | **Very High** |
| **Social Engineering** | Social engineering involves an attacker directly targeting another human. Technical measures to prevent such attacks are less effective than education and training. | | IT Developers;  Claims Dept.;  Sales Dept. | **4.1** | **3.9** | **16.0** | **High** |
| **Social Networking** | The use of social media for business and personal use and how that impacts risk to the company. | | IT Developers;  Claims Dept.;  Sales Dept. | **4.5** | **3.4** | **15.3** | **High** |
| **Email and Messaging** | Email is one of the primary means used for social engineering attacks. Email is also the most common channel used to communicate, in general, and share sensitive information. | | IT Developers;  Claims Dept.;  Sales Dept. | **4.2** | **2.2** | **9.2** | **Low** |
| **Cloud** | The use of cloud software is increasing at the company. Although the IT department is aware of much of it, some software is outside of IT control (i.e., directly sourced by a business unit). This software processes sensitive company data. Not all security measures used on the company network are available for use with cloud software. | | IT Developers;  Claims Dept.;  Sales Dept. | **3.2** | **2.8** | **9.0** | **Low** |
| **Mobile Device Security** | Company employees use a mix of company-issued and personal devices (tablets and phones). They have much of the same functionality as traditional computers, including their access to sensitive data. Many unique security considerations also exist. | | Claims Dept.;  Sales Dept. | **2.5** | **1.5** | **3.8** | **Low** |

*Important Notes:*

1. *TOG members received instructions to consider any mitigating factors they were aware of, including both process and technical controls. To reduce the potential for bias concerning mitigated risk, the Security group avoided any additional description of technical controls in place. E.g., the risks above reflect the perspective of the TOG members, without undue influence from Security.*
2. *Different audiences may receive different training for the same risk topic. Different training may exist for each group based on their collective characteristics to maximize benefit (individual engagement and value to the company). E.g., the IT Developers will receive more technical training about Data Security than will the Sales department. Also, people with high scores on their security assessment will get more advanced training on a topic than the lower-scoring cohort from the same Training Group.*
3. *Refer to both the Training Methods subsection in Section 4 and the Learning Objectives in the plan’s appendix for additional information about each topic.*

### Selected Topics

This section provides additional detail for the three top risks identified in our risk assessment. They are the focus of the training covered in this plan. In Section 3.3., a short description of each risk is available. Below, we further explain why training should include each topic.

*DATA SECURITY*

**Risk Score:** Very High

**Selection Reason:** US Insurance processes the personal information of 10+ million people annually. Much of this information is highly sensitive, such as detailed medical information. Unauthorized disclosure of this information could severely damage the business. In addition to the monetary penalties accompanying various US state security and privacy laws, the damage to company reputation and brand could be enormous. Much of US Insurance’s business comes through national insurance brokers. Damage to those relationships, by, for example, a loss of trust from a data breach, would create a bottom-line financial impact felt across the company.

The culture at US Insurance is such that business users often receive more access than they minimally need. The company values the sharing of information more than restricting access on a need-to-know or least privilege basis. Many sensitive files also exist as images, precluding security systems such as DLP from adequately protecting the movement of data outside the company network. Given these considerations, the likelihood of a security incident is quite high, and the main reason that the TOG selected Data Security as the highest human risk.

*SOCIAL ENGINEERING*

**Risk Score:** High

**Selection Reason:** Social engineering is a non-technical attack that relies on tricking an individual. Technical security controls cannot prevent these attacks. Examples include phishing, spear phishing, and tailgating. According to the 2019 Verizon Data Breach Investigations Report, the leading review of information security incidents, one-third of all attacks are social engineering. They are, in fact, the second leading attack method. Only hacking is more prevalent. Educating people to spot possible attacks and training them how to respond is the primary method for mitigating social engineering risk

*SOCIAL NETWORKING*

**Risk Score:** High

**Selection Reason:** The company relies on social networking (e.g., LinkedIn, Facebook, Twitter) to reach its customers. The company’s workforce also routinely uses social media in their personal lives. Frequent social networking is the norm in 2020, and although social networking has many benefits, the risks to the company are numerous. Some include:

* It’s easy for an employee to share sensitive information about the company through social media. An attacker may use even seemingly mundane information about an individual or their employer (or former employer) for hacking or social engineering.
* Social networking sites are well-known gateways for malware.
* Attackers often use social networking sites for phishing.

## Engagement Strategies (HOW)

An insurance company that does not protect its clients’ sensitive information will lose its clients’ trust. Accordingly, all of US Insurance’s workforce needs to understand the criticality of protecting data. The existing security awareness education communicates some of this message to the company. However, to effectively guard against the risks described in the previous section, the company needs more training. The strategy outlined in this section provides a path to increase security knowledge and enthusiasm through audience-specific training.

### Overall Strategy

The Security Awareness Program’s mission is to create a secure-aware organization that incorporates its knowledge of what to do into its collective behavior. The workforce must want to practice better security awareness to accomplish the mission. As a priority, people must understand why practicing security awareness is essential. Understanding will result from a combination of explaining why security awareness benefits the individual, as well as why it helps the company. After explaining why, there will be follow-up with relevant and engaging training on an ongoing basis, ensuring it adapts as risks evolve and the workforce changes. Metrics will demonstrate program effectiveness and support future decisions. The sections below outline the approach in detail.

### Organizational Culture

Executive management and senior leadership establish the culture at US Insurance. They are long-tenured, with many working at the company for multiple decades. Generally speaking, US Insurance’s culture is relatively conservative. Work-life balance is both advocated and practiced. Management encourages change, and it typically occurs in a measured and controlled manner. When significant change does occur, it’s usually implemented by a cross-functional committee rather than by a decree from management. Various subcultures also exist, which is evident in the training groups.

**IT DEVELOPERS**

The defining characteristic of this group is its newness to US Insurance. With approximately three out of every four developers hired within the past two years, they’ve begun to establish a subculture within US Insurance. This group consists of a mix of contractors and employees. Focused on their “technology” more so than broader business goals, this group values opportunities for skill development above all else. Consistent with one of the common stereotypes for coders, the group seems composed mainly of introverts. They likely prefer online training, but accept in-person training when delivered by a person perceived to have strong technical knowledge.

**CLAIMS DEPARTMENT**

Members of this group are exclusively employees. More than half have been with the company for greater than ten years. There’s a 50/50 mix of women to men. Of the newer employees (hired within the past five years), 75% of them have worked in claims jobs at other companies. Overall, this group is practical and content with the status quo. They are unlikely to seek out opportunities that don’t precisely align with their job or designated career path.

**SALES DEPARTMENT**

This group is the most outgoing of the three analyzed in this section. They receive a large amount of their overall annual compensation through commissions. If something helps them generate new business or retain current accounts, they’re highly interested. If no direct link exists, they’re typically uninterested. This group strongly prefers in-person communication but will accept other methods with a clearly defined “why” shared in advance.

### Branding and Imagery

Although US Insurance has a robust corporate brand, we will create separate branding to emphasize the importance of the Security Awareness Program. To date, Security has used the corporate logo and communication standards. As a part of this plan, the Communications Department will assist with developing a specific logo and advertising material geared toward generating interest.

### Localization

English is the native language for all people identified for training in this plan.

### Training Methods

For the Security Awareness Program to consistently deliver value to the business, its training framework will consist of the following features:

* **Baseline:** One ofthe reasons past attempts to add awareness training failed was the perception that training was not particularly relevant to people’s day-to-day jobs. Overcoming this perception is a critical success factor for this program. To deliver the most relevant and interesting material, each member of the training groups will complete a 10-15 minute online security assessment, delivered using the KnowBe4 security training application. (US Insurance already has a subscription to this product.) It’s critical to not only match up people with the most relevant topics but also to provide them the correct level of training. For example, an IT architect responsible for the design of externally facing web applications will certainly benefit from training in the general topic area of passwords. However, training will focus more on secure coding practices rather than basic concepts more appropriate for a non-technical user. Following this reasoning, the assessment will consist of 23 multiple-choice questions that produce an overall security awareness score. Assessment takers will fall into one of three groups based on the number of questions answered correctly:
  + Greater than 80% = HIGHLY AWARE
  + 60% to 80% = MODERATELY AWARE
  + Less than 60% = MINIMALLY AWARE

Scores will serve the purpose of matching people to the appropriate training levels and setting an aggregate baseline score for each training group. Individual scores will be kept confidential, with neither the assessment taker nor their management receiving the results.

The Deputy CISO and CISO will host a kickoff meeting with each training group before launching the assessment to reinforce its purpose and that of the overall program, as well as field any initial questions from the group. For the program to reach its goals, it’s critically important to minimize the perception that the assessment is to justify something negative such as a bad review. (We’re aiming to win hearts and minds, not merely publish information!)

* **Training:**

Each target group will receive one hour’s worth of training each month for three months. Training Group 2 will start one month after Training Group 1, and Training Group 3 will begin one month after Training Group 2. Staggering will allow time to tune the initial training based on early feedback, as well as allow time to build word-of-mouth anticipation in later groups.

The three-month training cycle will employ three separate modalities to increase the likelihood of finding a learning style appropriate for everyone and collect a varied amount of data for use in tuning the program.

Month 1 training will be the most personal, with the Deputy CISO presenting it in a group setting. With assistance in creating it provided by the Director of Learning and Development, the presentation will include:

* + Program goals, including increasing interest in security and reinforcing that the Information Security group is happy to assist with questions, suggestions, and ad hoc training requests. (They are friendly and want to help!)
  + Modules customized to the topic area identified for the training group as well as the level of the subgroup established from the security assessment. *E.g., the IT Developers will receive training on Data Security, but it may be split across two or more groups, based on the security assessment results, and customized to each.*
  + Knowledge-based questions meant to generate audience participation.
  + The three-month plan for training.
  + Expectations for reinforcement training.

Month 2 training will consist of computer-based training (two 30-minute modules) delivered by the KnowBe4 software. The purpose of this training method is to convey content-rich knowledge but do so by flexibility offering when to complete it. The software provides interactive reinforcement questions as well as recording the time each individual spends training. The Deputy CISO will encourage by personally following up with individuals who don’t complete the training within the month.

Month 3 training is once again intentionally in a personal setting. This time, it will be a bit more informal, though, delivered during a lunch-and-learn. The focus of this session is to hear from the training participants and communicate to them what they should expect going forward. As for their feedback, the Deputy CISO will moderate the meeting and ask the audience what they liked, what they didn’t like, how their view of security has changed, and what it would take for them to continue learning about security (and ultimately increasing their practice of security-aware behaviors). The meeting format will resemble that of a Lessons Learned session. Importantly, the room should be set up with tables and chairs in a circle or square to promote discussion. The meeting should be interactive, not a presentation or a speech. Going forward, the training participants should expect reinforcement training as outlined below in that section. In the lunch-and-learn, the Deputy CISO will present a list of informational resources as well as specifically request people to reach out with questions and training requests going forward. Metrics will track those touchpoints to demonstrate whether engagement increases.

* **Post-Training Assessment and Tuning:**

After completing the Month 3 training, each participant will receive the security assessment of the same style as completed before training. The assessment will take 10-15 minutes, and only the Training Group’s aggregate results will be published. A goal of the program is to see improvement reflected in these results. Regardless, they will be available to the company, and future training will review them when analyzing opportunities for program growth.

### Reinforcement Training

The training plan outlined above is just the start of what is necessary to effect long-term security awareness change at US Insurance. Similar to a typical software development project, this plan constitutes the initial implementation. However, perpetual maintenance and upkeep are needed post-implementation. Some examples follow.

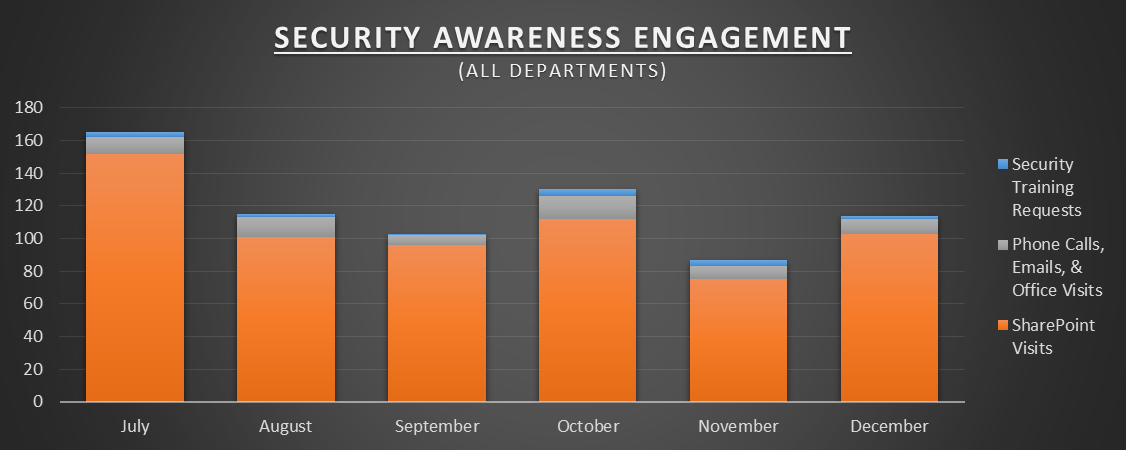
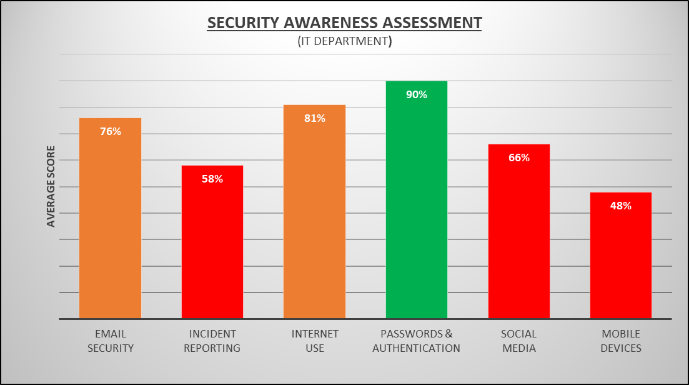
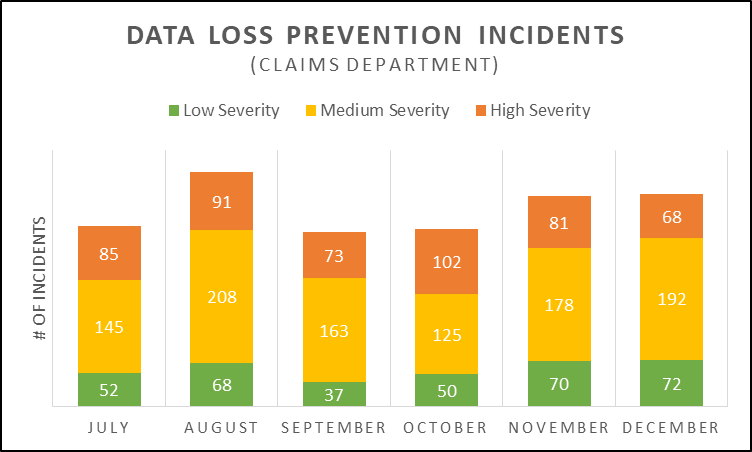
* The CISO will publish a **“Tip of the week”** to the company at-large. This information will be one or two sentences of non-technical “advice” meant to encourage everyone to think about security.
* The Security group will host **“Lunch-and-Learns”** about a specific security topicevery other month. Free food consistently draws an audience, so we’ll use that in exchange for 45 minutes of people’s discretionary time. Each session will include a maximum of 50 people to create artificial scarcity. Additional meetings may occur if sufficient demand exists.
* **Security Ambassadors** spread the “good word” of security at a grassroots level. Given that US Insurance has a relatively small workforce that’s centralized geographically, word-of-mouth publicity is powerful. Volunteer opportunities to join the Security Awareness Program as an ambassador will start as a part of the proposed project. The Ambassadors will meet quarterly to share information and discuss future security topics, and the Deputy CISO will coordinate and lead these meetings.
* The company already uses **Digital Signage** in its lobbies, hallways, and cafeteria. The Communications department will assist with distributing security awareness content monthly.
* Every six months, **Computer-Based Training** following the methodology established in the training section will be available to the company at-large. More training will be available on request. Each course completed will count for a specific amount of “points,” with gift cards awarded for individual and group achievement.

## Metrics

The goal of collecting metrics for the Security Awareness Program is to show tangible benefits to US Insurance. The three representative metrics outlined below will demonstrate the effectiveness of this plan in reducing the risks described in Section 3. Additional metrics may be created later in the project. Consistent with the overarching program goal to increase both awareness of and interest in security, these metrics will be available on the Information Security SharePoint site to promote the program.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Metric Name** | **Why is this Measured?**  (i.e., what Risk does this relate to?) | **What Is Measured?** | **How Is it Measured?** | **When is It Measured?** | **Who Measures?** |
| **Sensitive Data** | Data Security is the top human risk identified in Section 3. Success training should result in a decrease in the frequency of unauthorized attempts to transfer sensitive data from the company network. | The number of files blocked by security policies. | The Data Loss Prevention system (ForcePoint) already has reports built for this. | Continuously  (reported monthly from the DLP system) | Security Team |
| **Knowledge** | All three top risks (Data Security, Social Engineering, and Social Networking) should decrease if the company workforce has a better understanding of what is appropriate behavior. | Individual security assessment scores compared before and after training. | Awareness Assessment  (using KnowBe4 software) | Before Training (to establish a baseline);  Immediately after training;  Yearly after that | Security Team |
| **Engagement** | This metric also applies to all three top risks. Because value from security awareness training comes from people changing their behavior, a program focus is increasing security interest. We’re also expecting a higher number of requests to the Security team to answer questions and provide additional training. Minimally, people should more frequently refer to existing security documentation. | Are people actively seeking out instructions for how to behave securely? | Visits to the SharePoint site housing Information Security policies, procedures, and standards.  The Information Security group will track the number of ad hoc inquiries it receives and logs each touchpoint in ServiceNow’s service management application. | Continuously  (reported monthly from SharePoint and ServiceNow’s  service management application) | Security Team |

The following are examples of the metrics listed above. After project approval, these metrics may change.



# LEARNING OBJECTIVES

The purpose of this document is to identify and explain the learning objectives of this training module.

Risk

Data Security (*see Section 3)*

Training Title

Data Security for IT Developers

Target Audience

The target audience is the IT Developers group at US Insurance. Given that this group consists of technical users, the specific learning objectives for their training will differ from the Data Security training offered to business users.

Goal

Training participants will learn which data is most important to the company and be able to demonstrate the most common risks to that data as well as where to locate additional relevant documentation. As IT Developers both handle sensitive data directly and manage the systems that process the data, increasing their security awareness will lower organizational risk.

Background

US Insurance develops a significant amount of custom software. Their IT Developer group is also responsible for managing an extensive suite of third-party software. Collectively, the software processes a large amount of highly sensitive information about US Insurance clients’ employees and claimants under their insurance policies. This information includes regulatory information such as social security information and other Personally Identifiable Information (PII), as well as personal health information (PHI).

Applicable Human Risk

**Data Security** is the focus of the learning objectives listed below. It is the highest-rated risk identified in Section 3 of the project plan.

Learning Objectives

1. Learners can explain what data types are most sensitive to the company.
   1. *Individual Metric: Learner correctly identifies or matches Highly-Sensitive and Confidential data classification labels to real examples of the company’s data in a test question or interactive training session. This measurement is conducted by the Security group before and immediately after training. Follow-up testing occurs every six months.*
   2. *Organizational Metric: A sampling of files with data classification labels (under the company’s Data Classification Policy) added or modified during the measured period has the correct sensitivity assigned. The Security group conducts these measurements monthly.*
2. Learners can identify the most common ways unauthorized data exfiltration could occur at the company.
   1. *Individual Metric: Learner correctly identifies or matches the exfiltration technique to data type in a test question or interactive training session. This measurement is conducted by the Security group before and immediately after training. Follow-up testing occurs every six months.*
   2. *Organizational Metric: Data Loss Prevention (DLP) records are measured by the Security group to compare exfiltration attempts (unintentional and intentional) by the Training Group. The Security group measures this continuously and reports monthly.*
3. Learners know where to access Information Security Policies, Procedures, and Standards, and they routinely access them.
   1. *Individual Metric: Learner correctly identifies from a list of choices the applicable policy(s), procedure(s), or standard(s) for a given scenario in a test question or interactive training session. The Security group conducts this measurement before and immediately after training. Follow-up testing occurs every six months.*
   2. *Organizational Metric: Pageviews and successful file access attempts by the Training Group are measured. All security documentation exists on SharePoint, and the Security group will measure usage monthly.*

# RACI MATRIX



# Security Awareness Program Enhancements - Project Status Report

**Estimated Costs**

**Employee (Hours)**

|  |  |  |
| --- | --- | --- |
| **Planned** | **Current** | **Remaining** |
| 1345 |  |  |

**Other ($)**

|  |  |  |
| --- | --- | --- |
| **Planned** | **Current** | **Remaining** |
| $0 |  |  |

**Key Stakeholders**

**Executive Sponsor:** Jane Adams

**Project Owner:**  Winston Churchill

**Project Lead(s):** Abraham Lincoln

**Business Lead(s) for Training:** George Washington, Thomas Jefferson, Martha Washington

**Goals**

* Move from “Compliance” phase of maturity to “Promoting Awareness and Behavior Change” phase

**Progress**

(as of 2/14/2020)

|  |  |  |
| --- | --- | --- |
| **ON-TRACK** | **LATE** | **COMPLETED** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Milestone** | **Start**  **Planned/Revised** | **Finish**  **Planned/Revised** | **Status** | **Risk(s)** |
| **Select Advisory Board** | *18-FEB* | *28-FEB* | ON-TRACK |  |
| **Program Branding** | *2-MAR* | *13-MAR* | ON-TRACK |  |
| **Security Awareness Plan Updates** | *9-MAR* | *20-MAR* | ON-TRACK |  |
| **Senior leadership approval** | *23-MAR* | *27-MAR* | ON-TRACK |  |
| **Training kickoff meeting** | *7-APR* |  | ON-TRACK |  |
| **Baseline security testing** | *14-APR* | *28-APR* | ON-TRACK |  |
| **Training cycle 1** | *4-MAY* | *4-AUG* | ON-TRACK |  |
| **Training cycle 2** | *8-JUN* | *8-SEP* | ON-TRACK |  |
| **Training cycle 3** | *6-JUL* | *6-OCT* | ON-TRACK |  |
| **Launch reinforcement training** | *10-AUG* | *10-OCT* | ON-TRACK |  |
| **Propose additional project (if justified)** | *17-OCT* |  | ON-TRACK |  |

**Critical Success Factors**

* Support from senior leadership, department heads, and Communications department

**Assumptions**

* Communications Department support
* Follow-on work is expected

**Constraints**

* Limited time for training
* No dedicated Security Awareness resources

**Justification**

* Increase in measurable cyber risk
* Support of company growth