**Embers Credit Union**

**Security Awareness Plan**

**For**

**ISE 5300: Managing Human Risk**

This document is not a complete security awareness plan document.

It only covers the sections required by the ISE 5300 course offered as part of the SANS Technology Institute’s Master of Science in Information Security Engineering as of August 2021.

|  |  |
| --- | --- |
| **Prepared By** | Justin Store |
| **Date Revised** | 08/07/2021 |
| **Version Number** | 1.0 |

Table of Contents

[Table of Contents 2](#_Toc79588832)

[README 3](#_Toc79588833)

[1.0 Executive Summary 4](#_Toc79588834)

[2.0 Engagement Strategy 5](#_Toc79588835)

[3.0 Organizational Culture 5](#_Toc79588836)

[4.0 Branding 6](#_Toc79588837)

[5.0 Training Methods and Modalities 6](#_Toc79588838)

[5.1 In-Person New Hire Onboarding Training 7](#_Toc79588839)

[5.2 In-Person New Hire Follow-Up Training 7](#_Toc79588840)

[5.3 Monthly Phishing Training 8](#_Toc79588841)

[5.4 Monthly Security Newsletters 8](#_Toc79588842)

[5.5 Annual Computer Based Compliance Training 9](#_Toc79588843)

[5.6 Biannual All Staff In-Service Training 9](#_Toc79588844)

[6.0 Metrics 10](#_Toc79588845)

[6.1 Identity Verification 10](#_Toc79588846)

[6.2 Mishandling of Sensitive Information 11](#_Toc79588847)

[6.3 Phishing Email 11](#_Toc79588848)

[7.0 Appendix A: Learning Objectives 13](#_Toc79588849)

[7.1 Handling Sensitive Information 13](#_Toc79588850)

# README

I chose to develop a new security awareness plan for my current employer, Embers Credit Union. Embers is a small financial services organization with 130 employees that exclusively serves Michigan’s Upper Peninsula (the UP). The UP is a rural area with its own unique culture with a strong sense of community and affinity for the outdoors and rural life. Embers was originally the UP Catholic Credit Union until it was rebranded a few years ago to emphasize that our membership base includes more than the local Catholic community, even though that is still a key demographic of our membership. Since the rebranding, Embers has taken an opportunistic approach to growth by merging with two other credit unions and opening additional locations. This growth has resulted in Embers nearly tripling in size via all metrics (assets, location, and employees) in the last four years. To help manage this growth, Embers is actively redesigning many of its programs and processes to make them more scalable.

The section on engagement strategies is longer than the 2-3 pages recommended due to the inclusion of six different training types. Some of these could be removed to better align with the instructions of the assignment, but were left in place as they are intended to be used in real life and help create a more comprehensive plan.

# Executive Summary

Embers Credit Union is uniquely situated as a trusted financial partner for our 30,000+ members in the central Upper Peninsula. As a trusted financial partner, our members depend on us for financial security now and into the future. We provide that security through our full suite of deposit, investment, and credit services, each of which is tailored towards the needs of our members and our community. We excel at providing the services our members need, both at our traditional brick-and-mortar branches and with our modern and constantly evolving online banking services.

Maintaining these services directly depends on our ability to secure the information systems that support our mission. Any disruption to these systems would directly impact our members’ ability to leverage our services and could lead to a degradation of the trust we’ve worked so hard to gain. To that end, we are constantly evolving our use of security technology and employ highly trained security professionals dedicated to fine-tuning and improving our security program to adapt to the latest threats and attacks.

However, even with the right technology and security personnel working around the clock, there are still a wide range of risks that can’t be addressed by technology and security experts alone. This risk, known as human risk, exploits human nature itself by targeting and manipulating our employees. Human risk continues to be one of the fastest-growing risks to our organization as attackers continue to exploit it at an increasing rate, making it a critical component of fraud and network intrusions. As we continue to see a rise in data breaches and attacks involving extortion, ransomware, and a disruption of critical information systems, we must prioritize our efforts to manage and reduce human risk.

To comprehensively manage human risk, we must start by changing behavior in ways that directly combat the threats that target our staff and our members. We can accomplish this by implementing a security awareness program to provide training, education, and knowledge specifically tailored towards addressing these threats, with priority given to the threats that pose the greatest risk. Over time this will not only accomplish our goal of managing and reducing human risk, but it will also embed security within our culture to better protect our staff, our members, and our community.

# Engagement Strategy

The security awareness program’s goal is to manage human risk. This is ultimately done by changing the behavior of our employees. Behavior change doesn’t occur in a vacuum but is instead dependent on a variety of factors such as culture, individual motivation, communication methods, accountability, and human interaction. We need to consider how each of these factors contributes to our security awareness program to ensure we implement each component in a way that maximizes our chance of successfully changing behavior. To do so, we should incorporate the following essential elements as we implement each component.

Engagement Strategy Essentials

* Leverage existing culture
* Build strong working relationships
* Use incentives and deterrents to increase motivation
* Clearly communicate expectations and maintain accountability
* Choose different communication methods and training modalities based on the audience and training content
* Incorporate the following into all communications:
  + A focus on why this is important
  + Encouraging and positive messaging
  + Consistent branding

# Organizational Culture

To maximize the effectiveness of our security awareness program, it must be compatible with our culture. Engagement strategies should be applied tactfully to ensure they leverage or support the existing culture when possible and gently steer the culture when needed.

We have a relatively conservative culture rooted in tradition and a sense of small-town community. As such, our employees have a genuine desire to help our fellow members as they are our friends, family, and neighbors. We also have strong leadership that is open to significant change while pushing for continual improvement and increased accountability.

Culture Summary

* Financially conservative but supportive of costly initiatives that support strategic goals
* Socially conservative but moving towards neutral
* Community-oriented with a focus on customer service and community engagement
* Top-down decision making with management pushing for:
  + Rapid growth through redesigns, upgrades, new products, and restructuring
  + Increased accountability and transparently
  + Continual improvement

The combination of these elements lends itself well to behavior change as the culture can provide a significant level of motivation for employees to adhere to new policies and procedures. However, in some cases, this culture may result in demotivation if an employee disagrees with leadership or is not provided with enough transparency to understand leadership’s decision making. We can increase our chances of engaging all employees if we focus our communications around why we are pushing for specific changes and highlight the decision-making process along the way. If we can further tie decisions made back to our organization’s mission, strategic goals, and cultural values, then we can maximize engagement for all employees. Because our culture has strong elements of accountability and constant improvement, the biggest battle is ensuring we make it easy for employees to understand the need to change whenever we’re asking them to do so. Once they understand the need, the structure of the program and the overall culture should enable increased engagement and active participation.

# Branding

Our internal branding efforts will be leveraged to increase engagement further. We use fire-related themes for internal programs to play off our name (Embers). In this case, we intend to use an anthropomorphic fireball cartoon character named Blaze. This character will be a mascot of sorts that is presented as a mischievous but likable character that appears in security awareness training and communications, specifically any time action or inaction on the part of the employee could result in harm. It will act as a cue for employees to pay attention so they “don’t get burned” by simple mistakes. It will also serve as a reminder that threats may be waiting to capitalize on any of our mistakes. To ensure consistency and maximize effectiveness, this branding should be applied to all training sessions but focused on items that require specific attention. This is in addition to our standard logo and branded presentation templates.

# Training Methods and Modalities

The implementation of the program will leverage our engagement strategies through a variety of communication methods and training modalities. The program structure consists of three categories of training.

1. Employee Onboarding Training (One Time)
2. Reinforcement Training (Monthly)
3. Compliance and Governance Training (Annually)

It is worth noting that any in-person training can also be completed via remote meetings if necessary, but in-person is preferred.

## In-Person New Hire Onboarding Training

Description

All new hires will attend an in-person training session provided by information security staff. Information security staff will walk employees through the security presentation slide deck focusing on the top three most significant human risks, focusing on the actions employees should take and how those actions help reduce risk. This training will also cover any security topics that are required for compliance with regulations and policies. Since new employees are inundated with new information and training, training will be deferred for any topics that don’t address our top risks, along with any topics that are not required for compliance.

Engagement

Human resources staff will require all staff to attend this training before IT staff provides them with their initial network credentials. Human resources staff will also notify the new employees that they are expected to attend a follow-up session. Supervisors are expected to support the effort. The slide deck format has been chosen to be a structured visual aid to help focus on the three most significant risks. Blaze will be introduced and used within the presentation when highlighting actions employees should take. Information security staff are expected to focus on why these actions are important while encouraging questions. Information security staff are also expected to make a good first impression by presenting these topics in a positive and supportive manner as this is the first touchpoint employees have with the program and information security staff.

Goal

At the end of this training, employees should understand the most significant risks they can help address, along with the actions they need to take to do so.

## In-Person New Hire Follow-Up Training

**Description**

A follow-up training will be scheduled after a new hire has completed their first month at Embers. The follow-up training will reiterate the key aspects of the onboarding training slide deck while focusing on how that training is incorporated into their role-specific work duties. Any risk or compliance topics that were deferred during the onboarding training will be covered as well. At this point, the employee should have enough experience to better understand how security policies and their actions relate to their role, allowing for more effective integration into their workflow.

Engagement

Information Security staff will reach out to them directly to schedule their follow-up training in coordination with HR and the employee’s supervisor. An expanded version of the onboarding slide deck will be used to maintain the existing familiar structure, branding, and content while adding topics that surround lesser risks and additional compliance topics. Information security staff are expected to continue to focus on the importance of employee actions while presenting in a positive and supportive manner that encourages discussion. This discussion not only encourages employees to seek clarification and get practical guidance on how to integrate security into their workflow, but also encourages a stronger working relationship and overall comfort with information security staff. This relationship is a key to ensuring employees are comfortable asking questions and reporting any issues or security incidents.

Goal

At the end of this training, the employee should be comfortable with the security policies and procedures that pertain to their position, understand why and how their actions can meaningfully reduce risk, and be comfortable reaching out for support if needed.

## Monthly Phishing Training

Description

Employees will receive a phishing email each month as part of our reinforcement training efforts. Phishing emails will have an appropriate level of difficulty and be designed to focus on education and awareness. More specifically, phishing emails must not leverage any insider information and must have at least one red flag that employees are trained to identify. Employees who fall for a phishing email will be redirected to an educational infographic highlighting the red flags they could have identified.

Engagement

Any employee who reports the monthly phish will be entered in a drawing to win a gift card. This incentivizes reporting as employees who don’t report are not eligible even if they didn’t fall for the phishing email. In addition to the monetary incentive, the winner will be recognized in the monthly security newsletter. If an employee falls victim to a phishing email three times within the last year, they will be enrolled in a short computer-based training program surrounding phishing. Computer-based training lends itself well to this use case as it can be easily tracked and performed at the employee’s own pace. Additional failures will result in additional training and notifications to both their supervisor and human resources. Those who fall for the monthly phishing email will never be identified to the general staff, but instead only be reported to the employee’s supervisor and human resources when warranted.

Goal

These monthly training should provide insight into different types of phishing emails and ensure employees are continually identifying and reporting phishing emails.

## Monthly Security Newsletters

Description

Our monthly security newsletters are designed to reinforce training by leveraging any lessons learned from relevant security incidents. Information security staff will leverage both internal and high-profile external security incidents to highlight how staff can directly reduce the risks that contributed to these incidents.

The newsletter will also have the results of the monthly phishing campaign. In addition to announcing the winner of the drawing along with their prize, the results will also include metrics and visualizations that depict the overall trends surrounding success rates and reporting rates.

Engagement

Newsletters will be delivered via email and posted on our intranet. This ensures all staff receive the newsletters while also making them easily available for reference. The newsletters should be short, focusing on one or two key things that staff can apply at work or home. They should include information to support why those key things are important and how they address specific risks. This reinforces previous training and promotes continuous improvement and integration of security best practices into our employees’ lives at work and at home. Branding and positive messaging should be incorporated to ensure consistency with other security awareness communication.

Goal

These monthly newsletters should ensure employees can apply lessons learned from relevant security incidents while encouraging continual improvement to further embed security within the organizational culture.

## Annual Computer Based Compliance Training

Description

Staff will be required to complete a computer-based compliance training program each October as part of Security Awareness Month. This training will cover all the elements required to comply with our policies and regulations, focusing on how to securely store, transmit, and dispose of member information for both electronic and hard copies.

Engagement

Whenever possible, this training will be no more than 30 minutes, broken up into small videos of no more than 5 minutes each. Interactive and gamified training should be included whenever possible to increase engagement. Information security staff will announce the training in advance along with the deadline for completion. Information security staff will also send out at least one reminder as the deadline approaches. Everybody who completes the training on time will receive a small token of appreciation such as a candy bar or other give-away (SWAG). Information security staff will work with employee supervisors and human resources staff to follow up with any employees who have not completed the training until all employees have completed the training.

Goal

These annual computer-based training sessions reinforce employee onboarding training while ensuring that employees are trained according to security policies.

## Biannual All Staff In-Service Training

Description

Security training will be incorporated into at least one of our biannual in-service training sessions. Information security staff will present overall fraud and risk trends, including how they pertain to the credit union. The presentation will also cover any policy changes and what we expect in the coming months.

Engagement

In-service training sessions are ideal for in-person presentations as all staff are required to attend and participate. These training sessions should provide insight into security oversight along with the decision-making process that determines how and why our security policies change. As with other training sessions, these should be branded, have a positive message, and have a significant focus on how the content covered directly ties to our mission and strategic goals.

Goal

These annual or biannual training sessions provide transparency related to governance and decision-making while demonstrating management’s commitment to security.

# Metrics

To effectively monitor and manage the security awareness program, we must be able to measure its impact. Measuring impact is directly dependent on carefully determining the correct metrics to use. Choosing and implementing the most relevant metrics will allow us to analyze trends related to the risks we’re trying to mitigate.

To choose our metrics, we start with the most significant risks identified in our human risk assessment and focus on the actions our employees must take to mitigate those risks. In some cases, metrics may focus directly on the employees’ behavior (such as the percentage of employees reporting the monthly phishing email). In other cases, measuring the impact of behavior may be more appropriate (such as the percentage of security incidents related to not properly verifying the identity of a member). Ease of measurement may play a significant factor in metric choice but should not drive the decision entirely. Metrics must tie back to impact and risk reduction to be useful.

## Identity Verification

We’ve seen an uptick in the number of fraud cases related to the transfer of funds. These often include unauthorized wire transfers, ACH transfers, ATM withdrawals, and credit card advances. These incidents cost the credit union and our members thousands of dollars and degrade our members’ trust. In most cases, these transfers would be prevented if employees strictly followed our identity verification procedures.

Metric

We will measure the number and percentage of fraud and security incidents that involve an employee failing to follow our identity verification procedures.

Measurement Method and Frequency

All fraud and security incidents are investigated to determine the root cause. If it is determined that an incident was related to an employee not following identity verification procedures, then it will be flagged and added to a list. This information is compiled monthly and used to update a rolling trend analysis that covers both the number and percentage of incidents related to improper identity verification.

Goal

This metric is used to verify that employees are following the procedures for identity verification as covered in our security awareness training. This will help ensure our training efforts result in fewer fraud and security incidents surrounding improper identity verification.

## Mishandling of Sensitive Information

Employees mishandling sensitive information remains one of our biggest causes of security incidents. These incidents typically don’t result in monetary loss but they normally result in us having to notify a member that their information was accessed by an unauthorized third party, which in turn degrades their trust. Examples include mailing or emailing member information to the wrong member and accidentally giving too much access to a member’s account when linking accounts together (such as enabling account to account transfers).

Metric

We will measure the number and percentage of fraud and security incidents that involve an employee mishandling sensitive information.

Measurement Method and Frequency

All fraud and security incidents are investigated to determine the root cause. If it is determined that an incident was related to an employee not mishandling sensitive information, then it will be flagged and added to a list. This information is compiled monthly and used to update a rolling trend analysis that covers both the number and percentage of incidents related to improper handling of sensitive information.

Goal

This metric is used to verify that employees follow the procedures for handling sensitive information as covered in our security awareness training. This will help ensure our training efforts result in fewer security incidents related to the mishandling of sensitive information.

## Phishing Email

Phishing emails remain one of our biggest threats as they are often successfully used by attackers to gather credentials or compromise employee devices. While we have strong technical controls in place, we still depend on our employees to identify and report phishing emails to reduce the risk of system and credential compromise.

Metric

We will measure the success rate and reporting rate of our phishing campaigns.

Measurement Method and Frequency

This information is readily available within our phishing campaign management software. It will be compiled monthly and sent to management in addition to its inclusion in the monthly security awareness newsletter.

Goal

By monitoring the percentage of employees who pass phishing tests and report phishing email, we can determine how effective our monthly training is at both educating employees on phishing and encouraging them to report phishing. The risk of phishing decreases as our employees become more adept at identifying and reporting phishing.

# Appendix A: Learning Objectives

Our human risk assessment highlights the most significant human risks along with the associated behaviors our employees can perform to mitigate those risks. We develop learning objectives based on those behaviors to help develop our training curriculum. We develop metrics with these learning objectives to ensure the behavior change can be measured and monitored to ensure our security awareness program has the desired impact.

## Handling Sensitive Information

Target Audience

All employees, contractors, and volunteers that have access to sensitive member information such as non-public personal information (NPPI)

Goal

Learners will be able to describe procedures for identifying and handling sensitive member information such as NPPI. They will be able to describe approved methods for accessing, storing, transmitting, and disposing of sensitive information in both physical and electronic forms.

Background

Embers is entrusted with a significant amount of sensitive information related to our members. In the wrong hands, this information could be misused for identity theft and fraud. The proper handling and safeguarding of this information is critical to protect our members and maintain their trust. To that end, we need to ensure our employees can identify the different types of information and the proper handling methods for each. We also subject ourselves to additional risk and liability if we send sensitive information through insecure channels or ask our members to send us sensitive information through insecure channels (such as email), so it’s crucial that our employees know how to both send and receive sensitive information in accordance with our security policies and procedures.

Learning Objectives

1. **Determining Information Classification**. Learners can identify the difference between public, internal, and confidential information as outlined in our data classification and handling policy.
   1. ***Individual Metric****:* The learner can correctly identify each type of information during a training activity.
   2. ***Organization Metric***: A report of all employees indicates that 95% can correctly identify each type of information on their first training attempt.
2. **Sending Sensitive Information**. Learners can identify acceptable methods for sending sensitive information internally, to members, and to third parties
   1. ***Individual Metric:*** The learner can correctly identify approved methods for sending each type of information *under each circumstance* during a training activity.
   2. ***Organization Metric:*** A report of all employees indicates that 95% can correctly identify approved methods for sending each type of information *under each circumstance* on the first attempt.
3. **Requesting Sensitive Information**. Learners can identify proper methods for *requesting sensitive information from members*.
   1. ***Individual Metric:*** The learner can correctly identify the approved methods for requesting sensitive information from members per our internal security procedures.
   2. ***Organization Metric:*** A report of all employees indicates that 95% can correctly identify each approved method for requesting sensitive information from members on their first training attempt