Security Awareness Program: Example Project Plan



***Note****: This document is from the* [*SANS MGT433 Managing Human Risk course*](https://sans.org/mgt433) *and is based on the fictional company Linden Insurance. This template is an example of what a Security Awareness project plan can look like, we are in no way implying this is what your plan should look like. By security awareness we mean an organized effort to engage your workforce and manage your organization’s human risk. Other names we see organizations use to identify their program include security behavior and culture, security communications, security influence and engagement, security education and training or human risk management. Feel free to copy, modify and / or edit as you see fit or simply use the sections that help you the most for your own use.*

Table of Contents

[1. Executive Summary 3](#_Toc127959666)

[2. Ownership and Responsibilities 4](#_Toc127959667)

[3. Identifying and Managing our Top Human Risks 4](#_Toc127959668)

[Risk Prioritization 5](#_Toc127959669)

[Risks by Target Group 6](#_Toc127959670)

[4. Influence, Engagement and Training 7](#_Toc127959671)

[Why People Should Care 7](#_Toc127959672)

[Organizational Culture Analysis 8](#_Toc127959673)

[Communicating & Training on Security 9](#_Toc127959674)

[Simplifying Security 11](#_Toc127959675)

[Branding and Imagery 11](#_Toc127959676)

[Localization Requirements 12](#_Toc127959677)

[5. Long-Term Sustainment 12](#_Toc127959678)

[Annual Review 12](#_Toc127959679)

[Monthly Executive Briefings 12](#_Toc127959680)

[6. Metrics 13](#_Toc127959681)

[Compliance Metrics 14](#_Toc127959682)

[Impact Metrics 15](#_Toc127959683)

[Strategic Metrics 17](#_Toc127959684)

[7. Summary 17](#_Toc127959685)

[8. Appendix A – Communications Matrix 18](#_Toc127959686)

[9. Appendix B – Risk Tracking Matrix 19](#_Toc127959687)

# Executive Summary

***NOTE****: The purpose of an Executive Summary is to explain to leadership why your program is important to your organization. Do not focus on what you are doing but how it supports and enables their strategic priorities. Consider starting with your organization’s mission, how cybersecurity supports the mission, then how your program is key to supporting cybersecurity. The greater the sense of urgency you create, and the greater the perceived business value, the more likely you will gain leadership support.*

**Problem**: Our mission at Linden Insurance is to provide affordable insurance to working families in our community. Our customers depend on and trust us to insure them and their families against the incidents and dangers of today’s world. That trust depends on our ability to secure our systems and their information. If we experience a cybersecurity incident, we may not be able to provide our community the services they need, expose them to tremendous risk to include identity theft and we would experience tremendous financial and reputational costs and most likely be liable to extensive litigation and fines.

To support and secure our mission, our organization leverages the latest security technologies with a defense-in-depth strategy. However, a growing number of damagingincidents in our company are due to people, specifically human risk. Human risk is not only when cyber attackers actively target and attack our workforce, but with the growing adoption and complexity of technology, to include working from home and Cloud, it is becoming far more common for our employees to make mistakes. Human risk has become the fastest growing risk to our organization. [*NOTE: Provide any data points on human based incidents to your organization in past six to twelve months.]*

**Solution**: A security awareness program is an organization wide effort to effectively manage our human risk by changing our workforce’s behaviors and build a strong security culture through positive engagement, enablement and training. This program does not replace existing security controls, instead it builds on and helps address any weaknesses or gaps. In addition, as we are in a heavily regulated industry, we have numerous legal and compliance obligations to train and secure our workforce. To this end, we will build, maintain, and measure an active Security Awareness Program (SAP). The SAP is a long-term effort involving our workforce at all levels, with both foundational, organization wide training and targeted role-based training. This program will be led by our Human Risk Officer who will report directly to the CISO and be guided by a dedicated advisory board.

**Value**: The Security Awareness Program will ensure we can securely support our customers who depend on us for protecting their families and futures, support our digital transformation efforts, help protect our reputation and ensure we meet regulatory requirements.

# Ownership and Responsibilities

The Human Risk Officer (HRO) is overall responsible for the Security Awareness Program and our efforts to manage human risk. They will have a security awareness team dedicated to this effort with all members of the team reporting directly to the HRO. In addition, the Communications department will assign someone full-time to work with and embed in the security awareness team to ensure strong coordination with the Communications department. The HRO and their security awareness team will report directly to the CISO and work directly with members of the security team, to include Security Operations Center, Cyber Threat Intelligence and Incident Response. This ensures the Security Awareness Team will have access to all the data and resources they need to prioritize and manage human risk. In addition, the security awareness team will be in a far better position to support the security team in all their workforce communications, tool rollouts and security policy development and training.

# Identifying and Managing our Top Human Risks

***NOTE****: The purpose of this section is to identify, prioritize and document your top human risks and the key behaviors that manage those risks. Remember, every behavior you teach has a cost both to your workforce and your organization. In addition, the fewer behaviors you focus on the more likely your workforce will exhibit them. As such, our goal is not to address all human risks, but prioritize and focus on the top ones.*

The goal of our Security Awareness Program is to effectively manage our human risk. As we cannot address all human risk, we will identify and focus on the top human risks that have the greatest impact to our organization. Once identified, we will identify the behaviors that most effectively manage those risks. These are the behaviors we will focus and train our workforce on. The fewer risks we focus on, the more likely we will change those behaviors, minimizing costs and ensuring the greatest value for Linden Insurance.

We identified our top human risks by completing a human risk assessment of our organization. By risks we mean both accidental (such as someone emailing a document to the wrong person due to auto-complete) and deliberate (such as a targeted phishing attack). This assessment process included data from all incidents within our organization over the past 12 months, the results from two security assessments, a security survey of our workforce, reviewing three security intelligence reports from this year, and data from the FS-ISAC. In addition to managing human risk, several training topics are also included for compliance, policy or legal reasons.

We have broken down our risks into two categories. This is done to ensure we deliver the right training to the right people and no more, effectively making the most of our workforce’s limited time and resources.

* **CORE**: These are the foundational risks shared by everyone in our organization. Topics address common human risks such as passwords and social engineering attacks.
* **ROLE**: These are risks unique to specific roles, departments or regions and is often driven by what data or systems people have access to.

## Risk Prioritization

Below are the top seven human risks identified in our risk assessment and will form the foundation for our program. Our goal is to effectively manage these top seven risks through behavioral change and skills based training.

*NOTE: Consider providing a list of the topics you have selected, a brief description of each, and a short rationalization of why each was selected. This is both for Risk driven topics and Compliance driven topics. Here is an example of one topic.*

|  |  |  |
| --- | --- | --- |
| Topics | Description | Reason |
| Passwords | We cover what passwords are, why they are important, and what makes a strong password with an emphasis on passphrases. In addition, we cover how to protect and safely use passwords, including the use of a unique password for every account, leveraging password managers, and not sharing passwords with others. Finally this program will be used to train and support our MFA rollout. | We have made a change to our password policy, migrating from complexity to passphrases. We need to train people on these new policies. Also, we had three incidents last year due to password sharing/reuse. Finally, we are rolling out password managers and MFA company-wide, which we need to train our workforce on. |

## Risks by Target Group

Below are the specific training topics assigned to each target group based on risk and compliance requirements. Training highlighted in orange is considered the Core training for everyone. Training not highlighted is role based. This role-based approach to training ensures that the right training is assigned to the right people, making the most of limited time and resources.

|  |  |  |  |
| --- | --- | --- | --- |
| Risks | All Employees | IT Staff | Executives and Assistants |
| Social Engineering / Phishing | X | X | X |
| Cloud | X | X | X |
| Malware | X | X | X |
| Mobile Devices | X | X | X |
| Passwords | X | X | X |
| Data Handling | X | X | X |
| Reporting Incidents | X | X | X |
| GDPR | X | X | X |
| International Travel |  |  | X |
| Targeted Attacks |  | X | X |
| Privileged Access |  | X |  |
| Creating a Cyber Secure Home (Optional) | \* | \* | \* |

For a more detailed description of each topic and the behaviors we will be focusing on refer to the Learning Objectives in the appendix.

# Influence, Engagement and Training

***NOTE****: The purpose of this section is to document how you will communicate to, train and secure your workforce, what is your overall strategy to change behavior. You need to cover not only what you will be doing, but why people will care.*

Now that we identified our top risks and behaviors that manage those risks, we need to define our strategy on how we will communicate to, engage and train our workforce so they exhibit key security behaviors. Changing our workforce’s behavior is no easy task and requires aligning with our culture, understanding what motivates our people and communicating in a clear, simple and supportive manner.

## Why People Should Care

To be successful, we must first engage people; if our workforce is not listening or are not motivated to change behaviors, this program will fail. The first step is to ensure people believe in the value of security and why it matters. We will communicate this on two levels:

***NOTE****: We provide two different examples below of WHY a workforce should care. You do not have to provide multiple reasons like we do in this example, we simply wanted to provide you with multiple ideas.*

* **Organizational**: As one of the most trusted insurance companies on the east coast, we help build and maintain the stability and future of our customers and their families. The security and integrity of our organization is literally key to lives of millions of families. We will ensure our workforce understands that cyber is now the greatest risk to our organization and their behaviors can impact lives around the world. We will enforce that with the idea of “*Secure our data, protect our customers families and their peace of mind.”*
* **Individual**: Our training will emphasize that what people learn not only protects them at work, but also protects them at home and in their personal lives. Our intent is to not only engage people at a personal level, but also change how they act by exhibiting the same secure behaviors at home. Ultimately, security becomes part of people’s DNA.

## Organizational Culture Analysis

Overall, the company still has a strong family feel to it, even though it has grown dramatically in the past 35 years. Leadership likes to make sure employees feel taken care of, to include having very strong health and retirement benefits. Employees feel safe and trust leadership to take care of them. However, due to the original founders and the nature of the insurance industry and how heavily it is regulated, the overall culture is still conservative with a focus on stability. As such, edgy humor will most likely not be effective nor will we attempt to intimidate or scare people. Instead, we intend to leverage the family feel of our company.

Our training will be positive and encouraging. We want to create a sense of how we are all in this together working as a family, with an emphasis of how the security team is supportive, approachable and helpful. Many of the events and training will focus on not just work-related topics but home and family topics, such as securing your kids. We understand there may be cultural differences with our office in Montreal, Canada. As such, we will have a representative from each country on our Advisory Board to guide us on how to best approach each country. We will follow these five principles to guide our program and how we engage and train our workforce.

1. We will understand and align with our family focused culture. Whenever possible, we will focus on personal / family benefit as well as benefit to the organization.
2. Clearly communicate what outcomes are expected in an open and transparent way that is both easy for people to understand and follow.
3. Ensure that the “Why” is communicated for each behavior or topic.
4. Communications will be positive with an emphasis on enabling people to make the most of technology safely and securely. Our goal is to create trust between our workforce and the security team.
5. Use recognition as a primary incentive whenever possible. We want to make heroes out of those doing the right thing.

## Communicating & Training on Security

Before any training is released, we will communicate to the workforce what to expect to include the importance of the training, the goals, as well as the scope of employees receiving the training. We want to be as open, transparent and as approachable as possible.

**Primary Training**: The primary method we will use to train our workforce is Computer Based Training (CBT) through our internal Learning Management System (LMS). CBT is a common and effective method for content delivery. It allows our workforce to take the training on-demand as their schedule allows and is easy to implement in a way that we can track participation and include evaluations, assessments and surveys as part of the training. During online training, all individuals also take an online quiz to test comprehension of each module. The goal of the annual training is to both set the baseline training for our organization and ensure we are compliant. The Security Awareness Team assumes operational control of online awareness training and enforces this policy.

Emails will be sent out to the entire workforce members notifying them they are enrolled in the training. In addition, we will have automatic notifications that remind staff if they are past due. A final, automatic notification will be sent that congratulates individuals when training is successfully completed. For anyone hearing impaired, our training contains scripts and closed captioning for all online video training. For anyone suffering from loss of site or completely blindness, we will provide PDF versions of the modules that can be read with a screen reader.

**Reinforcement Training**: We understand and recognize that training people annually is not enough to change their behaviors. As a result, we continuously reinforce key behaviors through multiple reinforcement methods throughout the rest of the year by reinforcing one key topic each month. Each reinforced topic will not be introducing something new but covering material already covered in the primary training. By leveraging multiple modalities, we can reach the different generations and people with different learning preferences. To promote engagement with our workforce, we will also leverage public events in the news (such as very public breaches), focus on personal benefit when possible, and distribute content that is seasonal, such as key security steps during tax season or how to shop securely online during the holidays. This reinforcement training consists of the following:

* **Newsletters / Infographics**: We send out a monthly newsletter to all employees and staff. The newsletter is two pages and distributed in digital format. Topics focus on personal benefit, with the goal of people taking the newsletters home for personal use. Depending on reception of this, we may consider transitioning to something more concise and easier to consume, such as fact sheets or infographics.
* **Security Podcast:** The security team (in partnership with Communications) will host a bi-monthly podcast on the latest updates in cybersecurity. Each podcast will be very short (no longer than 3-7 minutes) with a focus on what the latest events in the cybersecurity world and how employees will be personally impacted and how they can benefit or take care of themselves. Our goal is to put a personal face on the security team.
* **Virtual Lunch-n-Learns**: We will actively promote and do on-site or virtal lunch-n-learns for any business unit or group that requests them. Topics are customized per the business unit’s request. For the employee-wide target group we will host quarterly lunch-n-learns that focus on topics that personally benefit people. In addition, we will look to bring in external speakers, such as the FBI or Secret Service.
* **Special Events**: We will hold a large security event twice a year. Events focus on personal security to encourage group participation, such as mobile device reviews. Our first planned special event will be an online Digital Scavenger Hunt.
* **Slack**: We have noticed that our internal social media / communications tool Slack is becoming very popular, especially with the younger generation or technically savvy employees. We will begin to use yammer as a way to open a dialogue with this community, to include YamJams and “Ask the Executive Anything” events. However, to ensure success and interaction we will need to dedicate half of a FTE (Full-Time Employee) to moderating such channels.

***NOTE****: One idea is to include a communications matrix in the appendix. We have included a generic one at the end of this project plan as an example. For more examples of communications templates, refer to the* [*MGT433 Digital Download Package*](https://mgt433.org/)*.*

***NOTE****: If you intend to roll-out an Ambassador Program, this is where you would provide more information. For details on Ambassador Program’s, refer to the Ambassador folder in the* [*MGT433 Digital Download Package*](https://mgt433.org/)*.*

## Simplifying Security

Changing our workforce’s behavior and creating a secure environment is not just limited to communications and training, we need to make security as simple and approachable as possible. The easier a behavior is, the more likely people will exhibit it. In addition, we lay the foundation for a much stronger security culture.

* **Security Communications & Tool-Rollouts:** The security awareness team will actively partner with the security team and assist them in all workforce communications. This ensures that all security communications are simple to read, understand and follow using clear and helpful language. In addition, the security awareness team will assist the security team in tool rollouts that directly impact the workforce and require them to change behaviors or learn new skills.
* **Security Policies**: The security awareness team will actively partner and work with the GRC (Governance, Risk and Compliance) team in our policy development and communication. We identified that our security policies are perceived as both complex and very difficult to follow, resulting in numerous policy violations, risk behaviors and ultimately driving a very negative security culture. Our intent is not to change policy, but simplify the requirements of policy whenever possible, and then communicate those simplified policies in a way that is both easy to understand and follow.

Our goal is to ensure that security is perceived by our workforce as helpful and supportive. To achieve that we must go beyond just training and simplify people’s every interaction with security.

## Branding and Imagery

While our organization has a very strong brand, we have purposely chosen not to use it. Instead, we developed an informal mascot called Samantha to assist in communicating our program. Samantha is a curious bobcat cub who always plays with technology and learns about the security issues involved. Samantha puts a softer, nonthreatening face on security. In addition, this fits well with the security team’s drive to create a more friendly, approachable security culture and is different than any other training program to date. Finally, when people have security questions or a security incident they want to report, they can submit it to Samantha, someone who may be far more approachable.

## Localization Requirements

Most of our organization speaks American English; however, we have small offices that require training in their local language, specifically Quebec, Canada. As such, our program will communicate in American English and Canadian French.

# Long-Term Sustainment

Our security awareness and education program is a long-term project. As such, we will review and update our program once a year.

## Annual Review

As part of keeping our program relevant, we will review and update the program on an annual basis. The two fundamental parts of the review include:

* **Risks**: We will complete an annual review of all human based risks and the behaviors that manage those risks. We want to ensure that at all times we are addressing the most current risks and teaching people the right behaviors. As both technology and cyber threat actors change, so to do the risks our workforce’s face.
* **Engagement**: How we communicate to and train our workforce needs to be continually updated and changed. Not only will this help ensure that our workforce is engaged, but as our workforce changes over the years so to does the way we communicate and train.

As part of these annual updates, we will maintain a risk tracking matrix that identifies our top human risks each year, enabling both the security team and leadership to see how our risks changes each year and why.

## Monthly Executive Briefings

We will conduct quarterly briefings with the executive staff led by the head of the Security Awareness team. These briefings are designed to communicate what the program is doing, the impact and value of the program, success stories, and any possible blockers the team needs help with. To ensure we are presenting information valuable to leadership, and in their terms, we will coordinate these efforts with the champion identified in our Advisory Board.

# Metrics

Metrics are an essential component of any program and managing human risk is no different. We have two strategic goals with our metrics program. First, to effectively measure and manage the program, we want to identify the areas we are weakest and strongest at and how we can improve. Second, metrics enable us to demonstrate and communicate the value and impact of the program to senior leadership to help ensure long-term support. We will leverage the two following metric categories; Compliance and Impact. Compliance metrics measure what we are doing, these are used primarily to communicate our activities to leadership and ensure compliance. Impact metrics measure what change we have caused in the organization, both behaviorally and culturally.

We will maintain full transparency with the workforce on what metrics we collect, how, and why; all findings are anonymized where applicable and privacy is always protected. Our goal is to avoid any name and shaming or punitive strategies while recognizing and making heroes out of those doing the right thing. The only time we will identify specific individuals exhibiting insecure behaviors is when they continually and consistently exhibit risky behaviors that expose our organization to unacceptably high levels of risk.

## Compliance Metrics

We track the following activities to ensure we meet the compliance standards of SOX, PCI DSS, and international and state privacy laws. These metrics track and measure what we are doing, not the impact.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Metric Name** | **What Is Measured?** | **How Is It Measured?** | **When Is It Measured?** | **Who Measures?** |
| Training Completion | Who has or has not completed online Computer-Based Training | Completion reports from Learning Management System | Annually | Whoever is responsible for primary training |
| Communication Methods | • Distribution of newsletters, posters, or factsheets • Number of booth events and number of attendees • Number of lunch-n-learns and number of attendees • Number of posts on internal social media channels (such as Slack) | Track and document when and how security awareness materials are communicated to the workforce. | Monthly | Security Awareness Team |
| Policy Sign-Off | People have completed / understand training and acknowledge they will adhere to our policies | Signature or sign-off | Part of annual review | Supervisor and/or Human Resources |

## Impact Metrics

The goal of impact metrics is to measure the impact we are having. By impact, we mean either the behaviors of our workforce or their attitudes and beliefs towards security. These metrics were selected as they measure the greatest risks to our organization.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Metric Name** | **What Is Measured?** | **How Is It Measured?** | **When Is It Measured?** | **Why is this Measured?** |
| Phishing Repeat Offenders | Number of workforce that repeatedly fall victim to phishing simulations. These individuals are not changing behavior and represent a high risk. | Phishing assessment | Monthly | Phishing represents one of the greatest human risks to our organization and is a priority of our program |
| Lost/Stolen Devices | Number of devices (laptops, smartphones, tablets) that were lost or stolen. What percentage of those devices were encrypted? | Reports to Security Team or by physical asset audits | Monthly | Lost devices happen far more commonly than many realize. |
| Cloud | Number of data exposure incidents due to IT Admins failing to properly secure their accounts or the sensitive data they handle in the Cloud | Number of identified or reported incidents. | Monthly | As part of leaderships Digital Transformation initiative, we have been migrating extensively to the Cloud, but are having multiple incidents driven by IT Admin behaviors. |
| Engagement | Number of requests the Security Team gets to do security briefings for other business units or teams | Tracking by the Security Team. | Monthly | The greater our workforce is engaged the more likely we can change behavior. |
| Workforce’s Attitudes Towards Security | Does the workforce understand the need for security, the important role they play, and support the behaviors needed? | Cultural survey | Annual or after training | This is critical for understanding and growing our security culture. |

***NOTE****: Another way to present metrics is you provide each metric individually, then with a paragraph explaining it. Here is an example of Phishing Click Rates.*

**Phishing Click Rates**

|  |  |
| --- | --- |
| **What is measured?** | Percentage of workforce that clicks on phishing simulation emails sent out by the Security Awareness Team. |
| **How is it measured?** | Phishing simulation solution we use to send out phishing emails will track how many individuals click on the links or open the attachments. |
| **When is it measured?** | On a monthly basis. |
| **Who measures?** | Security Awareness Team |
| **Why is it measured?** | Phishing represents one of the greatest human risks to our organization as its is one of the most common attack methods used by cyber attackers. This metric enables us to determine how vulnerable our workforce is to phishing attacks and if the security training is effective in changing peoples behavior. |

The Security Awareness team will manage and send out phishing simulation emails monthly to track workforce’s click rate. Simulations are considered and communicated as training, our goal is to help our workforce. Any individual that clicks or falls victim will be notified so they can learn, but neither their supervisor nor leadership will be notified, protecting the individual’s identity. Individuals who repeatedly fall victim will be identified as high risk individuals, as they will need to retake the training, and their direct supervisor and HR may be notified.

## Strategic Metrics

We will track the impact of the awareness program at a strategic level by measuring these two strategic metrics. These metrics are not unique to the security awareness program, instead they help measure the contribution of security awareness to the overall security posture of our organization. These two were selected as they are the strategic security priorities of the Chief Information Security Officer.

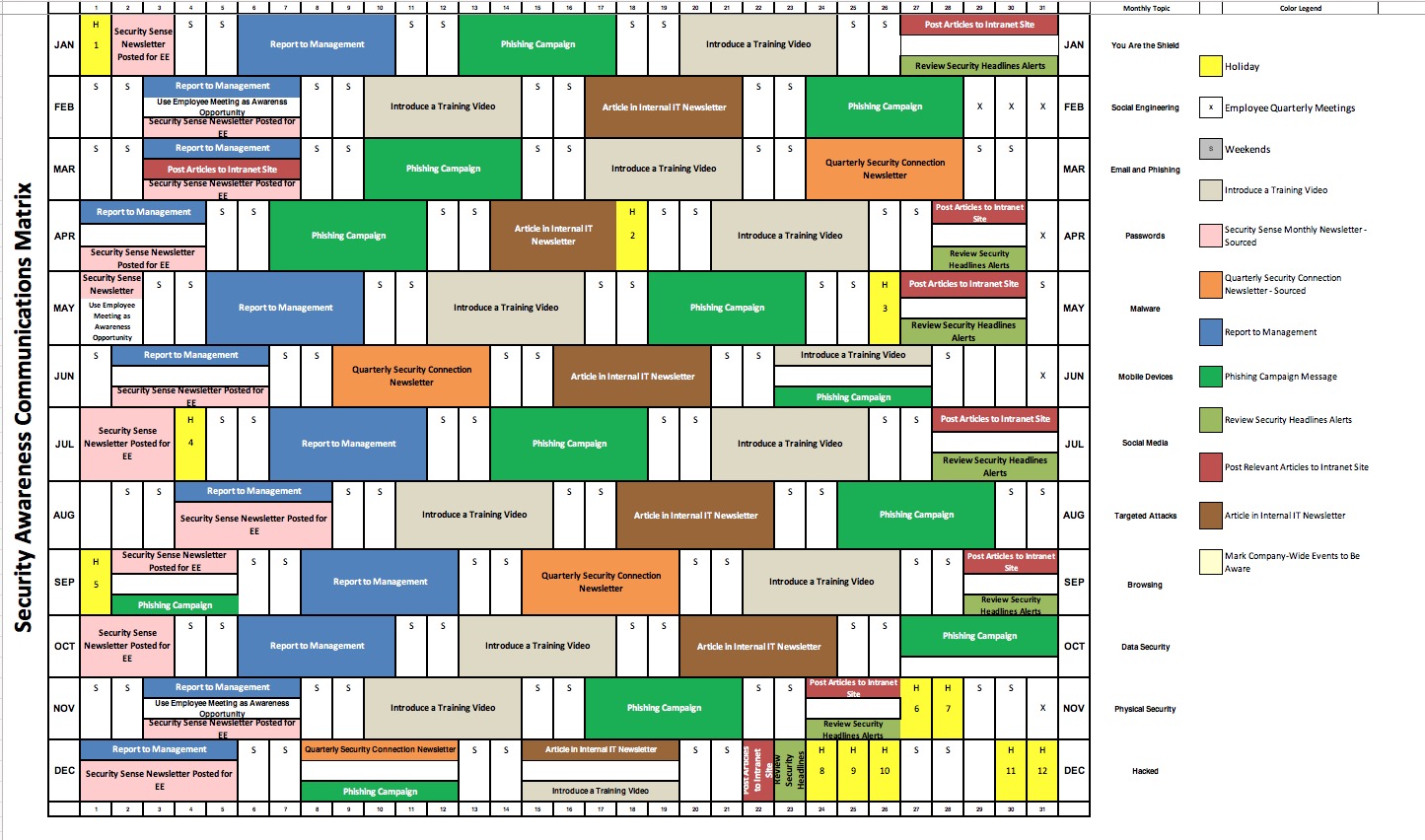
* **Number of Incidents**: As our workforce is trained, the overall number of major incidents we experience should go down.
* **Time to Detect**: As our workforce is trained to identify and report incidents, our ability to detect and respond should dramatically improve. This decreases attacker dwell time, minimizing the impact they may have.

In addition, in our quarterly briefings to leadership we will demonstrate how the Security Awareness Program and its activities are contributing to and supporting our alignment with the NIST Cybersecurity Framework.

# Summary

The purpose of the Security Awareness Program is to effectively manage our human risk, one of the greatest (and fastest growing) risks to Linden Insurance and its mission. This program will help ensure that we not only meet our legal and compliance requirements but protect our reputation and our ability to insure and support our community.

# Appendix A – Communications Matrix



# Table Description automatically generatedAppendix B – Risk Tracking Matrix