**Mattress & More Inc.**

**Security Awareness Plan**

**ISE 5300**

**Building Security Awareness**

[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 February 2021.]

|  |  |
| --- | --- |
| **Prepared By** | Wes Walker |
| **Date Revised** | 03/02/21 |
| **Version Number** | 1.0 |
| **Document ID** | ISE\_5300 |

Table of Contents

[README 3](#_Toc40527269)

[1.0 Executive Summary 4](#_Toc40527270)

[2.0 Engagement Strategy 5](#_Toc40527271)

[2.1 Organizational Culture 5](#_Toc40527272)

[2.2 Communication and Modalities 5](#_Toc40527273)

[2.3 Reinforcement 7](#_Toc40527274)

[2.4 Branding 8](#_Toc40527275)

[3.0 Metrics 9](#_Toc40527276)

[3.1 Security Awareness Training Completion 9](#_Toc40527277)

[3.2 Phishing Campaign Clicks 9](#_Toc40527278)

[3.3 Virus Reported 10](#_Toc40527279)

[4.0 Appendices 11](#_Toc40527280)

[4.1 Learning Objectives 11](#_Toc40527281)

# README

I have chosen to write a Security Awareness Plan for the organization Mattress & More Inc. I am basing this on my current place of employment and have anonymized the details. I have chosen this organization as it presented the challenge that it lacked a robust formal information security group. Network or IT engineers and IT system administrators perform almost all security-related functions. The company conducts its own in-house monitoring of systems for uptime and reliability but does little real-time monitoring of security alerts. They have a Security Awareness Plan that is in the early stages and has room for improvement.

Mattress & More Inc, founded in the late 1800s, is in the manufacturing industry with a focus on spring and foam mattresses. They are vertically-integrated in their bedding section, owning steel foundries, steel rod mills, spring manufacturers, foam manufacturers, and mattress makers that put it all together. They also own divisions that make automobile parts, office furniture, and aerospace industry parts. With over ten thousand employees located in branches in dozens of countries on five continents, their employee and customer base are diverse.

The company has struggled in the past with the vast differences in employee types across the company. There are generational and cultural differences that make companywide training programs difficult. They are also a traditional and family-friendly company; as a result, training is forced to be very bland and safe.

The Security Awareness Plan would be to enhance and improve the one deployed by the organization. There has been a large upswing in support for cybersecurity issues in the last few years. The program currently in use has been effective, and it is time for enhancements to the program to continue to improve our security posture.

# Executive Summary

Mattress & More Inc. is a diversified manufacturer with various components and products that one can find in most homes and automobiles worldwide. When we uphold our mission to "create innovative products" and "provide sought-after jobs in communities around the world," we drive increased employee productivity, customer retention and loyalty, and help provide for the communities which help us operate. Technology is playing an increasingly significant role in bridging the gaps between all levels of the company, making it easier for everyone from skilled factory workers to upper management to communicate with each other and our customers. Our ability to collaborate and take advantage of the enormous amount of talent and information available to us is one of our biggest strengths.

As an organization with a global footprint and a very diverse portfolio of products and services, we have a litany of regulations and standards with which to comply. Our health insurance department requires us to comply with HIPAA, the fact that we take credit cards requires us to comply with PCI-DSS, our business with the European Union requires us to comply with GDPR, to name only a few. To date, our security awareness plan has been focused on these compliance issues. We have made excellent progress in ensuring our employees have been given the required information. However, it seems our program has seemingly stagnated at that point.

The breadth of services we provide and the countries we serve makes the organization vulnerable to human risk. Our employees utilize email and digital communications for the vast majority of our business. It makes them susceptible to phishing scams that could harvest credentials, credit card information or lead to potential outages due to ransomware. The realities of doing business today necessitate using the internet, making them vulnerable to viruses and malware merely by searching and browsing. A more serious risk, although remote, could arise in the compromise of an industrial control system. Such an attack could potentially lead to injury of personnel. A security incident preventing us from fulfilling client orders promptly negatively affects our reputation and could result in potential fines for breach of contract. A security incident that results in a client data breach or employee data breach reduces trust and could lead to business loss.

Implementing a next phase and future path for our security awareness plan will allow us to improve on the education of our workforce and provide appropriate metrics to help address training gaps and help us focus on additional areas of concern. The proposed plan for the next 24 months will allow us to move from a compliance-focused security awareness program to a more mature program that promotes security awareness and behavior change. By reducing the human risk, we increase productivity and be true to our core organizational mission to provide for our customers and staff in the communities we serve.

# Engagement Strategy

The Security Awareness Program’s main objective is to create a workforce that can detect risks and respond appropriately. Our employees have access to a wide variety of sensitive information and are continually using email to conduct business and share information. To effectively reduce this human risk, continuous training is essential. Its effectiveness depends on an appropriate tone to communicate critical threats that can be trackable via measurable outcomes. The training must be engaging and show examples that not only improve cybersecurity at work but how it applies to cybersecurity in the user's personal life.

## Organizational Culture

Mattress & More employs more than thirteen thousand employees on five continents. Our employees represent all generations in the workforce, and it is a challenge to engage them all. A very established and publicly traded company, Mattress & More is very traditional. With offices located all over the world, we have to be very aware of the many cultural and religious differences that exist as well.

There have been strides made in recent years to be more informal in some settings and more relaxed. This company has always been family-focused, though, and it has no desire to be too much like a Silicon Valley startup.

The organization fosters a sense of family and community with its employees, and they regularly stay abreast of each other's lives and families. Any training program should strive to use this sense of community and family to shape the content and context of our security topics and events.

## Communication and Modalities

The primary method for delivering content to employees is through mandatory computer-based training (CBT). This training would allow our employees to use their work computers and complete in 30 minutes as their schedule or shift allows, making the most efficient use of their time. A review will be made of the existing training with our Legal and Human Resources departments and updated for compliance or condensed based on our documented objectives in this Security Awareness Plan.

It will consist of several primary modules that apply to all employees. Users will be asked to complete a simple 5 question quiz at the end of each module to validate the employee’s comprehension of the topic just covered.

These include:

* Compliance Requirements, both department-specific requirements like PCI and companywide requirements like Anti-Corruption.
* Privacy, including Personal Identifiable Information (PII), and how to identify and protect it.
* Information Security topics, including web-browsing safety, unauthorized software use, phishing emails, and social engineering attacks.

At the end of the training, employees will have to read the organization’s Acceptable Use Policy and attest that they have read, understand, and will comply with the policy. Users that have not completed training on time, as described in this plan, will have their immediate managers notified and asked to take the training as soon as possible.

The requirements for completion depend on whether the employee is a new hire or an existing employee performing an annual review.

**New Hire Training:** All new hires must go through company-mandated orientation on their first day on the job. Information Security will be part of the agenda, with a member of Information Technology/Security presenting for 15-20 minutes. The goal is to highlight key points, including:

* The importance of security to our organization
* Why employee actions are necessary and why they are a potential target
* Explain Acceptable Use Policy Sections that apply to Information Security

The presentation is kept brief with a reminder that they must complete the Security Awareness computer-based training within 14 days of their first day. An email with a link to the CBT system will be sent to all new employees.

**Annual Computer Based Training**: All employees will be required to take the Security Awareness computer-based training every year to satisfy compliance for security awareness training. The training will be open on February 1st of each year, and users will have until March 1st to complete and attest to Acceptable Use Policy compliance. If the amount of compliance-related training is deemed too numerous to finish in one sitting, we can split the mandatory training up into manageable sections.

Employees will be notified by email with a reminder based on the following yearly schedule.

| **Notification** | **Date** |
| --- | --- |
| Initial security awareness training announcement with expectations and dates of availability and completion. | January 15th |
| An announcement that security awareness training is now available. | February 1st |
| Reminder sent to users that have not completed the security awareness training. | February 15th |
| Second Reminder to users that have not completed the security awareness training. | February 21st |
| Notice that training was not completed on time and that immediate supervisors have will be notified. They are advised to complete the training as soon as possible. | March 1st |

In addition to the email notifications, posters advertising the security awareness training will be put up in mid-January in strategic places throughout or offices, such as break rooms, lunchrooms, and common areas.

## Reinforcement

The annual training described is excellent for compliance but is not sufficient for creating a lasting security culture. Key concepts must be continuously reinforced to affect the behavior change we want to see and measure. As our program matures, we will introduce advanced tiers of testing. Once an employee becomes proficient at our initial tests, we can start training them to identify more sophisticated threats.

**Phishing Campaign**: Email is the crucial component of how our employees communicate with our clients. The Security Awareness Program will start with a phishing campaign for all employees, including senior leadership, quarterly. This campaign simulates a generic email attack. Our plug-in to the email client will allow employees to report a phishing attempt. After the first year, phishing campaigns will be performed monthly. At this point, we will also determine whether more targeted campaigns are warranted and update the schedule accordingly. Any employees found to have clicked repeatedly on our phishing emails will first be referred for extra training. Subsequent repeat click violations will result in an email to their manager to discuss the issue.

| **Phishing Campaign – Phase 1** | **Schedule** | **Target Group** |
| --- | --- | --- |
| Campaign #1 | 2021 – Q3 | All employees |
| Campaign #2 | 2021 – Q4 | All employees |
| Campaign #3 | 2022 – Q1 | All employees |
| Campaign #4 | 2022 – Q2 | All employees |
| **Phishing Campaign – Phase 2** | **Schedule** | **Target Group** |
| Campaign #1 | 2022 – October | All employees |
| Campaign #2 | 2022 – November | All employees |
| Campaign #3 | 2022 – December | All employees |
| Campaign #4 | 2023 – January | All employees |
| Campaign #5 | 2023 – February | All employees |
| Campaign #6 | 2023 – March | All employees |
| Campaign #7 | 2023 – April | All employees |
| Campaign #8 | 2023 – May | All employees |
| Campaign #9 | 2023 – June | All employees |
| Campaign #10 | 2023 – July | All employees |
| Campaign #11 | 2023 – August | All employees |
| Campaign #12 | 2023 – September | All employees |

**Cybercafés (Lunch and Learn):** Once a month, a member of the Information Technology/Security team will act as the instructor and perform in-person and virtual lunch and learn branded as Cybercafés. The session will last 30 minutes to discuss specific information security topics relevant to our industry with real-world examples and current events.

The session will be limited to 30 people via RSVP, with lunch provided at the corporate office. Our branch locations will also be encouraged to host their own events following the same theme of the month. Each session will be broadcast via live webcast to employees at other sites, and a recording will be made available to the rest of the organization on our company’s Intranet. During this session, topics will be introduced by the instructor for the first 10 minutes. The next 10 minutes will split those in attendance into breakout groups with whiteboards to discuss things such as what the security risk was, how it was exploited, and how it could have been prevented. The final 10 minutes will consist of a group discussion about what users may have learned and how it could apply to their work and personal lives.

A survey will be made available to be completed within two weeks of the event that can be submitted online. A prize will be awarded each quarter for participants. This prize will be a $25 Amazon Gift Card.

## Branding

The Mattress & More Inc. corporate logo will be used for all branding in the first year of the Security Awareness Program. We will be coordinating with members of our Creative Services division and select team leaders to create a Security Awareness Program-specific branding that will be used in our emails and posters by the second year of the program.

# Metrics

Having quantifiable ways to measure behavior change is a crucial element to make sure our Security Awareness Program is on the right track. We must first create a new baseline of behaviors through metrics to understand how far our current program has taken us and which behaviors still need more attention. We can then analyze how those behaviors negatively impact the organization, what is our acceptable risk to those behaviors, and how to improve those behaviors to move the needle in a direction that improves our security posture.

Metrics are categorized as compliance or impact metrics. Compliance metrics are focused on proving that our organization is meeting compliance standards. Impact metrics measure the impact our security awareness program is having. Up to this point, our company has been focused on compliance metrics. We will also be introducing impact metrics with the goals being to measure how effective our implementation plan is and to guide us on either continuing with our objectives or if we need to adjust and reconsider how security awareness is communicated to our employees.

Listed below are the initial metrics we will be collecting in the first two years of the program. They are subject to change based on updated or new industry standards and government regulations with which we must comply.

## Security Awareness Training Completion

**What is Measured**: We will measure the number of employees who have completed the mandatory yearly Security Awareness training and those that have not.

**How it is Measured**: The learning management system used for delivering the computer-based training will keep track of all users that have completed all the modules that are required, including the date of completion.

**How Often it is Measured**: The information will be collected quarterly and combined at the end of the year. While we only need to report information once a year, collecting quarterly will allow us to take corrective action for groups or business areas where there could be a larger number of users not completing the training.

**Why It is Measured**: This is a compliance metric needed to comply with our many regulations and requirements.

## Phishing Campaign Clicks

**What is Measured**: We will measure the number of employees who click on a phishing email link sent as part of the phishing email campaign.

**How it is Measured**: The phishing campaign tool used for generating emails and campaign targets will track users that clicked on specially crafted links in the emails sent.

**How Often it is Measured**: This metric will be collected based on the deployment schedule. Two weeks will be given after the campaign commences before it is considered closed. In the first year, the metric will be collected every quarter. In the second year, the information will be gathered every month.

**Why It is Measured**: Our staff relies heavily on emails. Not only is it used for business communication, but it is extensively used to engage with our clients. While we have technical controls to reduce the number of malicious emails coming through, our employees need to be able to know how to detect suspicious emails and be able to report them. Falling victim to phishing emails could lead to stolen credentials, compromised systems, and tricking the user into providing information to unauthorized parties.

## Virus Reported

**What is Measured**: We will measure how many viruses our anti-virus and anti-malware software detects. We will also determine how many viruses were successfully able to infect our systems.

**How it is Measured**: Data will be collected by our anti-virus and anti-malware software. The data collected can measure detections by the system and by location. Successful infections will be tracked in our help desk ticketing system by our desktop support staff for desktops and laptops and by IT system administrators for server systems.

**How Often it is Measured**: The data will be collected every week and reported monthly.

**Why It is Measured**: For our staff to perform their duties effectively, they have broader freedom in their ability to conduct research on the internet. It increases the probability of infection by unknowingly and unintentionally visiting malicious sites that will download viruses and malware. Having a knowledgeable and security-aware staff should lead to the number of viruses detected as they will be able to identify suspicious sites before visiting. It is an important metric to capture even with no infection. Confirmed infections are essential to measure since not all malicious files can be detected. The cost to eradicate them is real and measurable in lost productivity hours by staff and IT personnel.

# Appendices

## Learning Objectives

The purpose of learning objectives is to give the security awareness program a method to measure behavior change by breaking down our human risks into manageable and identifiable pieces of knowledge our employees should possess. It allows us to reduce specific risks and have a way to measure our employee’s ability to identify them and follow the appropriate procedures.

**Title**: Managing Sensitive Data

**Target Audience**: All employees, with special consideration given for our financial, management, and human resources departments.

**Goal**: Employees should be able to identify all types of data they come across as part of their day-to-day activities, including identifying credit card data, PII, HIPAA protected data, and confidential company information, know-how to securely access the data, where it should be stored, and how to transmit the data securely to authorized persons.

**Background**: To perform their duties, most of our employees have access to sensitive information of one kind or another. They are authorized to use this information to process payments for services and products, insurance claims, orders to vendors, and producing goods on the factory floor. This puts tremendous trust in our employees. Any unauthorized disclosure of this information, whether intentional or not, could lead to regulatory fines, contractual penalties, and loss of reputation, which could result in loss of current and future business.

**Applicable Human Risk**: Employees who must have access to sensitive data.

**Learning Objective 1**: Employees can identify the different types of sensitive data.

* *Individual Metric*: Employee correctly identifies data elements that are considered sensitive data in a quiz that is part of the annual Security Awareness Training CBT.
* *Organizational Metric*: Collection of number of users that correctly identified data elements considered sensitive data in a quiz that is part of the annual Security Awareness Training CBT

**Learning Objective 2**: Employees can identify authorized software and systems that can store sensitive data.

* *Individual Metric*: Employees can identify appropriate software and systems that can store sensitive data in a quiz that is part of the annual Security Awareness Training CBT.
* *Organizational Metric*: Data loss prevention software configured to detect sensitive data will track where this information is stored without divulging the data itself.

**Learning Objective 3**: Employees can demonstrate how to transmit sensitive data securely.

* *Individual Metric*: Employees are asked to demonstrate how to use the MMFTP internal secure file-transfer service.
* *Organizational Metric*: The email firewall configuration tracks sensitive data transmitted in an email. The email firewall will track the number of occurrences it has detected and blocked such emails.