Security Awareness Maturity Model

- Non-Existent
- Compliance Focused
- Promoting Awareness & Behavior Change
- Long Term Sustainment & Culture Change
- Metrics Framework

SANS - Securing the Human
### Defining Variables of Risk

An incident is any type of security event that causes harm to your organization. An incident is not limited to just deliberate attacks by cyber attackers, but can also be the results of accidents by employees, contractors or other trusted 3rd parties.

<table>
<thead>
<tr>
<th>Probability</th>
<th>Impact/Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Very High</strong> (5)</td>
<td>95% or greater chance of happening in next six months.</td>
</tr>
<tr>
<td><strong>High</strong> (4)</td>
<td>1. Loss of life or permanent loss from work.</td>
</tr>
<tr>
<td></td>
<td>2. Executive leadership must report to congress for public hearings.</td>
</tr>
<tr>
<td></td>
<td>3. Permanent negative reputational damage.</td>
</tr>
<tr>
<td></td>
<td>4. Shutdown of operations for more than 5 days.</td>
</tr>
<tr>
<td><strong>Medium</strong> (3)</td>
<td>1. Critical employee injury, 1 month or more lost from work.</td>
</tr>
<tr>
<td></td>
<td>2. Financial loss of $1 million - $10 million.</td>
</tr>
<tr>
<td></td>
<td>3. Leadership directly involved in legal proceedings.</td>
</tr>
<tr>
<td></td>
<td>4. Long-term negative reputational impact and public exposure.</td>
</tr>
<tr>
<td></td>
<td>5. Shutdown of operations for 1-5 days.</td>
</tr>
<tr>
<td><strong>Low</strong> (2)</td>
<td>1. Severe employee injury, 1 week to 1 month time lost from work.</td>
</tr>
<tr>
<td></td>
<td>2. Financial loss of $100,000 - $1 million.</td>
</tr>
<tr>
<td></td>
<td>3. Leadership directly involved in legal proceedings.</td>
</tr>
<tr>
<td></td>
<td>4. Serious negative reputational impact and public exposure.</td>
</tr>
<tr>
<td></td>
<td>5. Shutdown of operations for 1 day.</td>
</tr>
<tr>
<td><strong>Very Low</strong> (1)</td>
<td>1. Minor employee injury, no time lost from work.</td>
</tr>
<tr>
<td></td>
<td>2. Financial loss of $10,000 or less.</td>
</tr>
<tr>
<td></td>
<td>3. Minimal to no legal involvement.</td>
</tr>
<tr>
<td></td>
<td>4. Minimal to no negative reputational impact and public exposure.</td>
</tr>
<tr>
<td></td>
<td>5. Shutdown of operations for less than an hour.</td>
</tr>
</tbody>
</table>

#### Defining Variables of Risk

The probability you will have an incident is determined by two variables; Vulnerabilities x Threats. The more vulnerabilities you have, and/or the more threats you have and/or the more motivated they are, the more likely you will have an incident. To determine probability, work with people such as your Security Operations Center, Help Desk, Human Resources or Incident.

To determine the harm a certain incident can cause, work with the business owners that would be impacted.
<table>
<thead>
<tr>
<th>Human Risks/Topics</th>
<th>Probability</th>
<th>Impact</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example Risk</td>
<td>Very High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Example Risk</td>
<td>5</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>You Are the Shield</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Engineering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email and Messaging</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browsing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Networking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Device Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passwords</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Working Remotely</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Targeted Attacks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creating a Cyber Secure Home</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacked</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* For the descriptions of each topic, refer to the Topic Descriptions page in your lab workbook.
* To help you define probability and impact, refer to the Risk Definitions page in your lab workbook.
Security Awareness Module Descriptions

You Are the Shield
Employees often believe they are not a target, which exposes your organization to tremendous risk. This module addresses this misconception by explaining how and why they are under attack. In addition, we explain that this training not only protects them at work, but also at home. This engages people and helps ensure the success of your organization’s security awareness program.

Social Engineering
Many of today’s most common cyber attacks are based on social engineering. As such, this module explains what social engineering is, how attackers fool people, and what to look for. We then demonstrate a common social engineering attack. We finish with how people can detect these attacks and how to respond to them.

E-mail and Messaging
One of the primary means of attack and exploitation is through e-mail. E-mail is used for both simple, large-scale attacks and more targeted spear phishing attacks. We explain how these attacks work, including recent examples of phishing, spear phishing, malicious attachments, and links and other scams. We then explain how to detect and stop these attacks.

Browsing
The browser has become the gateway to the Internet; it is the primary tool that employees use for online activity. As such, browsers and their plugins have become a common target for attackers. We teach people how to browse safely, including keeping the browser and plugins updated, avoiding bad neighborhoods and being careful of and scanning what they download.

Social Networking
Sites such as Facebook, Twitter, and LinkedIn have exploded in popularity, with employees and managers posting all sorts of private information, not only about themselves but also about their work. Cyber attackers know this and use this information for identity theft, spreading malware, scams, and even targeted attacks. We discuss these risks and the steps your employees can take to protect themselves and your organization.

Mobile Device Security
Today’s mobile devices (such as tablets and smartphones) are extremely powerful. In most cases, these devices have the same functionality, complexity, and risks of a computer, but with the additional risk of being highly mobile and easy to lose. We cover how to use mobile devices safely and how to protect the data on them.

Passwords
Passwords are the keys to the kingdom and employees must guard them well. 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 different passwords, password managers, and not sharing passwords with others.
Malware
An overview of what malware is, how it works and two common examples. We focus on the fact that technology alone cannot stop malware, instead people need to also be security aware and exhibit secure behaviors to protect systems from becoming infected.

Data Security
Organizations have a tremendous amount of sensitive information that they must take extra steps to protect. This module explains these steps, including using only authorized systems to store or process sensitive information, restrictions on transferring or sharing such information, and requirements for securely disposing of sensitive data.

Working Remotely
For many organizations, employees are no longer working at the office. Instead, they work from home or on the road while traveling. Because organizations no longer have physical control of the user’s work environment, there are unique risks. This module focuses on how these employees can protect themselves, including laptop security and creating a secure, mobile working environment.

Cloud
The cloud is a powerful tool that enables your employees to increase their productivity while reducing organizational costs. But it also comes with tremendous risks, including how organizational data is stored and shared with others. This module explains these risks to employees and shows them how to safely use authorized cloud providers in your organization.

Targeted Attacks
Targeted attacks such as APT or CEO Fraud is not an individual acting on his own, but trained professional targeting your organization. This module explains what targeted attacks are, how they operate, and how your employees can detect and protect against these dangerous cyber threats.

Physical Security
Although physical attacks against your data are less likely to happen than cyber attacks, they can have a much greater impact on your organization when they do. In this module we explain how attackers attempt to trick and fool their way into restricted areas. We also discuss how employees can protect the physical security of your facilities.

Creating a Cyber Secure Home
Security is not just an issue at work, but at home. This module covers steps people can take to protect their home networks, including their personal devices and Wi-Fi network. By building good security behaviors at home, people are more likely to use them in your organization.

Hacked
No matter how effective a security team and its processes are, there will be incidents. This module focuses on how employees can help by identifying and reporting an incident. We cover things to look for, such as suspicious activity or virus alerts and whom to report an incident to.
Learning Objectives: Mobile Device Security
1. Module Learning Objectives

The purpose of this document is to identify and document the learning objectives of this training module. This information determines the contents of the training module, regardless of how it is communicated.

Title: Mobile Device Security

Target Audience

All organization employees and contractors who use a mobile device for work purposes are the target audience. These individuals are assumed to be nontechnical.

Goal

Course participants will learn the need for and will be able to explain and demonstrate how to secure their work or personal mobile devices. The decisions people make as a result of this training will lower both organizational and personal risk when using mobile technology.

Background

Mobile devices have become one of the primary ways people communicate and interact with information, both for personal life and work. However, with such small and powerful devices comes unique risks and dangers. This module teaches the steps individuals can take to safely use mobile devices.

Learning Objectives

1. Learners can explain the need for strong authentication on mobile devices, the different types of mobile device authentication, and demonstrate how to enable strong authentication on their mobile devices.
   a. Individual Metric: Learner correctly identifies or matches the strong authentication method in a test question or interactive training session.
   b. Organizational Metric: A sampling of mobile devices demonstrates that a certain percentage of mobile devices have some type of approved authentication enabled.

2. Learners can explain the need for downloading apps from only trusted sources as well as distinguish trusted versus untrusted sources.
   a. Individual Metric: Learner correctly identifies or matches the trusted versus untrusted sources for downloading mobile apps in a test question or interactive training session.
b. **Organizational Metric**: A sampling of mobile devices shows that less than a certain percentage is infected due to malicious apps.

c. **Organizational Metric**: Send a phishing email inviting people to download and install a certain mobile app.

3. Learners can explain the reason for backing up their mobile devices, explain how to do it, and do so on at least a monthly basis.
   
a. **Individual Metric**: Learner correctly identifies or matches the reason for backing up a mobile in a test question or interactive training session.

b. **Organizational Metric**: A sampling of mobile devices shows that a certain percentage of mobile devices were backed up in the past 30 days.

4. Learners can explain the security need to run the latest version of their mobile device operating system and mobile apps.
   
a. **Individual Metric**: Learner correctly identifies or matches the reason for updating mobile devices and apps in a test question or interactive training session.

b. **Organizational Metric**: A sampling of mobile devices shows a certain percentage of mobile devices are running the latest version of the operating system approved by their organization and all apps are configured to automatically update.

5. Learners explain the risks involved with jailbreaking or rooting and do not jailbreak or root their mobile devices.
   
a. **Individual Metric**: Learner correctly identifies or matches the risks of jailbreaking or rooting mobile devices in a test question or interactive training session.

b. **Organizational Metric**: A sampling of mobile devices shows that less than a certain percentage of mobile devices have been jailbroken or rooted.

6. Learners can identify the different indicators of an attack in a text message or an SMS attack.
   
a. **Individual Metric**: Learner correctly identifies or matches the indicators of an attack in a test question or interactive training session.

b. **Organizational Metric**: Less than a certain percentage fall victim to an SMS or a mobile text messaging phishing assessment (sometimes called smishing).
7. Learners know they may not access organization data or e-mail with a personal mobile device unless they have prior authorization.

   a. **Individual Metric:** Learner signs the organization Acceptable Use Policy and correctly identifies or matches the correct answer in a test question or interactive training session.

   b. **Organizational Metric:** A sampling of mobile devices shows that at least a certain percentage of personal mobile devices do not have any work-related data. Those that do must have proper security organization software and approval of their supervisor.

8. Learners can explain how to report a lost, infected, or stolen mobile device issued by work and whom to contact.

   a. **Individual Metric:** Learner correctly identifies or matches the proper reporting method in a test question or interactive training session.

   b. **Organizational Metric:** When surveyed, a certain percentage of people can explain proper reporting procedures.
LAB – WHAT: Defining Learning Objectives

The purpose of this lab is to develop your skills at creating Learning Objectives. Select a topic from your previous lab (note: it can’t be passwords or mobile devices as we already covered the Learning Objectives for them). Then complete the document below for that topic. For the actual Learning Objectives, identify and document three of them. Be sure they are specific and measurable. Avoid verbs like “know” and “understand” as they are vague and difficult to measure. Instead use action verbs like “demonstrate”, “identify” or “explain” as they are easier to measure. The more specific the Learning Objectives, the more likely you will be successful in changing and measuring them.

Title:

Target Audience:

Goal:

Background:

Learning Objectives:
LAB – Metrics: Defining Your Top Three Impact Metrics

Identify and define your top three impact metrics, how you would measure them and why you selected them. Oh, and it can’t be phishing.

First Metric

• What is the metric?

• How will you measure it and how often?

• Why did you select this metric?

Second Metric

• What is the metric?

• How will you measure it and how often?

• Why did you select this metric?
Third Metric

- What is the metric?

- How will you measure it and how often?

- Why did you select this metric?
LAB2-R04: Achieving and Measuring Success with the Security Awareness Maturity Model

Post-Conference Summary

Lance Spitzner
Director, SANS Securing the Human
@lspitzner
# Table of Contents

**INTRODUCTION** .................................................................................................................................................. 3  
  Thanks for attending! ........................................................................................................................................ 3

**LAB SUMMARY** .................................................................................................................................................. 4  
  The Security Awareness Maturity Model ........................................................................................................ 4  
  Creating a Plan .................................................................................................................................................. 5
  **WHAT:** Prioritizing Your Behaviors ........................................................................................................ 5  
  Measuring Your Behaviors .............................................................................................................................. 6

**FURTHER RESOURCES** ........................................................................................................................................ 7
Introduction

Thanks for attending!

I know just how busy RSA Conference can be. With over 700 talks you had a huge number of options. I’m thrilled and honored that you picked this Lab as one of your choices. It not only shows your interest in what I feel is one of the fastest growing fields in cyber security, but it demonstrates your trust. I hope you found it as engaging and educational as I did, and that the Lab provided you everything you hoped it would.

This summary is designed to recap key discussion points and topics that made up our time together in the Learning Lab. In addition, I provide resources where you can learn more and further your education. The challenges of security training, awareness and culture are complex and varied, and as you saw in the two hours we had was barely enough to scratch the surface. Everyone should be proud of the work we did at the conference, and I hope that the rest of your RSA Conference experience was as rewarding for you as collaborating on this Lab was for me.
Lab Summary

The goal of the two-hour Lab was to introduce you to the Security Awareness Maturity Model. Specifically what the model is, how to leverage the model in establishing a mature awareness program and finally the ability to measure your program.

The Security Awareness Maturity Model

This model was created through a consensus effort of over 200 security awareness officers six years ago. The model enables you to not only visualize where your program is and where you want to take it, but provides a roadmap on how to achieve your goal. In addition, all attendees were provided a copy of the Security Awareness Roadmap poster, which details each stage of the model and the steps to achieve them. A key point in building awareness programs is we cannot tell you how to build your program, every organization is too unique. Instead by leveraging the model we provide a path, a series of questions, and by answering those questions you build your plan.
Creating a Plan

To build a mature awareness program you need a plan. A common indicator of an immature awareness program (often in the compliance stage) is there is no plan. Instead random topics are picked on an ad-hoc basis and presented a couple times a year. To establish a truly mature awareness program you need a long term strategy, and to achieve that you need to answer three key questions.

- **WHO**: Whose behaviors are you attempting to change.
- **WHAT**: What behaviors are you attempting to change. This is the question we focus on in the Lab, as the WHAT part you teach also drives what you will measure for metrics.
- **HOW**: How will you change those behaviors (key element is communications)

Due to the time limitation of the Lab, we only focused on the second question. One of the questions we received in the Lab is what about answering the question WHY. WHY is a critical part of HOW. In order to effectively engage people, you have to first explain to them WHY cyber security is important. The most effective awareness programs engage people at an emotional level. However, due to time limitations we were not able to cover that. To learn more about consider attending the SANS MGT433 course, covered in the Learning More section.

**WHAT: Prioritizing Your Behaviors**

A key element of a mature awareness program is focusing on as few behaviors as possible. Not only does every security behavior have a cost to both the employee and your organization, but people can only remember so much before they hit what is called *cognitive overload*. This is where they are so overwhelmed with information they simply forget it all. This is a common failure of awareness programs as security teams want to mitigate all risk, so they try teaching as many behaviors as possible. This does not work. Ultimately, you should have a compelling reason for every behavior you teach. By focusing on only a few key, high impact behaviors you are far more likely to change behavior and have an impact. This requires you to conduct a human risk analysis to determine your top human risks. We did this as part of our first lab using a qualitative risk analysis. As part of Lab groups, you were required to prioritize your 9 top human risks out of a list of 18.

However, as we explained in the session, identifying your top human risks is only half the battle. After identifying your top human risks, you then had to identify and document the top behaviors that manage those risks. This is a commonly ignored or forgotten step. As an example of this process we used passwords. Passwords are a common human risk that many organizations cover in their awareness program, but often do it wrong by overwhelming employees with confusing, complex and inefficient behaviors. We covered how this topic could be vastly simplified, with the end result of more likely changing behavior AND effectively managing risk. We then covered how these behaviors are documented in the Learning Objectives document. As a final lab you were required to pick your own top human risk and then create a Learning Objectives document for that risk identifying all the key behaviors.
Measuring Your Behaviors

I’m often asked by people what they should measure in their awareness program. This is the wrong question. The question every organization should ask themselves is what behaviors do you care about the most, what behaviors will manage the greatest amount of risk? Once you have identified and prioritized your key behaviors you in essence have your metrics program. That is why we completed the WHAT process first. This is also why the Learning Objectives document is so important. Each document lists all the behaviors used to manage that specific human risk. These behaviors drive your metrics. Some of the key takeaways for an effective metrics program include:

- Do not ask what you should measure, but start with what behaviors you care most about. That should drive your metrics program.
- Focus on only a few, key metrics, the ones most useful for you. A common mistake is using too many metrics that can be distracting and/or waste your time.
- The biggest difference between human metrics and most other security metric programs is that we are measuring people, and people have emotions. This is where most awareness programs go wrong. You want an assessment program that people are not threatened or insulted by. If done correctly, any type of metrics program can become gamified, where people perceive it as a friendly competition or learning experience. This means do not do a wall of shame, send out Viagra phishing emails or try to trick people with advanced social engineering tests. Instead focus on common, real world attacks.
- Make heroes out of people who do the right thing. Not only is recognition a huge motivator, but hero stories help reinforce the key behaviors you do want people to do.

Awareness programs are an extremely effective way to manage human risk. You can and will change behavior and ultimately your organization’s culture, however, you need to have an effective long-term strategy to accomplish that, which that is why the Security Awareness Maturity Model is so powerful. It provides the roadmap to success.
Further Resources

Our journey in securing people is only beginning, we all have a tremendous amount to learn as a community. Here are some resources to help you down that path.

**Lab Handouts**: These are the handouts from the Lab. Additional handouts are also included, which you can learn more about in the SANS MGT433 course.

**SANS MGT433 Course**: Two day course on building a mature security awareness program. This course is taught by Lance Spitzner multiple times a year all over the world.

**Security Awareness Summit**: Held 2/3 August in Nashville, TN with over 200 security awareness officers and industry leaders from around the world sharing lessons learned and resources on creating mature awareness programs.

**Security Awareness Roadmap Poster**: Have the Roadmap poster shipped to your organization to hang in your office as a reference.

**BJ Fogg’s Behavior Course**: Private boot camp led by Dr. BJ Fogg on behavioral change. Limited to 10 people, he hosts the class at his home in California.

**Leading Change by John Kotter**: The book / industry standard on change management. Surprisingly easy to read yet extremely informative.

**Made To Stick by Chip and Dan Heath**: This book is becoming the industry standard for security awareness officers on effective engagement and communication.