Planning and Execution of an Effective Security Awareness Program

Experience

- Project Management
- Cybersecurity Degree
- ISO @ Texas Facilities Commission
- Security Program at Alamo Colleges

Martha Smith, Information Security Officer
Texas Facilities Commission
martha.smith@tfc.state.tx.us

Outline – Questions Answered

- What is a Security Awareness Program and why is it important?
- Do I need Buy-in?
- Who is part of the Program?
- What is part of the Program?
- How do we implement the program?
- How do we get the word out?
- Organizational Presence
- Metrics and Reporting
- Marketing

What is a Security Awareness Program and why is it important?

A Security Awareness Program is not just about training

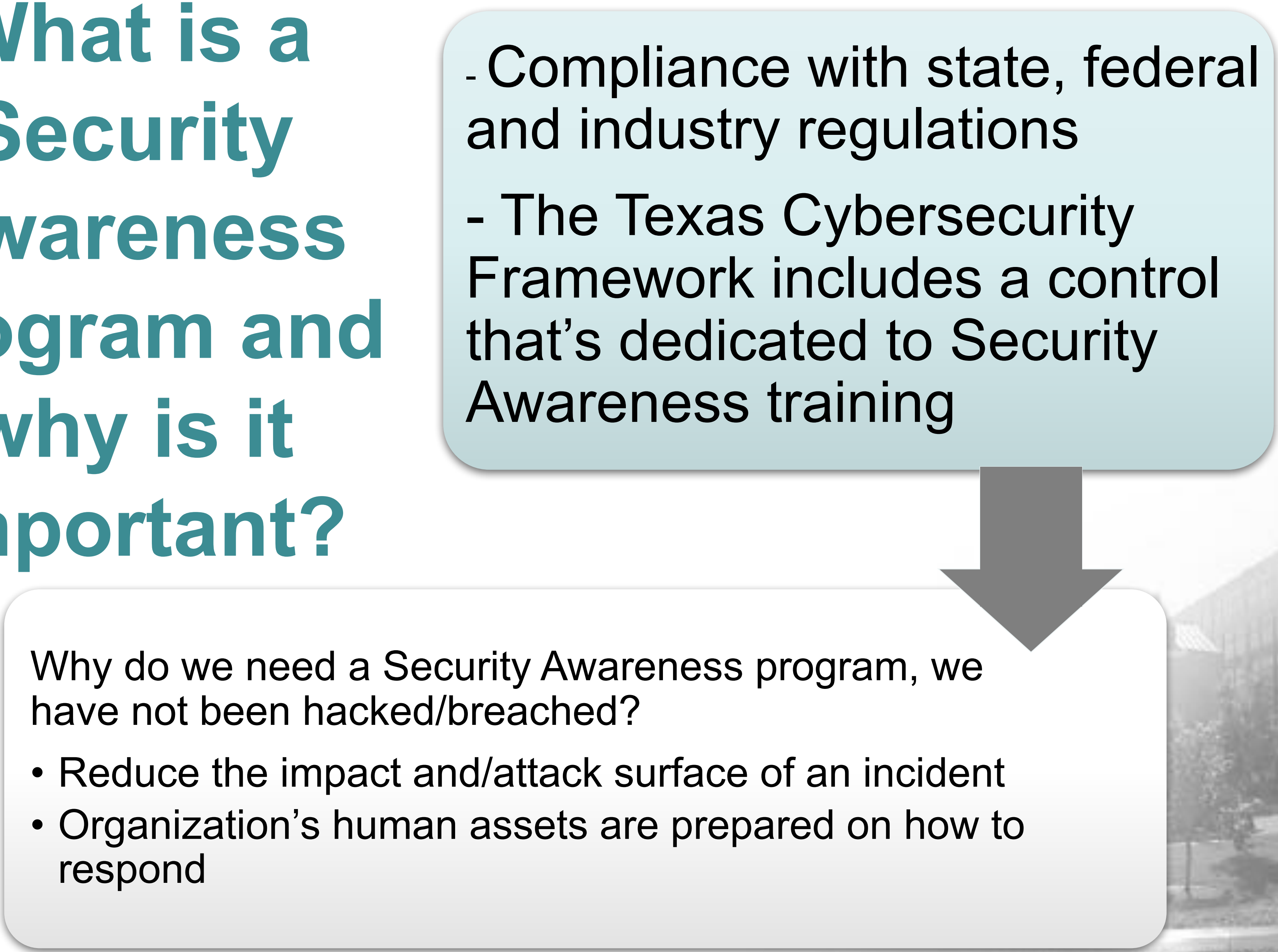
- It's about being security aware while doing business
- It's how we engage online
- It's how we exchange information

- Our users get better at protecting our organization from the inside out by being cognizant of what to look for in phishing attempts
- Our users are our first line of defense
- They notice anomalies before technical tools

Lesson Learned

- Most don’t know what Security Awareness looks like
- Users don’t realize the value of data
- Users are hyper-curious
- You don’t want to impart the “Big brother is watching”
- You have to make it personal
- I’m am the first ISO at my agency

What is a Security Awareness Program and why is it important?



- Compliance with state, federal and industry regulations

- The Texas Cybersecurity Framework includes a control that’s dedicated to Security Awareness training

Why do we need a Security Awareness program, we have not been hacked/breached?

- Reduce the impact and/attack surface of an incident
- Organization’s human assets are prepared on how to respond

Lesson Learned

- Sensitive data can reside in public domains
- Data can cross contaminate to other servers – Reduce the attack surface
- Don’t want to figure out how to respond to incidents when you have an incident

Buy-in

Security Awareness is **NOT** an IT initiative

- Everyone shares the responsibility
- Establish C-level support
- If it’s important to C-level staff others will follow
- Come prepared with Strategy/Vision

Lesson Learned

- Users should not feel like IT is happening to them, collaborate with HR on delivery,
- If it's important to C-level staff, others will follow
- Strategy should show real data/metrics

Champions Why they are even **more** important?

- They can speak about the program and the importance to their department's role in effecting change (it just takes one person to start the momentum)
- They can assist in the delivery of what Security Awareness means to their day to day operations
- Should include partners from various functional business units: Finance, HR, IT, Operations, etc.
- *It's not a siloed endeavor*

Lesson Learned

- Security Council
- Educating users on things that are relevant to their personal space

[redacted]

Who should be part of the Program

- Employees
- Any one who has access to your organization’s IT resources and/or data assets
- Contractors and/or Third Parties (think Target) https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
- Board of Directors, Commissions, etc.

Lesson Learned

- Contractors represent a large number of our user base
- Remote users are in systems after hours
- If there’s a compromise, who you gonna call?

Okay, I’ve gotten approval from C-Level and I have partners…now what?

High Impact Initiatives:

- CBT on subjects that are currently relevant such as Phishing
- Tools to complement training
  - Wombat or other type product that provides a vantage point
- Be a resource :Create a reporting mechanism to make it easy for users to report such as a web presence where users can **easily** find information (standards, guidelines, etc.)
- Presentations to departments specific to their business units
  - How they handle data and how it aligns with Organization’s guidelines and standards

Lesson Learned

CBT Training

Should have a start and an end date
Must be Interesting
Must be relevant
Must be short and sweet (from 45 → 24)

Things that must be in place

- Train the IT Helpdesk on how issues will be addressed/answered (SME)
- Delivery of training
- New Hires (that start after the compliance start period)
- People that move
- Report Frequency Beginning: once a month, End: twice/monthly

Marketing: How to get the word out (it’s an ongoing endeavor)

- Cardstock to highlight frequently asked questions such as password guidelines, etc.
- Computer based training
- Posters (people love posters, make them fun)
- https://free.thesecurityawarenesscompany.com/downloads/category/videos/page/2/
- Be your own organization’s vendor at functions

Lesson Learned

Face to Face

If your agency is decentralized, making those connections are especially important

October Security Awareness Month

Make it a point to educate what OSAM is about

Organization Presence

Dedicate a webpage on your Portal/Intranet for users to get quick answers to:

- Launching pad to current initiatives
- Find policy, guidelines and standards
- Security Forms for provisioning
- Security-centric information
- How -Tos
- More importantly: Create a brand for Information Security

Lesson Learned

SharePoint or other Portal application

- One repository for information
- Users only have to remember one URL
- Make it Security-centric
- Use the site to further educate users

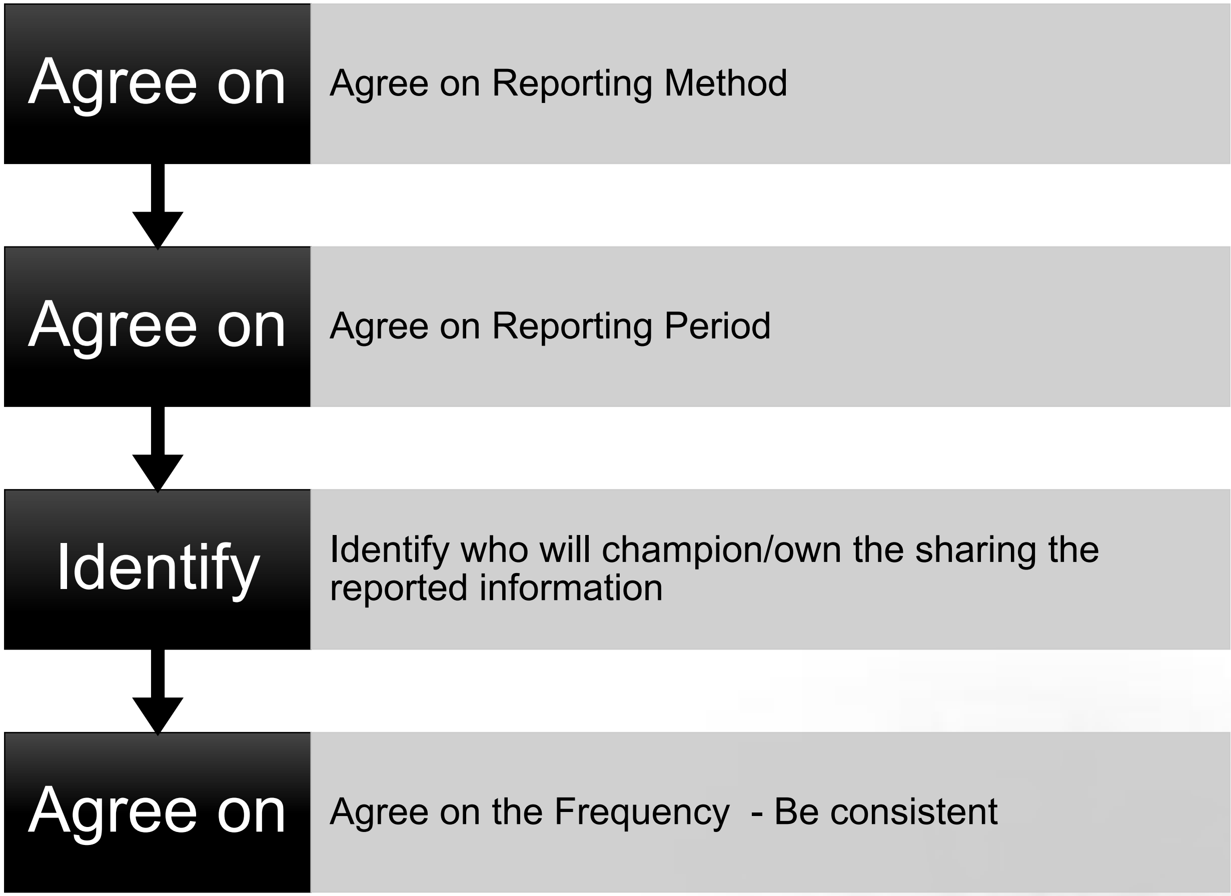
Metrics and Reporting

(In order to create a metric, you need a baseline to determine the efficacy of your program)

Baselines can provide you with where to start with your initiative

- Can be a manual endeavor (number of suspicious emails being reported today – this is a starting point)
- Work with partners to find out how many of their users are encryption when data sharing with external entities
  - Defer them to the How-To on your Information Security Webpage
- Take a sample of how many users know how often their password must change

Metrics and Reporting



Agree on

Agree on Reporting Method

Agree on

Agree on Reporting Period

Identify

Identify who will champion/own the sharing the reported information

Agree on

Agree on the Frequency - Be consistent

Lesson Learned

Accuracy is very important

- Departments take ownership and if reports are inaccurate, they lose confidence in their effort
- Make the reporting look the same across all departments
- Consistency – if you promise to send reports every 2 weeks/monthly – keep your word

Questions

Martha Smith, Information Security Officer
Texas Facilities Commission
martha.smith@tfc.state.tx.us
512-463-8695