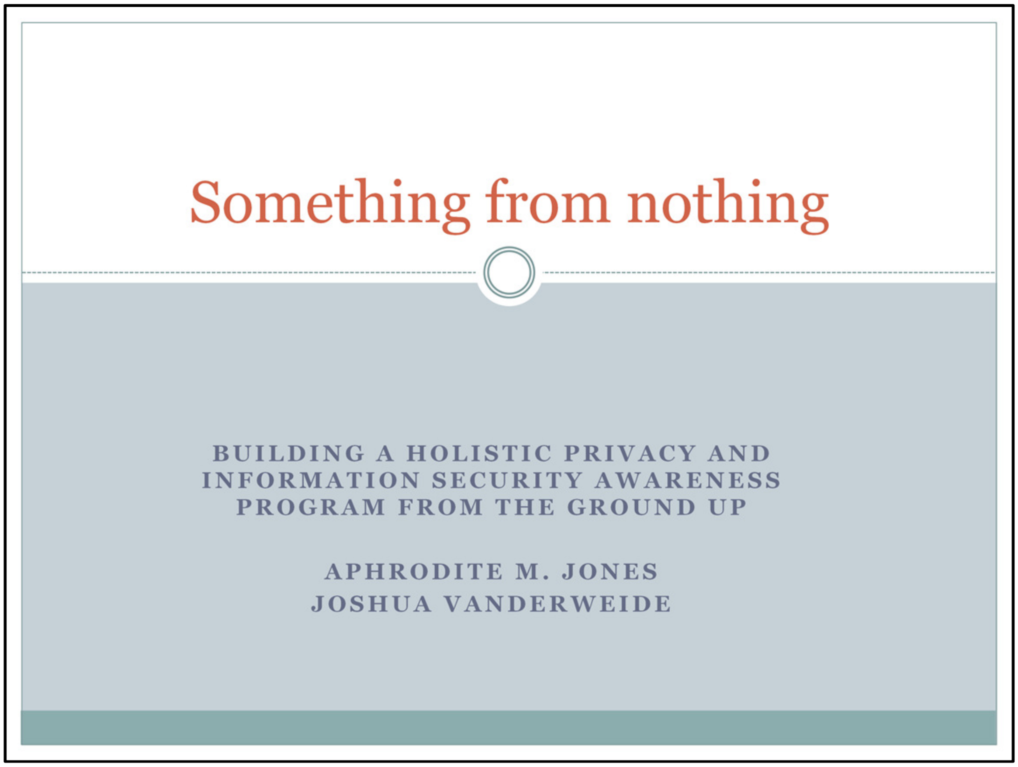
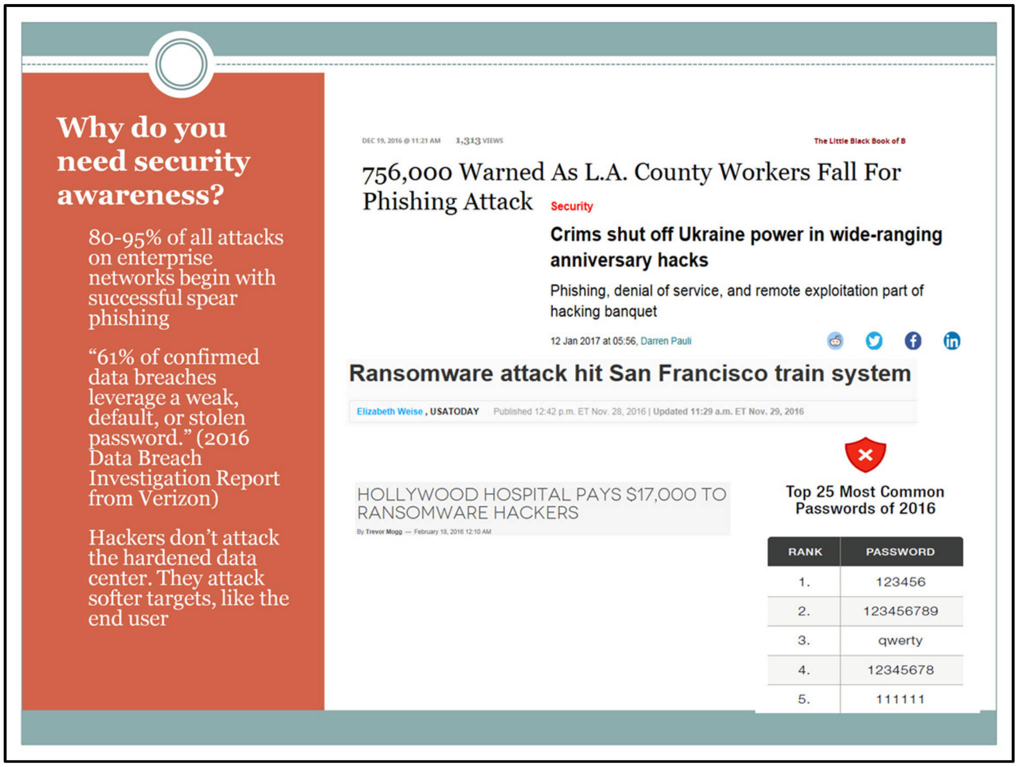


Something from nothing

BUILDING A HOLISTIC PRIVACY AND INFORMATION SECURITY AWARENESS PROGRAM FROM THE GROUND UP

APHRODITE M. JONES
JOSHUA VANDERWEIDE



Why do you need security awareness?

80-95% of all attacks on enterprise networks begin with successful spear phishing

"61% of confirmed data breaches leverage a weak, default, or stolen password." (2016 Data Breach Investigation Report from Verizon)

Hackers don't attack the hardened data center. They attack softer targets, like the end user

DEC 19, 2016 @ 11:21 AM 1,313 VIEWS The Little Black Book of B

756,000 Warned As L.A. County Workers Fall For Phishing Attack

Security

Crims shut off Ukraine power in wide-ranging anniversary hacks

Phishing, denial of service, and remote exploitation part of hacking banquet

12 Jan 2017 at 05:56, Darren Pauli

Ransomware attack hit San Francisco train system

Elizabeth Weise , USATODAY Published 12:42 p.m. ET Nov. 28, 2016 | Updated 11:29 a.m. ET Nov. 29, 2016

HOLLYWOOD HOSPITAL PAYS $17,000 TO RANSOMWARE HACKERS

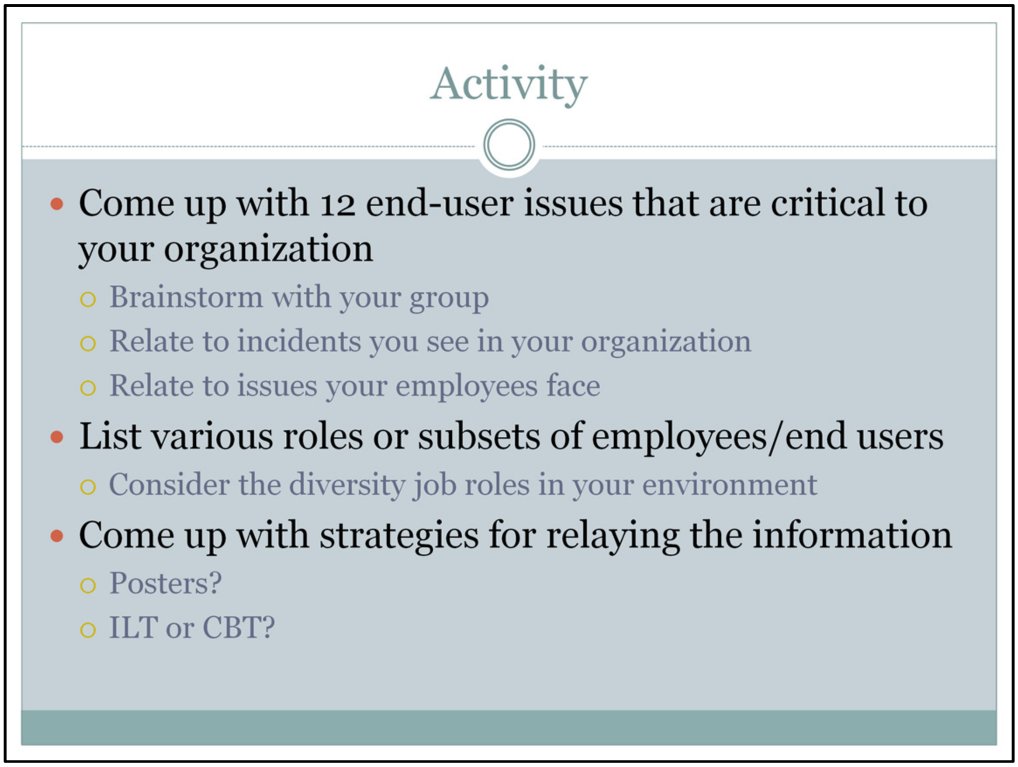
By Trevor Mogg — February 18, 2016 12:10 AM

Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111

We see news articles all the time about organizations that were impacted by cybersecurity issues. Most of these issues begin at the end user with successful spear phishing. From there, they leverage weak or compromised passwords to access the system further. The value in security awareness lies in preventing these issues, and continuing to harden your vulnerable surface.

We start every instructor led presentation with a new story relevant to the current audience (or role) to make a quick impact on the audience and get their attention and explain the "why" are we learning this.



Activity

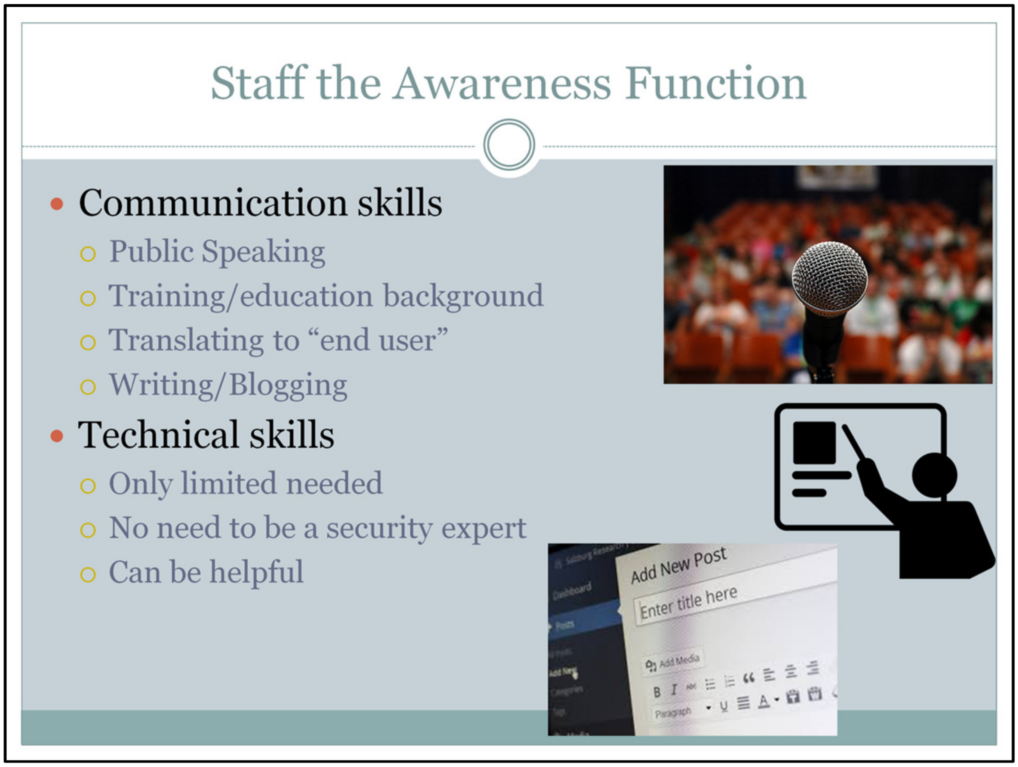
- Come up with 12 end-user issues that are critical to your organization
  - Brainstorm with your group
  - Relate to incidents you see in your organization
  - Relate to issues your employees face
- List various roles or subsets of employees/end users
  - Consider the diversity job roles in your environment
- Come up with strategies for relaying the information
  - Posters?
  - ILT or CBT?

It’s important to understand the organizations threats.

Then match the individual threats to the roles that are a possible risk for that threat

And understand the strategies for communication and training of the threats.

Where to begin?



Staff the Awareness Function

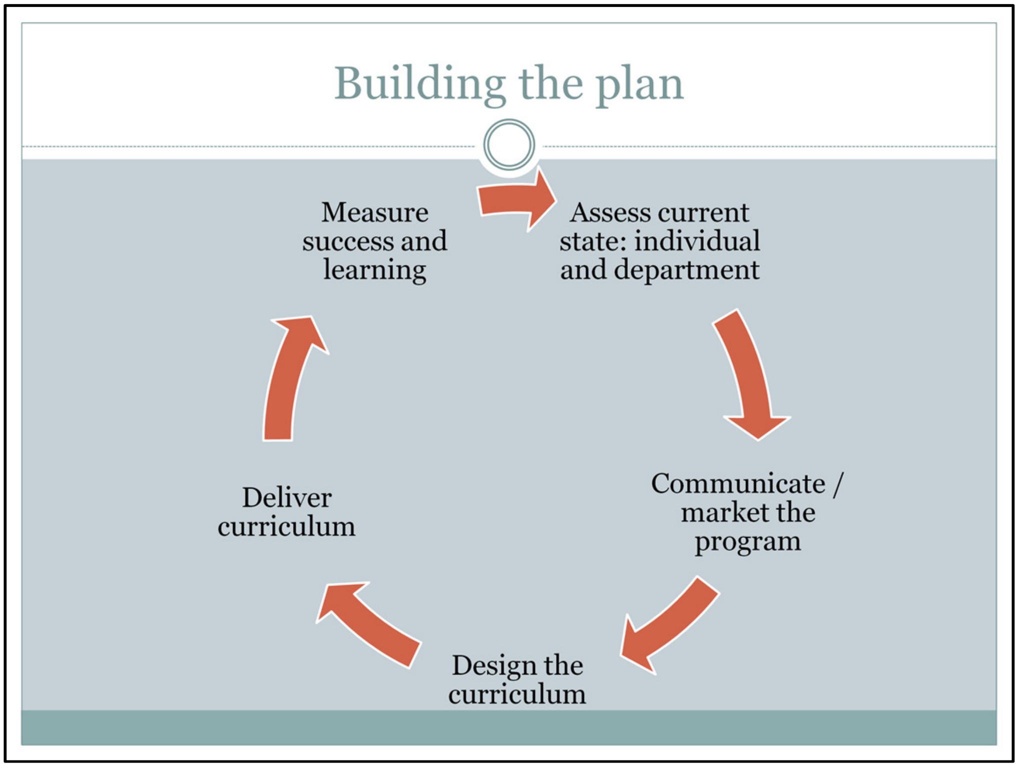
- Communication skills
  - Public Speaking
  - Training/education background
  - Translating to “end user”
  - Writing/Blogging
- Technical skills
  - Only limited needed
  - No need to be a security expert
  - Can be helpful

Add New Post
Enter title here
Add Media
Paragraph

When filling the position, first consider the cost in relation to time. Having an individual to focus on this allows your engineers, analysists, and leadership to utilize their skillsets appropriately and allows the organization to get the most out of the hourly expense they invest in those individuals. It’s all about Return on Investment (ROI).

The person selected to operate the awareness function must have communication skills. They will need to be able to communicate with various departments and employees at various levels of the organization. They will need to be **comfortable and capable of public speaking as well as composing written communications**. They must also be able to translate high level security concepts to simple and digestible nuggets that the end user can understand.

Technical skills/knowledge, particularly those required to be a security engineer, are not necessary and may even be a hindrance when communicating with the end users. They should have enough knowledge to be able to extract the relevant information from the security space without bogging the end user down with details.



Building the plan

Assess current state: individual and department

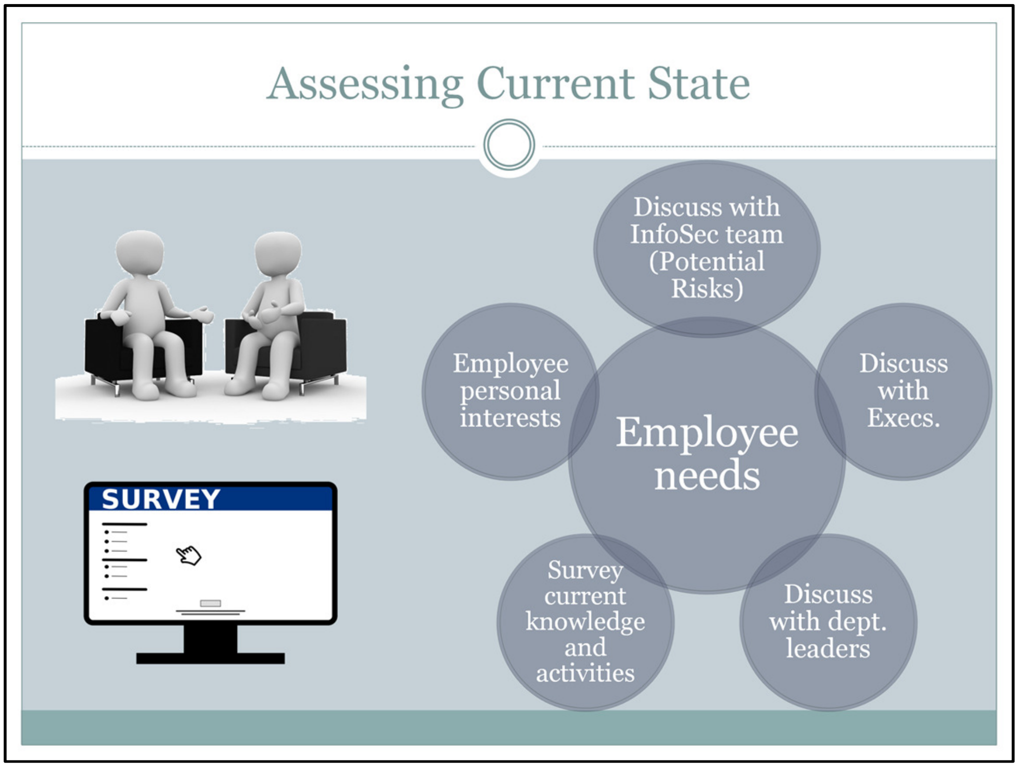
Communicate / market the program

Design the curriculum

Deliver curriculum

Measure success and learning

When you build your plan, consider it a cyclical process. Begin by assessing the current state of awareness efforts. Evaluate at the individual, departmental, and organizational level. Gather a baseline for your organization and discover the needs that your program will address. Next you will need to lay out how to communicate your plan to your organization. Design the curriculum based around the needs you discovered, and deliver in a manner that is meaningful to the end users. After deploying content, measure the success and value in order to inform further iterations of your program.



Assessing Current State

Discuss with InfoSec team (Potential Risks)

Employee personal interests

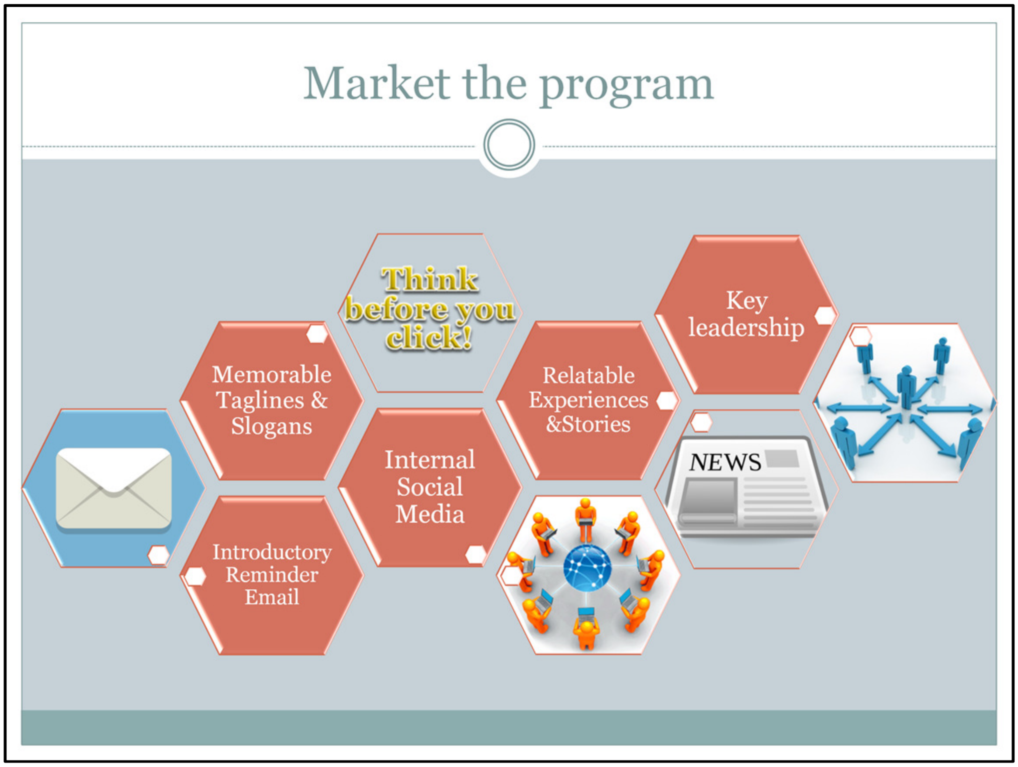
Employee needs

Discuss with Execs.

Survey current knowledge and activities

Discuss with dept. leaders

When assessing the current state, begin with the InfoSec team. Discuss potential and known risks to the organization that start with the end user. Next, discuss with executives. They may have a particular agenda in regards to awareness that they want covered. This gives you the chance to gain support from the top levels of your organization. Next, discussions with department leaders will give you a scope of what they see from their employees. This includes questions their staff are asking or issues they have had to report/had reported to them. Collect information from the staff directly. Get their input and feedback in order to understand their level of knowledge. Finally, find their personal interests in the survey process. If you can connect to them personally, you can connect to them professionally and build habits. At the center of all of your consideration should be what the employees need. If they don't see a need for it, you will lose the opportunity to connect at a deeper level.



Market the program

Memorable Taglines & Slogans

Introductory Reminder Email

Think before you click!

Internal Social Media

Relatable Experiences &Stories

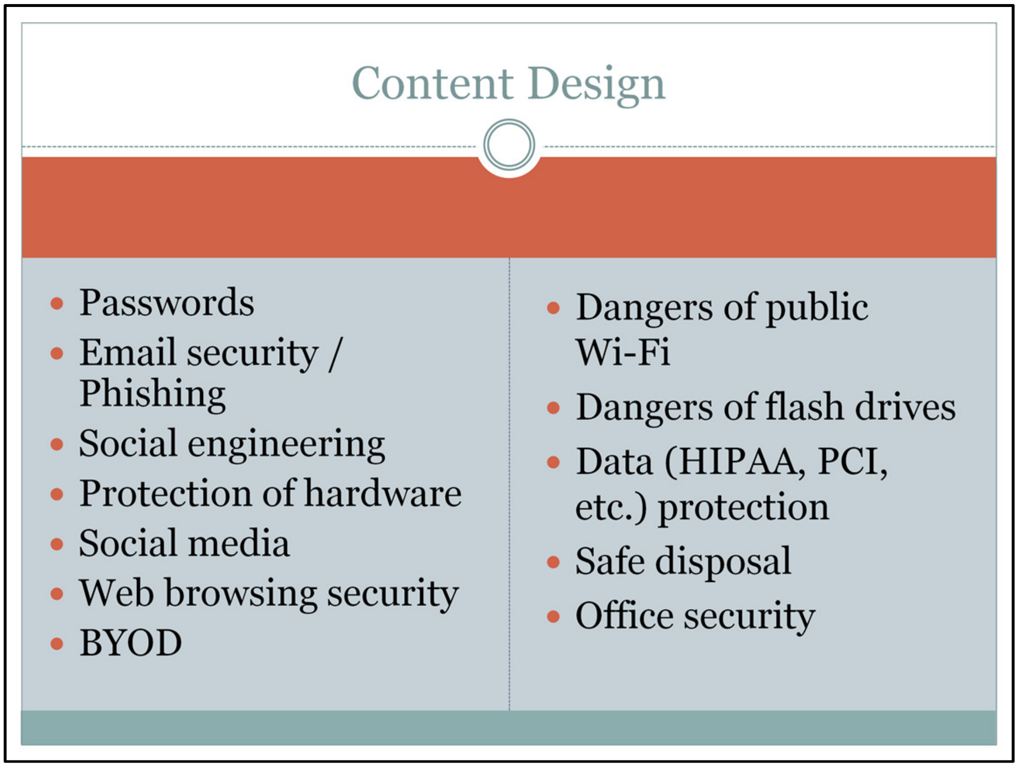
Key leadership

Market the program using various methods. Making it memorable and relevant is essential to its success. Work to ensure that your efforts stay fresh and meaningful. Over communication can make your program part of the “white noise” that will be ignored by the audiences that need it most.

Remember never share more technical terminology with the end users than is necessary or they will be overwhelmed. Relate it to their personal lives!

Use multiple methods to market your program. Make sure everyone sees the training awareness unit as a positive venture not another training that takes away from their jobs. Bring value to the experience with relatable and memorable stories! Make it “personal” to the end user whenever it’s relevant to do so.

Use memos sparingly. Use email sparingly for only the most important and timely communications.



Content Design

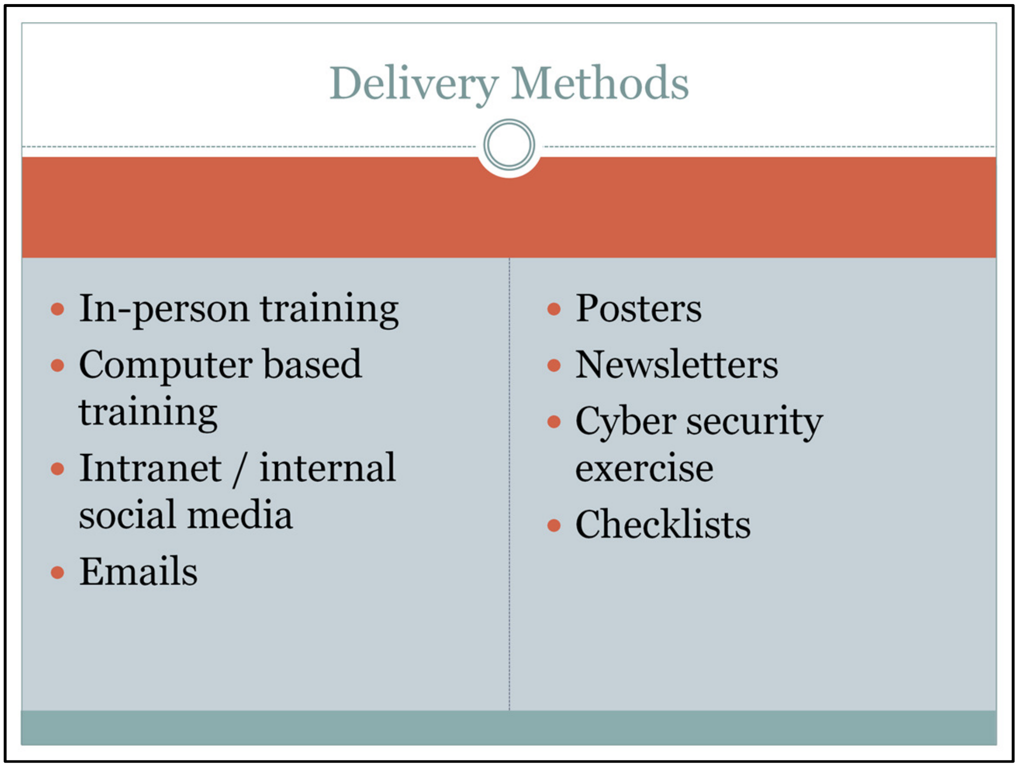
- Passwords
- Email security / Phishing
- Social engineering
- Protection of hardware
- Social media
- Web browsing security
- BYOD
- Dangers of public Wi-Fi
- Dangers of flash drives
- Data (HIPAA, PCI, etc.) protection
- Safe disposal
- Office security

Here are our examples of topics we use. Content should be focused on a single topic, and the trainings should be brief. Your goal is give the audience content that they can walk away with and use immediately. Actionable steps

It's important to always review your topics to make sure they are relevant and cover all the risks that your organization might face and that compliance requires.

Remember the research shows that focusing on a specific topic for a period of time in many delivery formats creates the best retention of the subject matter. Possibly one month per topic.

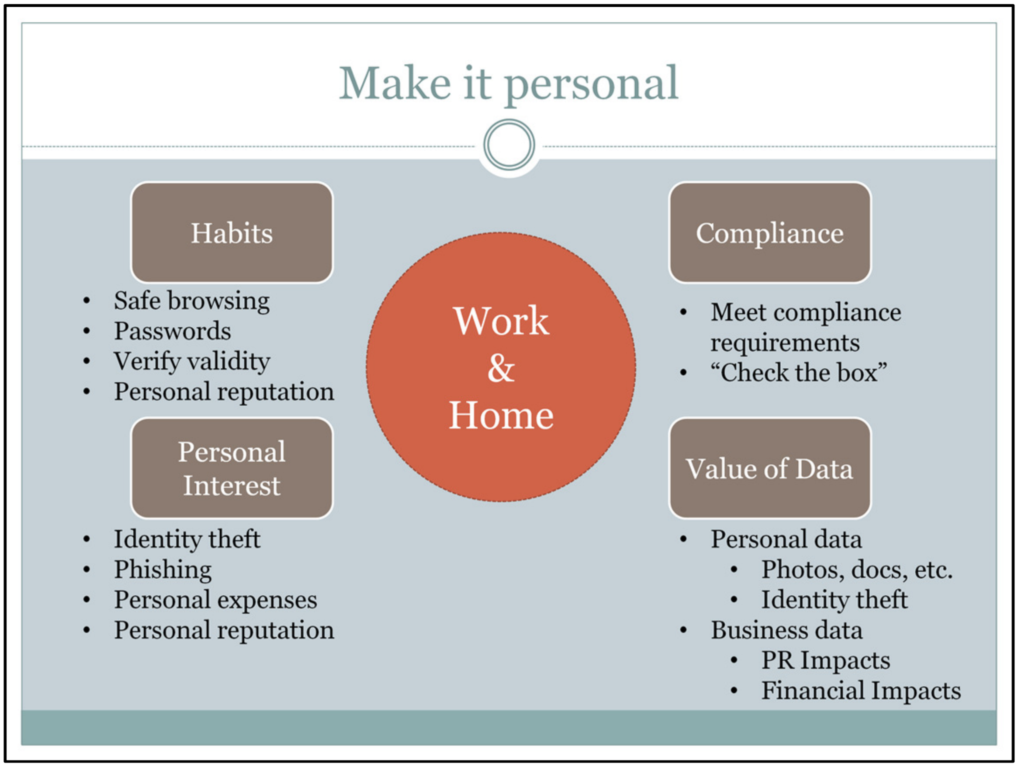
Research also shows that the optimal amount of training (whether instructor led or computer based) is 120 – 200 minutes per year. Another less or more actually has diminished value.



Delivery Methods

- In-person training
- Computer based training
- Intranet / internal social media
- Emails
- Posters
- Newsletters
- Cyber security exercise
- Checklists

Multiple methods speak to multiple learning styles. Some should be optional and some should be mandatory. Remember to start with the baseline of what you need to meet compliance for your mandatory and work from there.



Make it personal

Work
&
Home

Habits

- Safe browsing
- Passwords
- Verify validity
- Personal reputation

Personal Interest

- Identity theft
- Phishing
- Personal expenses
- Personal reputation

Compliance

- Meet compliance requirements
- "Check the box"

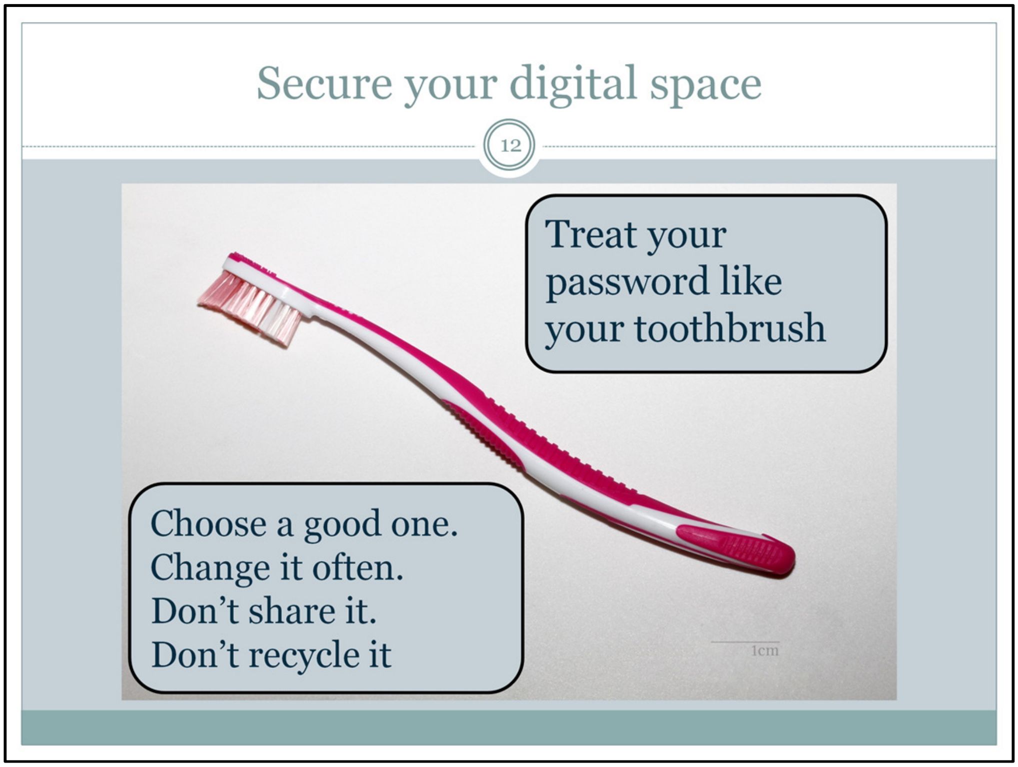
Value of Data

- Personal data
  - Photos, docs, etc.
  - Identity theft
- Business data
  - PR Impacts
  - Financial Impacts

Making it personal helps gain buy-in and interest from the user. It's important for your end user to see personal value to help with retention and behavioral changes.

Personal items can be put in with corporate items.

Or related to both.



Secure your digital space

12

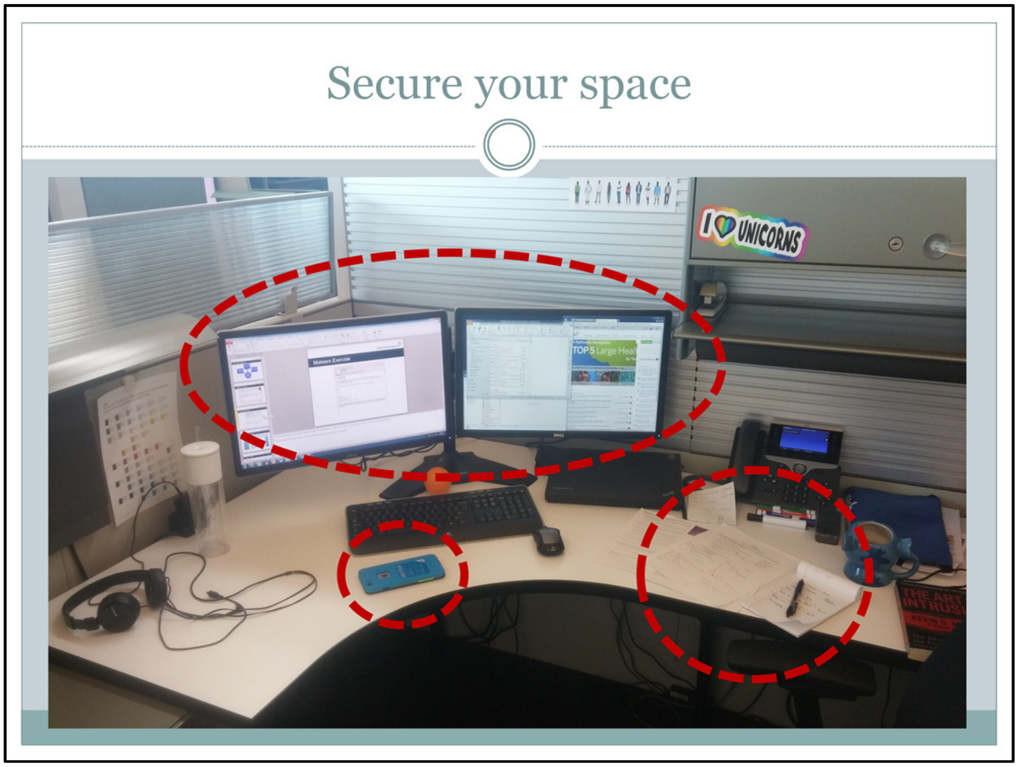
Treat your password like your toothbrush

Choose a good one.
Change it often.
Don’t share it.
Don’t recycle it

A sample of content you can use to deliver your content. Use imagery that sticks with them and can tie to concepts relating to them. We are taught from a young age the basics of toothbrush hygiene and the concept of sharing it seems disgusting to most. Comparing this to passwords makes the concept of choosing a good one, not sharing it, and not recycling old passwords stick with them.

A similar concept mentioned in discussion was “Don’t connect to Wi-Fi anywhere you wouldn’t walk barefoot”. The idea of walking barefoot in a coffee shop or other public space is unsettling and memorable.

It’s also important to use **HUMOR** when you can. **HUMOR** helps a person connect to the material permanently and they remember it.

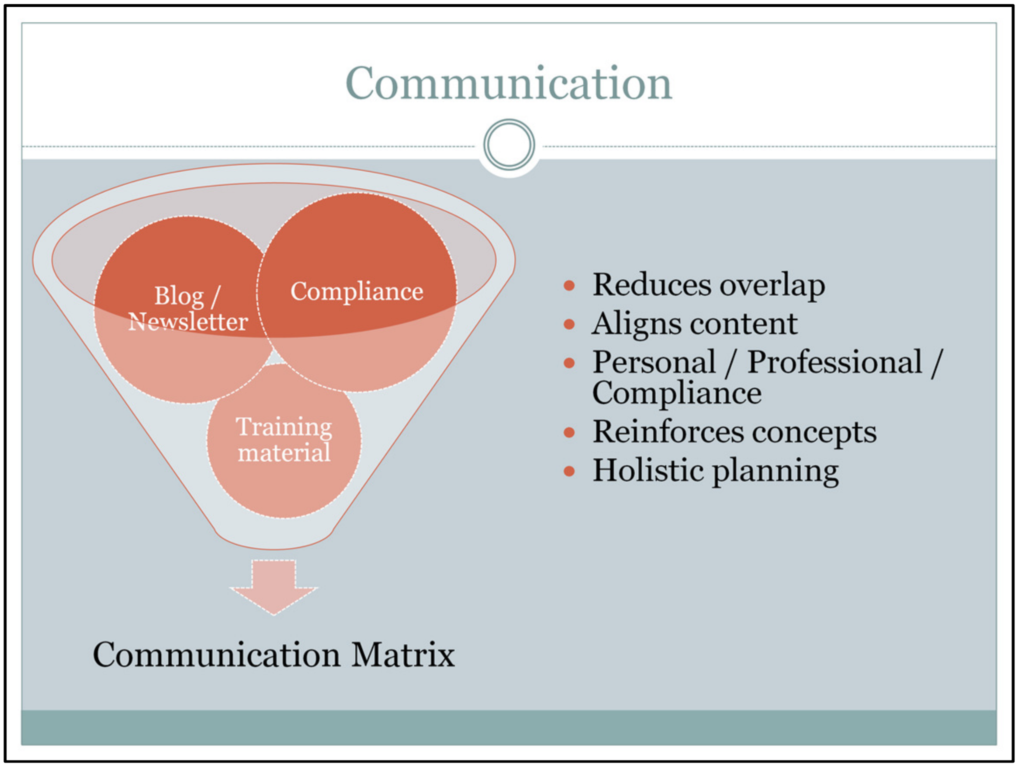


Secure your space

Another example of a slide that drives at important issues and provides some personal connection, and allows for some interaction. Ask The employees to identify the issues with this workspace. An open computer is a connection to all of your data. Some will say “I don’t have access to anything,” but it is important to emphasize that they have access to *people* who have access to data. Such as C-level leadership or IT users with administrative access.

A personal cell phone can be used for 2-factor authentication, it may be used to check work emails or conduct other business. It is also an expensive device that the employee paid for. Even if they aren’t concerned with the data at risk, they will care about personal financial impact.

Lastly, papers are exposed. Emphasize that papers need to be properly stored or disposed of (which sometimes means shredded). A bad actor does not need to steal the papers either as everyone is carrying a high-definition camera on them at all times within their cell phones.



Communication

Blog / Newsletter

Compliance

Training material

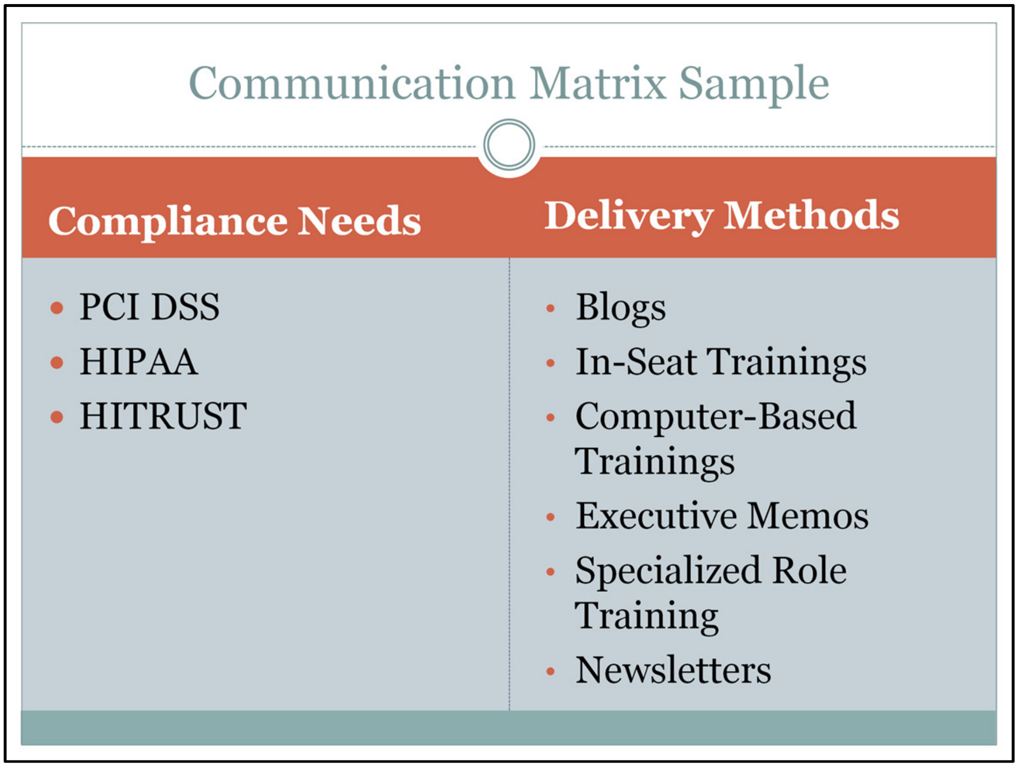
Communication Matrix

- Reduces overlap
- Aligns content
- Personal / Professional / Compliance
- Reinforces concepts
- Holistic planning

Taking your communication methods and combining them into a communication matrix is key. This ensures that you remove overlap across topics, that personal, professional, and compliance needs align and that you determine the best time of year to communicate them.

For instance using holidays to communicate credit card risks sticks and makes sense to an end user and can satisfy PCI at the same time if it is both personal and professional.

Try to get this matrix to address all your compliance needs, training needs, the methods and the timing. Then you can extrapolate each out to individual training plans for each topic/compliance concern, or method of delivery depending on your preference.



Communication Matrix Sample

Compliance Needs

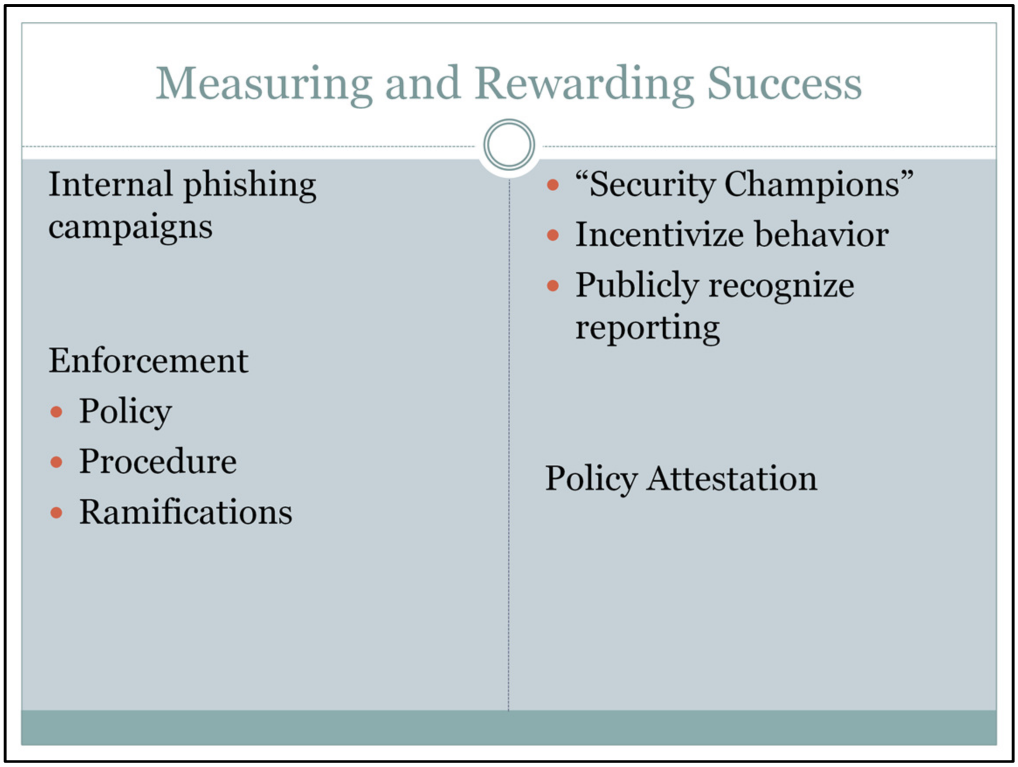
- PCI DSS
- HIPAA
- HITRUST

Delivery Methods

- Blogs
- In-Seat Trainings
- Computer-Based Trainings
- Executive Memos
- Specialized Role Training
- Newsletters

In our space, we looked at different compliance requirements (PCI, HIPAA, HITRUST), and created a spreadsheet. Each column represented a different communication need, and each row was a period of time (split months into thirds). We then filled the grid with blogs, in-person trainings, computer-based trainings, memos, etc. and identified where there was overlap. We consolidated the message for each month and made sure that we could find alignment across all required spaces.

Remember for retention of the material it is best to stay on one main topic for a period of time.



Measuring and Rewarding Success

Internal phishing campaigns

Enforcement

- Policy
- Procedure
- Ramifications

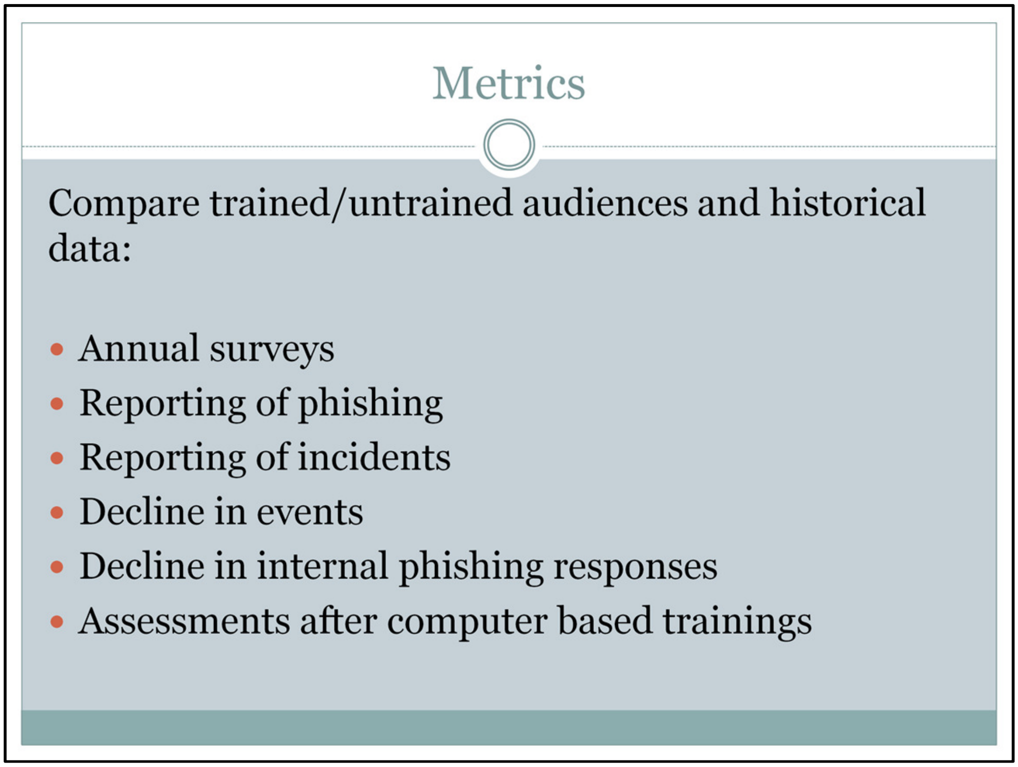
- “Security Champions”
- Incentivize behavior
- Publicly recognize reporting

Policy Attestation

Measuring success and rewarding success require a few key things. Measure according to metrics such as internal phishing, policy attestation, and others (outlined in the next slide). It is important that you differentiate the roles responsible for enforcement of policy and the incentivizing of behavior. Enforcement should be rooted in policy and should come directly from the department leadership rather than from security/security awareness.

Positive reinforcement: Incentivizing behavior can have a positive impact but it needs to be small. When behaviors are rewarded with large gifts, people will do the behavior strictly for the purpose of getting the gift. With a small reward such as a magnet, they are achieving the behavior more for bragging rights and the intrinsic reward.

Negative reinforcement: Remember that the research actually shows that while positive reinforcement can improve results, threat of negative reinforcement actually increase results more than positive. So it is important to have a mixture of both positive and ramifications for negative.

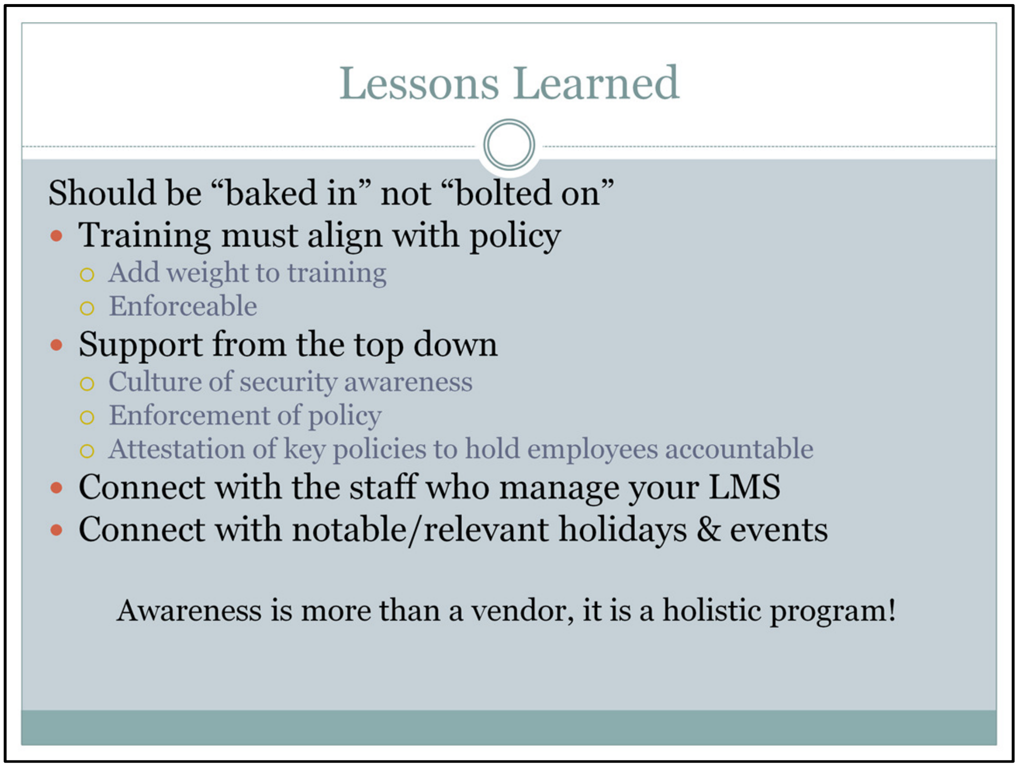


Metrics

Compare trained/untrained audiences and historical data:

- Annual surveys
- Reporting of phishing
- Reporting of incidents
- Decline in events
- Decline in internal phishing responses
- Assessments after computer based trainings

Gathering metrics on training that can be directly tied back to ROI can be difficult. You struggle to prove a causal relationship between training and a lack of incidents. Historical data is important to show that the data you collect is at least correlative to your training efforts. Items you can measure include internal phishing failures, reporting of internal phishing, reporting of actual phishing, increased reporting of incidents, and assessments attached to computer based trainings.



Lessons Learned

Should be “baked in” not “bolted on”

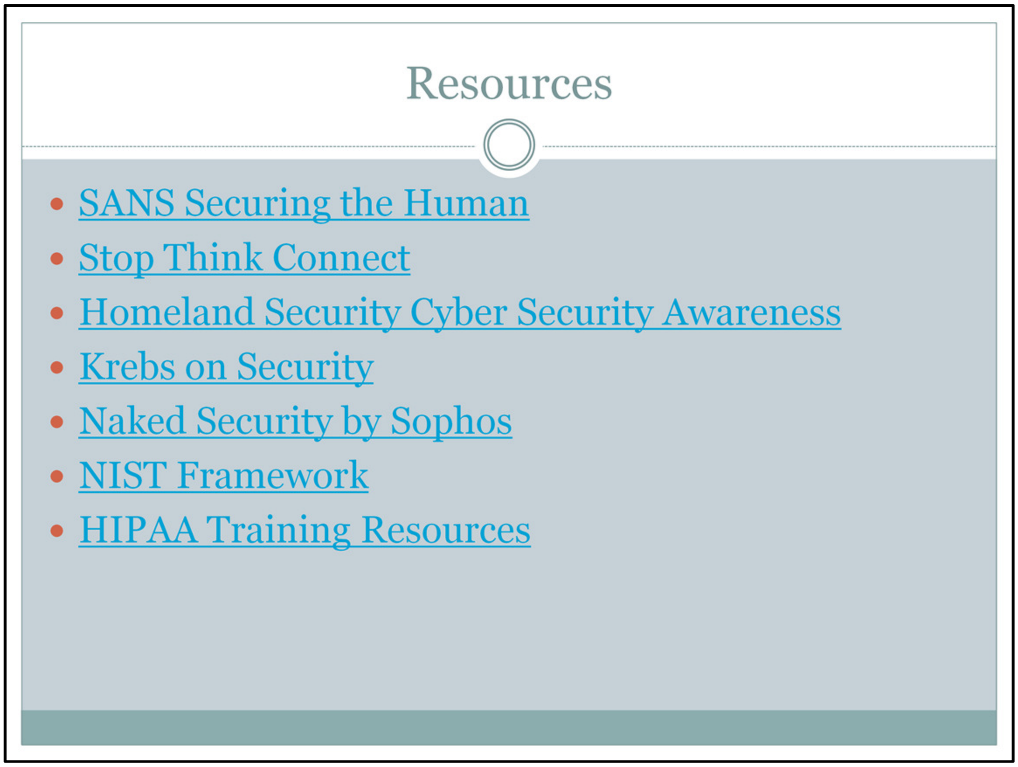
- Training must align with policy
  - Add weight to training
  - Enforceable
- Support from the top down
  - Culture of security awareness
  - Enforcement of policy
  - Attestation of key policies to hold employees accountable
- Connect with the staff who manage your LMS
- Connect with notable/relevant holidays & events

Awareness is more than a vendor, it is a holistic program!

The biggest lesson learned is that awareness training cannot be quickly added on, it is a process. You must make sure that your training starts with policy. Policy is necessary to make your training enforceable and to add weight behind the concepts taught. This can also ensure that your support comes from the top down.

When working with a vendor or building computer based trainings, be sure to connect with the staff that manages your Learning Management System to ensure a seamless deployment of a training solution.

Connecting your content with notable events and holidays can make it more relevant to your end users and provide you with an opportunity to repeat content without the core concepts getting stale.



Resources

- SANS Securing the Human
- Stop Think Connect
- Homeland Security Cyber Security Awareness
- Krebs on Security
- Naked Security by Sophos
- NIST Framework
- HIPAA Training Resources

- https://securingthehuman.sans.org/
- https://www.stopthinkconnect.org/
- https://www.dhs.gov/national-cyber-security-awareness-month
- https://krebsonsecurity.com/
- https://nakedsecurity.sophos.com/
- https://blog.knowbe4.com/
- https://www.nist.gov/cyberframework
- https://www.hhs.gov/hipaa/for-professionals/training/index.html

Some resources to help get you started. And there is a Gartner Magic Quadrant for external training programs for security awareness.