Banning Whining, Avoiding Cyber Wolves, and Creating Warriors

Sandra (Sandy) Dunn
October 2016
GWAPT, GCIH, GCCC, GSEC, GCPM, GSLC, GSNA, CISSP, ISTQB
Whining about cyber security is an unfortunate first response from all parts of an organization discussing cyber security challenges. CEOs whine that no one cares about the business data and the bottom line, business and product managers’ whine that no one cares they have deadlines, users whine that they are confused about how to avoid bad guys, and the Cyber Security team whines that no one cares about security and how hard their job is. Do you have any “whining” about security in your organization?

Safely protecting an organization and its data in an increasingly hostile and more connected cyber world depends on changing employees from cyber victims to cyber warriors. This presentation highlights common misconceptions in security awareness programs, how to avoid common pitfalls, and how to effectively target security awareness and turn intimidated, confused workers into empowered protectors that are an organization’s first line of defense.

The Objectives for today’s presentation are:

- The valued of employee engagement or “Building the Front Lines”
- Point out that people really aren’t good at determining risk so we need to provide them better tools to identify risk
- How to have the Security Awareness Budget conversation with your
management team
• The importance of creating before and after baselines
• The danger of canned programs or another way to say it is “Security posters do not = correct action”
• The importance of avoiding scare tactics
• The value of using “Nudging” tactics
• How to effectively target your audience so you are getting the right message to the right people. A security awareness program for executive administrators should have different information than the ones aimed at developers.
Building the Front Lines through Crowd Sourcing Security:

Each work culture has its own nuances but in most cases deputizing everyone in an organization to be part of the security team is more effective than having a small group of people be the cyber security police. The receptionist at the front desk knows who the normal UPS person is, the electrical engineer knows who should have access to the closet, the nurses know what reasonable access to patient data is.

How you communicate your message is important. One of the parenting hacks I learned is giving orders has been the least effective way to motivate my girls. When I made their lunches I noticed vegetables were eaten and treats were often left if I labeled the vegetables “Eat carefully, these provide extraordinary super powers” (carrots eyes, peas strength, cucumbers ability to jump high).

Our goal is to turn people from Cyber victims who believe they are helpless and can’t defend themselves into cyber warriors who have the right information to help defend the organization. That includes knowing what to do when something bad does happen and an Incidence Response process must be initiated.

Security is like quality and safely protecting an organization and its data in an increasingly hostile and more connected cyber world is dependent on changing how people think about security in your organization. The quality of a product starts with the person responsible for the initial design and includes everyone in your organization such as the person who designs the web site, to the person who answers the support call, to the person who ensures that the building looks professional. Encourage your organization to embrace this same philosophy with
security and include it as part of every job description.

- Your message is to empower employees and give everyone within the organization permission to say “I don’t recognize you, I’m not trying to inconvenience you, but I would like to call security, my manager, or someone else who I trust to collaborate why you should be here.” or “I think this requires a review by the security architecture team. I don’t think we should use WeChat even though it’s the most popular social media tool in China.” (The fine print in the WeChat terms of service states that the Chinese Government owns all the data on WeChat.)
• Regardless of the type of organization you belong chances are you don’t have unlimited funding to build a security awareness program.

• Things to consider:
  
  • A short weekly news letter with personal and business tips that includes urls to policy is an inexpensive way to start a business thinking about security.

  • Pre-canned and often expensive programs may not be personal enough or interactive enough to actually engage your team. Sending an email that says “Watch this” doesn’t provide the same level of engagement or feedback from users. It’s possible that you pulled people away from being productive, haven’t moved the needle on security, and now won’t have metrics that validate this was a good investment.

• When discussing budget think big picture. You’re not asking management for money to protect the business this year, you’re also preparing for next year, and the year after that, 5 years, 10 years, 20 years. Fortress foundations laid now build a strong wall of defense for future adversaries.
Invest

- Security training a good investment in your employees
- Help people with their data and they will help you with yours

• Reinforce to management that Security Awareness is an investment for the future.
• One of the best Security Awareness tips I learned when taking the SANS 433 Security Awareness training was to include security training tips in each session on how to protect things users care about. For example, their children, their money, their data. Those good habits move into the work environment and they protect the organization’s data.
Creating a Baseline

- Use recent significant threat landscape events like ransomeware
- Use frequent events within the organization
  - Certificate misconfiguration
  - XSS
- Measure, pivot

- Creating a baseline is important so that you can verify the return on investment and measure what measures worked where.
- Read into the data carefully
  - Real life example of ransomeware which was a symptom of the real problem of remote desktop turned on and a bad password.
- Measure and pivot if necessary. If you’re not getting the expected results, try to understand why and then try something different.
  - Real life example of a Git mistake pointed to lack of general training.
Cyber Security is a complex and to many people a confusing and intimidating topic.

In an effort to do “something” generic training and posters are frequently viewed as the only available option but they are not valuable if they don’t drive measurable change.

The problem with posters, static, generic, the best solution for one organization may not be the best choice at another organization.

People can often be confused about who is at real risk and who should be concerned – keyboard example

Why are scare tactics bad

- People can’t get their job done. Use a car analogy. If people are scared to drive what happens basically everything grinds to halt. The web / internet is key to business our job is to help people do it as safely as possible and if something bad happens know what to do – if you get in an accident what are you supposed to do? (call 911, get each other insurance, don’t leave, etc)
In his paper “The Psychology of Security” https://www.schneier.com/academic/paperfiles/paper-psychology-of-security.pdf Bruce Schneier addresses the psychology of security. Mr. Schneier leads his paper with the statement “Security is both a feeling and a reality. And they’re not the same.” He uses the term “Security Theatre” when things are done to make people feel more secure that don’t necessarily make them mathematically more secure. An example he uses is the screening and limiting of liquids used by the TSA.

The best way to improve security in an environment is to use Security Theatre tactics that align with the actual measurable reduction of security risks. Using a psychological approach when implementing security controls and building a security awareness program simplifies security for the user and drives to align actual risk with potential events.

Mr. Schneier lists these as common misjudged security behavior:

- People exaggerate spectacular but rare risks and downplay common risks. For example most people are extremely afraid of being attacked by a Shark and not afraid of driving.
- People have trouble estimating risks for anything not exactly like their normal situation.
- Personified risks are perceived to be greater than anonymous risks
- People underestimate risks they willingly take and overestimate risks in situations they can’t control
- Last, people overestimate risks that are being talked about and remain an object of public scrutiny.

Examples of psychology with security? Data labels that add color. In your training reinforce that emails from outside vendors should receive the same scrutiny as other emails outside of the organization and people should not put their guard down just because it appears to be from a familiar business. Apply extra scrutiny to new or passion projects where a developer might overlook security in exchange for using something that is new. Printers that send information
encrypted have a different panel color than printers that send information unencrypted.

- Andy Ruins Everything https://www.youtube.com/watch?v=QKEdKdgi2hg&spfreload=10. An example of getting engagement play this episode at a “Bring your own lunch meeting” maybe provide dessert? Have a contest for the best security reality / security theatre.
• The fly in the urinal is one of the most common example of a “nudge”. It was originally proposed by Jos Van Bedoff for the Amsterdam airport over 20 years ago. A 12 pack of stickers are $10.00 at http://www.urinalfly.com/


• A Nudge is a strategic approach to encourage people to take the actions you want them to take.

• Thefuntheory.com
I would like to walk through some examples of security awareness posters. Why their message may be considered confusing, how to say the same thing and drive measurable change, and some ideas on nudging behavior.

Why this confusing:
• Is the internet really a jungle?
• Can animals use the internet?
• What is dangerous?
• What are the proper precautions?

Better example:
• Information is a digital currency. The internet is accessed by over 3 and ½ billion people [http://www.internetlivestats.com/internet-users/](http://www.internetlivestats.com/internet-users/) that are motivated by a variety of political, social, economic reasons that may include accessing your and your companies information. Any information you share publically on Twitter, your public Facebook profile, or other social media can be accessed by those 3 & ½ Billion people.

Nudge behavior
• A security awareness class on using a VM Player image for home computers when accessing new sites or doing internet research in unfamiliar places.
• This is similar to the previous poster. As a user what message are you receiving? “Avoid the internet you will be eaten by a scary looking wolf”
• Suggestions on making it better?
Why this is bad.

- This sends the wrong cultural message. If a company is concerned about the people inside the network they should review their hiring practices. If people aren’t following policy, standards, and guidelines try to determine why. Are they too difficult to read? (techno babble), outdated, or not targeted at the right audience (written for protecting IT network not for product expectations)?

Better example

- We need you (mimic recruiting poster) to help protect our organization.

- It seems harmless but.. (show a flow chart of someone accessing protected information and the consequences such as someone with admin credentials on server surfing the internet)

Nudge behavior

- Free wifi access in the breakroom so you use your personal devices to check Facebook, read your personal email, and watch that funny dog video!
Why this is bad

- Does it explain what a “Cloud” is? How many users would connect that Gmail is a cloud, Instagram is a cloud, your Fitbit data is in a cloud.
- Most major organization have some sort of cloud strategy. What do you think the lead cloud architect wants to do to you after you hung this up? Throttle you. You just spun him into damage control and he has to go explain to every executive, administrator, and sales person in the organization that he isn’t going to destroy the business.

Better example

- Poster explains what the Cloud is.
- Keeping data safe on a local system vs local network vs cloud. Remember to target the audience. Highlight things like the use of GIT and safe backups to developers. Highlight data labeling to Executive administrators.

Nudging behavior

- A lunch and learn where you open with an open discussion on benefits and challenges of daycare vs staying at home and compare it using the cloud. Stay at home one person does all the same work for a limited amount of children. Daycare almost same amount of work for lots of children, more benefit to the
family Mother can work. (Don’t let this get out of control, your trying to get relatable engagement and for people to understand why it makes sense to put resources into the cloud. Then provide 30 minutes of “ask any Cloud question”
Why this bad
• They have said what is bad they haven’t explained what is good.
• They haven’t explained that there is more value in some passwords than others.
  What is the most important password you need to protect? The email account used to reset all other passwords.

Password managers
• A word on password management tools. I use one, I have to. There are just too many passwords I need. I am aware though that it is my “keys to my kingdom”. I encourage people to make their own risk based decision.

Better example
• A poster that has marbles in a bowl that represents the number of different possibilities based on random characters and length. Minimal randomization and length fewer marbles, more randomization and length more marbles.

Nudging Behavior
• Group policy that enforces password policy
Employees and Social media

- Social media isn’t necessarily all good or all evil. It is just ones and zeros like all data that is converted from text to binary to positive and negative pulses and pushed into cable or sent wirelessly through the air. The message we need to convey to people is make a risk based decision on the information you share. Have a social media policy that provides easy to follow and provides sensible guidelines. Your employees are your best advocates. A social media policy that says “You’re not allowed to reference anything about where you work and what we do.” Loses out on employee posts that say “I love working at ABC company because I believe we are truly making peoples lives better and they appreciate the work I do” which could influence future rock star candidates.
- As evidenced by these headlines too much information can have dangerous consequences

---
Build the front lines
Budget and Baselines
Avoid scare tactics, use Nudging
Target your audience
Easy to find information
- Open and accessible security culture
- Cyber Security Wiki
- Incident Response
- Policy
- Recognize good
- Provide useful tools

If people feel intimidated or that they are going to made to feel stupid they won’t ask the questions that help secure your organization.

Create a Cyber Security Wiki. It should be in a centralized location. It should include links on where to find additional information, be well organized and up to date. Previous Security Awareness training should be accessible from the wiki. When people run into a situation they may want to go back and refresh “Why data labels are so important”.

The goal is to implement every necessary security control to keep your organization secure but make sure if the worst happens people are ready. The Incident Response process, including who to call should be communicated often and easy to find when people are faced with an event.

Make sure policy isn’t so complicated and long that people
just give up. What the laws are should be clear

- Useful tools Point users to tools like NoScript, https://noscript.net/getit, Ghostery https://www.ghostery.com/, or this site where they can find tools to look up malicious sites https://zeltser.com/lookup-malicious-websites/