Enterprise Security: Some Ways to Move From Awareness to Culture

There may be as many office cultures as there are offices. This means any attempt to sway an office in one direction or another needs to be carefully crafted to fit the preferences of the actual humans that create that office. This article will be focusing on moving from an organization, or office, that focuses on providing security awareness training to being an organization that grows the strength of its security aware culture. The intent is not to provide a comprehensive playbook of how to build a security aware culture; rather, discussing training, alerts, competitions, leader-boards, and lunch dates should provide some ideas to consider as a starting place. Moving from a security awareness training program to a security aware culture is not an overnight endeavor and appropriate expectations should be set, it takes time but consider this, baby steps are better than nothing when the target isn't moving but attackers are always moving the safety line.

There was a time when compliance was the chief reason for providing security awareness training to user and in many cases compliance is still the reason organizations provide security awareness training. While meeting compliance is a good reason to provide security awareness training, not being in the news for having high profile accounts seized by criminals is a better reason. Users need to know the mechanisms used to attack them. The best analogy is a user understanding the difference between a teller having a friendly conversation in a bank and a person pointing a gun at a teller in a bank while speaking in a friendly tone. If a user didn't know what a gun was they wouldn't understand the risk, likewise, if a digital users doesn't understand digital risks they can become victims due to ignorance. Because users are victimized by attackers security training providers should be evaluated based on both the content they provide in the training as well as how that content is delivered. If content is very high quality but delivered in a monotonous way the user will be prohibited from being able to mentally retain the content. Likewise, if security awareness training is too long in duration or is bundled with other "annual enterprise training" the user may experience information overload and essentially be a spud that is letting information in one ear and out the other despite any intention of retaining the content. One way to emphasize certain training points may to use alerts.

The security landscape is continuously changing while at the same time remaining consistent. There are constantly new techniques to steal passwords but attackers are still stealing passwords for instance. This gives an avenue to provide regular snippets of security awareness training regularly in the form of a 1 to 2 minute format. This could be in a video-graphic format or written and can be disseminated through chat, email, or on an intranet, extranet, or public site. The intent here is to create a message that relays a current threat that is active in the wild (actually being used by attackers,) and append that with a snippet from the security awareness training. The important part is the consistency of the security awareness snippet as it should be verbatim as that will imbue that knowledge (through repetition) into the users' knowledge banks. If this is sent via email the subject line and first sentence is critical. Many users will not open email alerts but will read the subject line and may have their email configured to display the first line of content within an email. To provide an example, if the security alert is about password stealing phishing the subject line might be "Phishing Email Stole Passwords: Company x Breached". Keep things simple and obvious, trying to be clever or technical will certainly cause some users to misunderstand the intent.

Competition is a force around the world with fans that are willing to paint their bodies, stand half naked in freezing weather, and even become physically confrontational in defense of a particular brand. This force should be leveraged in a positive way to assist with the crafting of a security culture. There are two main types of security culture competition, the department vs. security team competitions and the all departments competing against each other competitions. In the case of the department vs. security team competition the idea is to host a competition between the security department and the "defending" department with the "defending" department awarded if they are able to meet the goal. In one example, the defending department may be given a prop (maybe a sparkly bowler hat with a big red feather sticking out of the top) and instructed to write a word inside the hat. The "defending" department should then be instructed to keep the hat in their department for a month without letting the security department determine what word is written in the hat. Before the competition begins there needs to be agreed to rules that reflect the maturity of the department's security awareness and posture. For instance, in most circumstance it would be unfair if the security department stole the hat in the middle of the night. Likewise, the department should be restricted from unfair advantages like locking the hat in a cabinet or safe for the entire month. This should build a cohesion through friendly competition as well as assist the "defending" department get to know the faces and contacts in the security department. Competitions that put all departments in competition with each other should be used for enterprise wide initiatives to improve the quality of reporting. For instance, one competition could be created to award the department that accurately reports the greatest number of phishing emails. The key here being "accurately" which penalizes departments that erroneously report every spam email as a phishing email. The rewards for these competitions need to be relevant to the organization and departments that are involved. Whether it be an extra day off, a catered lunch, or being recognized on the main page of the intranet (not internet because that would give attackers targeting data), the reward needs to be something that department members actually want to help gain participation. Keeping an internally viewable leader-board for competitions can be a motivator for departments as well.

Leader-boards aren't just for leaders, they are to normalize stigmas about mistakes too. Having leader-boards promotes transparency and can be a tool for improvement. Choosing the correct items to be promoted on the leader-boards is critical and must be tailored to the motivations of the community. One organization may choose to have an enterprise level leader-board that displays the total number of phishing attempts detected and stopped, the number of phishing attempts that succeeded, the number of organization security incidents, and the number of reported incidents and/or phishing emails. Another leader-board may have a list of departments with the number of technical and social engineering incidents detected and prevented, the number of successful compromises, and the number of privacy incidents. No sensitive information or information that can lead to embarrassment or targeting should be used on enterprise leader-boards. For instance, leader-boards should never list users' names with failures (such as failing phishing exercises), not only can this be highly embarrassing and alienating, it could cause legal issues or even lead to the development of an insider threat. Leader-boards, when used appropriately, can create transparency and remove the stigma of cyber threats while building unity or competitive spirit. A more personal touch may be required for environments that are not competitive or where leader-boards are not effectively implemented, a lunch date between security and other organizational department may be required.

Creating a security culture is very much an exercise in wooing. The security team must woo all other departments into loving the idea of keeping their coworkers and company safe from the threats posed by mean outsiders and naughty insiders. The idea of the lunch date is to invite a department to a catered lunch with the security department. The lunch should be about two hours and be informal. The idea is to provide the guest department and opportunity to explain what they do, what their concerns are, and ask any questions they may have for the security department. The security department's responsibility is to gain the trust of the department, assure the department they are not there to judge or get anyone in trouble, take notes, and provide guidance, feedback, and resources that answer any questions or concerns. It may take more than one lunch for a department to really build a relationship with members of the security team but building strong cohesion between outside departments and the security team is one of the most effective ways to move from security training to security culture. The more comfortable people outside of the security department feel when approaching security personnel for advice and guidance the better equipped a company will be to detect evolving threats very early in the attack. The key thing to remember about this cohesion is to ensure there is a process that permits users to get "self-help" and a way for security to triage requests for information and guidance without alienating the requester. Lunch dates are a great way to woo the organization but care must be taken to ensure no department becomes a needy dependent that can't effectively exists without constant input about minutia from the security department.   There are many office cultures and many ways to move from training to culture but lunch dates is one idea worth considering.

There may be as many office cultures as there are offices. This means any attempt to sway an office in one direction or another needs to be carefully crafted to fit the preferences of the actual humans that create that office. This article has focused on moving from an organization, or office, that focuses on providing security awareness training to being an organization that grows the strength of its security aware culture. The intent was not to provide a comprehensive playbook of how to build a security aware culture; rather, discussing training, alerts, competitions, leader-boards, and lunch dates should have provided some ideas to consider as starting places. Moving from a security awareness training program to a security aware culture is not an overnight endeavor and appropriate expectations should be set, it takes time but consider this, baby steps are better than nothing when the target isn't moving but attackers are always moving the safety line.

Thank you for reading

-Andrew Kosakowski

www.Anthko.com