WHY A POSITIVE SECURITY CULTURE MATTERS – FOR ANY COMPANY

One of the newer buzzwords in cyber security is ‘Security Culture’, but a lot of people still are not sure what that means or why they should care.

All culture derives from shared viewpoints. Security culture follows the same principle. What employees think about their company’s security policies, procedures, and posture creates their security culture.

In most companies, people are the most valuable resource, and those same people are also the company’s biggest security risks. Unlike other resources, they are much harder to patch and maintain when it comes to security.

But people do follow group dynamics. If they join a group, or company, where everyone already shares common beliefs and work ethics, they will tend to follow along to get along if nothing else. And when interviewing and hiring, people look for others who they think will fit into the existing culture of the company.

Cybersecurity Culture Tip #1: When built up correctly, the employees will start to reinforce the culture themselves.

Even if companies don’t realize it, their security culture already exists – be it good or bad, large or small. When employees look at security as preventing them from doing their jobs, the company suffers. They do the minimum to meet security requirements, and in some cases knowingly bypass security measures because it is easier and quicker than following procedures.

A healthy security culture is more than just having security controls in place. It is more than just having employees take a security awareness training class once a year. It is instilling the belief that the company and everyone who works there includes security in everything they do - and not just because they were told to. They make security part of their job because they believe in it.

Cybersecurity Culture Tip #2: The employee who minimalizes security to get their job done will support security measures if they believe it is an important part of their job.

They believe company security is not only the job of one or two people in the IT department, but that security is everyone’s responsibility. From the CEO to the entry level new hire, everyone knows that their job includes security, and they are invested in the process and outcome. And in turn, the company must invest in the education and security training of all their employees to make security relatable and applicable to everyone.

Cybersecurity Culture Tip #3: Shorter training sessions and more frequent reminders work better than longer training sessions less often.

A good security culture is not one of secrets and impediments to production. One of the major aspects of a good security culture is a high level of communication. You cannot have an organization of silos all acting independently with no one looking at the big picture on how it all integrates. Every person must understand how their part plays into the greater whole. They must communicate how their part works to others so everyone else understands how that part fits into their plans also.

When done right this communication builds a level of security awareness across the company. As each individual increases their communication and security awareness it pushes others in the company to respond and evolve. A good culture must be built and encouraged to take root and grow, it cannot be forced.

Cybersecurity Culture Tip #4: Communication is not limited to security. Once they are communicating, other aspects being discussed will help with production, scheduling, and team building.

In this environment, security is not something to add on after-the-fact just to meet requirements. It is as important and vital at every stage of the process as every other aspect of the project. Security should be part of all pre-project planning, code reviews, and change control processes.

One of the issues many companies must address is finding the correct balance of review with their employees. Honest reviews of security issues and problems are important. However, an environment based on blame and focusing only on negative examples of security failures can hurt the security culture. Incidents must be looked at as ways to evaluate both the good and bad activities that occurred. Negative issues must be looked at as learning opportunities and the positive should be celebrated and encourage.

Cybersecurity Culture Tip #5: Many companies have had great benefits with bug bounty programs. Setup a way for your employees to submit specific security issues they find and in return reward and recognize those individuals.

No matter the size of the company or the industry you are in, building a positive Security Culture will benefit both the employees individually as well as the company as a whole.

A final takeaway to remember is that a good security culture is not a switch you can just turn on and leave. It is part of the company's security maturity that must be developed and maintained in an ongoing process.

For more information please contact Rick Bush, Cybersecurity Architect, RESPEC, rick.bush@respec.com.

Rick Bush

CISSP GCIH GPEN GCFE

CyberSecurity Architect

RESPEC