Why cyber security awareness?
People are the weakest link in any cyber security program and it is important for organizations to change the ways people think and behave with regard to cyber security. Start by creating a culture within your organization where employees have an understanding that cyber security is not just for the geeks or IT staff - it is the responsibility of every employee. Focus on educating employees on how to recognize and respond to threats and vulnerabilities appropriately.

Who is my audience?
Since every employee, contractor, and vendor has a hand in maintaining the security of the organization, the awareness program should be targeted at these groups. Be sure to include leadership as they set the tone at the top for the organization.

How do I start?
Begin by demonstrating Senior Leadership support. A few ways to do this is to have management launch the program, for example by sending an e-mail. They could also kick start the process in a staff meeting or a special meeting which is held only to discuss the importance of security awareness. This message should emphasize the fact that cyber security is everyone’s responsibility.

What about cyber security policies?
Review your current security policies to determine if you need to create or revise them. At least annually, all employees should review these policies and sign an acknowledgment. Job descriptions and performance reviews should include security responsibilities.

How should I get this message out?
While there are several ways to get the message out, the key is to make security a part of everyone's day without being obnoxious or repetitive. To be successful, it must be an on-going program and requires creativity and constant care and feeding. You can start with methods such as luncheons, weekly messages on the corporate intranet, or hard copy newsletters but be creative. A cyber security day may be another effective way to bring security to the forefront of everyone’s mind. This could be a great opportunity to hand out messages on mugs, shirts, or note pads.

Provide information on the latest threats such a virus, worm, or social engineering. Security audits when used as a training mechanism can also help to raise awareness. You can also consider office space reviews (look for passwords under keyboards) and annual self-assessment surveys.

Distribute security awareness tips by e-mail about once every two weeks. Tips should advise of best practices and reinforce policy. Here are a few topics to start off with:

- Viruses
- Passwords
- Workstation security
- Destruction of sensitive materials
- Photography
Laptop security
Don't be afraid to say no
Social engineers
Operations security
Backup your data
Reporting Security incidents

Ensure that cyber security awareness is not based only on negative events. It takes time to make a change. Finally, lead by example. If you believe in security and explain why, it is much easier to bring others around to your way of thinking.