What to expect from Cyber Awareness Training

Never has it been more important to ensure that your workforce is cyber aware when it comes to mitigating the risk of a cyber attack. A key element of this preparation is ensuring that employees have a good understanding of the threat landscape together with the steps they can take to help keep these increasingly sophisticated and determined cyber criminals at bay.

Our unique approach provides everyone from the board to the shop floor with the knowledge and skills to defend your organisation.

A typical training program can look like the below:

1. Initial meeting with key stake holders

We will come in and meet with you to discuss your business goals and requirements. Find out where you are on your journey to cyber awareness and where you want to get to. As well as discuss any previous data breaches or cyber attacks where staff have been responsible. This discovery session will help us to design and delivery a training program that works for your business and staff.

2. Half day workshops or Lunch and Learns

Once we have agreed on a training program that works for you, we will arrange for this to happen. Because of the nature of the interactive session, the maximum number of staff we can have in one session is 20. This can be done over one half day workshop or we can provide a number of 1 hour sessions during a lunch break if this is more convenient.

3. Assessment

After your staff have completed the workshop we will provide them with a short quiz to test their understanding. Once they have passed this, we can issue you with a certificate that shows your staff have received the training.

4. Review

We will then review the results with the key stake holders to share our thoughts on how aware your staff are and raise any risks which we have identified in the sessions so that you can look out for them in the future.

5. Testing your staff

If your staff just attend for a checkbox exercise, it isn't worth their time or your money. So to ensure they have really taken on board the learnings from the session we recommend testing them after the sessions. This can be done through a Phishing simulator which can send out emails which look legitimate to test if anyone clicks on them. We can then provide further training to those who need it.

Cyber awareness training is vital, from mitigating against an insider threat, understanding the supply chain risks or ensuring your executive management understand the issues and their responsibilities. Regardless of size, industry or geography cyber crime knows no boundaries. Educating users can help detect, deter and defend against the cyber threats that every business and individual faces.

20%

Only 20% of businesses have had staff attend some form of cyber security training in the last 12 months, with non-specialist staff being particularly unlikely to have attended.