Cooking up security awareness & training

Karen Renaud

The published article is available from doi:
http://dx.doi.org/10.1016/S1353-4858(18)30047-3

Cooking up "Security Awareness & Training"

No one would suggest making pancakes without heat. Everyone knows you need a catalyst to transform the ingredients into a delectable treat. The ingredients added to the pancake batter must be used in the right proportions. Timing is important: too little and the pancake will not cook, too long or too hot and it will burn. Understandability is key. If you're based in the UK and you try to use a pancake recipe from an American cookbook, you might be confounded by having to make sense of unfamiliar measurements and weights. If you make a mistake, the pancakes will flop. Improving employee resilience by establishing a security awareness training strategy is a process that shares the need for a number of key ingredients, mixed together, and given time to come together and produce their desired outcome.

Some organisations think that they can deliver security awareness training in one session, almost like some kind of inoculation. Having thereby delivered warnings and imparted the information and skills employees need, they feel they have ticked the "security awareness and training" box, and all will be well. This is like trying to make a pancake using the wrong or too few ingredients and without allowing the resulting mixture to rise slowly over a heat source.

Many essential elements are required to improve employee resilience to cyber attack, and to encourage good security hygiene. The security awareness "whole" requires a number of "parts": the parts interact and support each other to help foster and build resilience over time. It takes time for the security practices to penetrate, to be interpreted and to become part of the organisation's culture of operation.

The parts you use to build resilience should be chosen with great care. In the first place, the requirements imposed on employees have to be feasible and understandable. Mandating procedures that users find impossible to align with will eventually lead to apathy and disinterest and an eventual failure of the awareness programme.

Recommendations for the ingredients of a good security awareness programme:

1) Training ought to be scenario-based, not a mere list of rules. This helps people to contextualise the required security behaviours.
2) Training should explain the **value** of particular security practices, and highlight their contribution to the continuing survival and profitability of the organisation.
3) You should not try to scare or shame people into behaving security; this is counter-productive.
4) Encourage people to report near misses, successes and also when they make mistakes. There should be no reprisals for such reporting. The aim is security, not payback.
5) Management buy-in is essential. Many academic studies have shown that "*do what I say, not what I do*" will render all interventions redundant and eventually fail in terms of improving resilience.

Cyber resilience requires a repeated delivery and implementation of many different interventions. This is more akin to a process than a one-off inoculation that is delivered to employees to "fix" them. Organisations have to deliver ongoing training to keep people up to date with the latest attacker strategies.

There is simply no shortcut in terms of building employee resilience. Attackers are becoming ever more determined, computers (and smartphones) are hyper-connected, and technology advances rapidly. It is impossible to be 100% secure; the only way we can possibly get close is to be realistic about how to improve resilience, and to put some effort into helping employees to weave security practices into their day-to-day lives.