Effective Security Awareness Programmes

Michael Barwise

Real, effective awareness programmes have to be very specific to your business, as they primarily operate at the business process level, not the technical, and have to be closely integrated with the development of those business processes. Getting a bunch of people into a spare room and talking about passwords is not awareness training - it's a tiny component of a relatively small technical part of it.

Security only sticks if it ceases to be an externality to your people. They're busy doing their real jobs, so if they have to remember extra stuff (security rules) on top of that, when the pressure is on they'll forget. So the ideal is for working practices to be designed with security in mind (eliminating the externality) and for awareness training to primarily consist of explanation as to why they're like that. That way, your staff are on your side and you've covered most of the bases in your processes, so your staff only have to deal with exceptions to the rule. Then, you have a reasonable chance of minimising your exposure.

Mostly, though, policies impose - frequently arduous - obligations on individual users, often to cover exposures that could better be covered by technical or process measures. These policies are thrown at new staff to read and sign off against in the rush of enrolment when they join, and subsequently serve as punitive instruments to thrash individuals with when occasional (often inevitable) breaches occur. Awareness training in such a regime consists of lots of arbitrary rules that folks have to remember on top of their day-to-day workload. Your staff will resent or ignore most of it, as you yourself would.

For awareness training to work, it has to be created in concert with your security policies, which in turn must be reciprocally interdeveloped with your business processes. So off the shelf awareness programs work no better than off the shelf policy sets - which is often hardly at all. At the end of the day, you're protecting your business, so the protection must be tuned to its specifics.

So your awareness training programme must be "original". What can save you work (and improve effectiveness) is an off the shelf awareness training framework. That's about how the training is presented and delivered. The hierarchy is framework ⇒ programme ⇒ content. The first has been well researched and methods have been optimised for different scenarios, so it's worth making use of that. The second and third have to be your responsibility as they are critically dependent on their fit to your business for effectiveness. Otherwise you'll just have a simulacrum that gives you a false sense of security.

Originally appeared on LinkedIn, November 2010