Security Awareness Training

One of the few good security metrics

Taz Wake
Halkyn Consulting Ltd
Security & Risk Management Specialists

Security Awareness Training – One of the few good security metrics

Recently we discussed both the value and problems around developing security metrics as part of your organisations overall management strategy. One of the best metrics you can generate revolves around security training and staff awareness. It vastly outweighs the value of measuring additional activities like patching within 30 days or updating AV data bases.

Properly delivered, security training is one of the most cost effective ways you can improve your organisation's security posture (we discussed this topic last year) and if you don't currently have a rigorous programme for delivering awareness training, you really should develop one now.

The important question is how do you ensure that your security awareness training is properly managed and working to support your organisations goals.

This is where it links into your security metrics – but you have to make sure that you measure properly; otherwise you create a situation where human nature will conspire against you.

When it comes to awareness training, there are three factors you need to consider – and all of these can be used to build metrics if it is in the interests of your organisation's management goals.

1. **Attendance**. Everyone within your organisation should attend your security awareness training. No one is too senior or too junior, too important or too unimportant for them to not need to know your policies. A metric you can build around this is fairly simply counting how many of your staff attend each session and using this to track until you hit 100% for each training cycle.

2. **Understanding**. Simply attending security awareness sessions is a good start, but this doesn't account for the fact that people will day dream through lectures and fail to understand key concepts. Good awareness training packages will come with some

form of assessment which can be used to measure understanding and this provides a useful metric for your management. Most organisations will stipulate a “pass mark” and then measure what percentage of staff reach this, mandating additional training for those who fail.

3. **Follow On Testing**. It is a mistake to think that giving your employees a 45 minute presentation once a year (even if they are tested at the end of the session) is a solid way to improve your organisation’s security culture. Unless people are frequently reminded about security, it is easy for it to slip and people will revert to previous bad habits. One good way to combat this is to have a “security test” process which runs between formal sessions and serves as both a reminder for your employees and an assessment of how much they have retained since the last formal session. This can be as simple an automate process – using on-line tools – or it can be as formal as running a classroom session. From this you can build metrics showing how many staff have been re-tested and what their scores are. These metrics not only help you measure the changing security culture, they allow you to gauge the effectiveness of your training packages.

As with all metrics, the ones you pick – and how you implement them – must always be driven by your organisation’s culture and goals. However, picking good security awareness metrics is one of the best ways you can measure your security posture and identify cost effective ways to improve it.

About Halkyn Consulting

Halkyn Consulting Ltd is a specialist security consultancy based in North Wales, experienced in providing security advice to local, national and international clients including government agencies, multinational corporations, small businesses and homeowners.

For more advice on how to properly use passwords or any other questions you may have related to security and protecting your home, business or other assets, you can reach Halkyn Consulting at www.halkynconsulting.co.uk or info@halkynconsulting.co.uk.