thirty nine cyber 39

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 10

PRINCIPLE 10 - Staff Awareness & Training

Culture Gem

thirty nine cyber 39

Culture Gem

ASSESS. ADDRESS. **SUCCESS.**

Enabling You to Make the Right Decisions About Your Security.

STUART.AVERY@THIRTYNINECYBER.COM

To the reader

Welcome to my opinion – covering the tenth principle in NCSC's CAF framework – Staff Awareness & Training.
This subject is important and yet to most organisations it is overlooked, training for many lacks innovation and is immediately forgotten once that box is ticked. In fact it's so important I have invited a guest author to add their opinion too, Say Hi to Jemma from Culture Gem.

So here we go...

Key takeaways [TL; DR]

I have discovered that sometimes people don't want to invest in reading the whole document unless they have a good idea of what it covers – ok fair, so I have added a new bit to give you a summary view.

So, what's in it

1. Why it's important to consider your team as a risk as well as an asset
2. What you can do to foster a security focussed culture

Still fancy reading it?

Ok, strap in.

Staff Awareness & Training

Essentially, staff awareness & training is about making sure that the humans you employ to run your business are less likely to create an incident through inexperience or misadventure.
Sounds simple enough, but when you consider how many incidents start with the misinformed action of an employee or agent, it's an area that deserves at least as much focus and resource as the technical controls that you implement.

A tickbox exercise it ain't!

Key Aspects Covered:

1. Cyber Security Culture: You develop and maintain a positive cyber security culture. Embedding awareness so it becomes cultural muscle memory.
2. Cyber Security Training: Training your people to avoid costly mistakes. Using a range of training methods to reinforce awareness.

Jemma from Culture Gem adds:

Organisations benefit from making it straightforward for individuals to understand their role in cyber security. This includes fostering an environment where people know how to raise concerns without fear of negative repercussions. When staff actively participate and collaborate on security efforts, they're more likely to be engaged, bringing unique insights from their areas of expertise that strengthen overall security.

Why is the Staff Awareness & Training principle important?

Why would you invest in making your digital environment resilient and not ensure the user is too. Harden your team not just your systems

Here's why it's important:
Most cyber incidents are caused by Human Misadventure, we are after all, not born with suspicion, we tend to take the path of least resistance and can be too trusting in the familiar, that's just who we are as a species, suspicion and caution are reactions we learn, usually by trial and error or a guiding hand in our early years, that doesn't really change. If your organisation has an appetite for the trial and error approach then stop reading now, if not read on.

It's important to expose your team to cyber threats and compromise techniques in a safe way but does training really work? Is there a better way?
The exposure technique you choose should turn into second nature, this is important because when we are busy we don't tend to pause to consider the training we recieved 12 months ago, it just doesn't work like that.

So should we adopt a more cultural approach backed up by training and awareness programmes?

Jemma's advice supports that view, she writes.
A strong cyber culture is essential for proactive security. Leaders must set a clear example by stressing the importance of cyber security and ensuring that everyone feels accountable for it. For this, executive management must explain the importance of cyber security to all employees, demonstrating that reporting issues is welcomed and supported. When employees know their efforts are recognised, cyber security becomes a shared commitment rather than merely a policy to be followed.

Organisations gain from making it easy for employees to understand their role in cyber security. This includes creating an environment in which people feel comfortable raising issues without fear of negative repercussions. Staff that actively participate and contribute on security activities are more likely to be engaged, offering unique insights from their areas of expertise that improve overall security.

Training to support a deeper cultural awareness isn't just a formal annual exercise; it's a way to build a resilient, informed organisation that views security as everyone's job. Teams that have practical, relevant skills don't just keep systems secure; they directly contribute to safeguarding business continuity and resilience.

Things to consider

There are some considerations to make when approaching Staff Awareness & Training, this isn't exhaustive but may help you define a strategy

Considerations:

- Training for resilience. Training is more than just a one-time exercise; it's about continuous improvement that resonates with everyone, from junior staff to senior leaders. Think about creating a well-structured, inclusive training programme that adapts to varied roles and responsibilities across the organisation.
- Use different methods to reach the greatest number of team members. A mix of teaching methods ensures training reaches the widest possible audience. Accessible information and regular training refreshers keep cyber security awareness alive and relevant.
- Build a cyber security culture. Promote behaviours like raising concerns and sharing experiences, positively recognise your team for raising suspicious behaviour like phishing attempts or spoofed emails. Ensure the senior management team set an example and communicate regularly on cyber security matters
- Access to information. Ensure that information regarding cyber compromise techniques are accessible to the broad user base NOT just the IT team
- Measure progress. It's essential to track training progress, evaluating effectiveness and identifying areas for improvement.

Ok so I hope that all made sense, I'd love to hear from you if you agree or disagree, I want to thank Jemma at Culture Gem for her sage advice and narrative. If you want to discuss a particular area in more depth you can reach out to me at stuart.avery@thirtyninecyber.com or Jemma at jemma.davis@culturegem.co.uk

Like this? Please follow ThirtyNines LinkedIn page – https://www.Linkedin.com/company/thirtyninecyber and read more in this series as they are released.