LAYER 8 SECURITY
THE HUMAN FACTOR

LAYER 8 SECURITY BASELINE - IN SHORT

Understanding, not only the knowledge of staff, but also their way of thinking and behaving towards security is essential in business today to help to better address the risks that staff pose to cyber security.

To do this, we have built the Baseline program, (a human behavioural gap analysis) to not only provide a good picture of your human risk, but to also allow you to focus the training to the people that require it as well as providing a point of Base to measure your progress in your journey of human risk reduction.

As staff all have different needs and strengths, as such we need to ensure that we target the areas that each person requires to make them the most security efficient people to help reduce the risks to our organisations.

As some people may already be proficient strengths (behaviourally) with certain topics of security, it would be unproductive to put them through training courses in these topics. It is better to focus staff training into areas that they require it most.

There are also certain people who don't believe that security is their responsibility. These people wouldn't pay serious attention to any training and as such, no change in behaviour. These people need guidance as to why they need to undertake a different perspective towards security.

Others may be too busy to undertake training and these people may need tailored training to work within their busy schedules.

Ultimately, everyone is different, and we use the Baseline program to identify any individual concerns or issues to better target the training.

The Layer 8 Security B.A.C.K.S program stands for Behaviour, Attitude, Culture and Knowledge for Security. This is an integral part of establishing the Baseline report, to help identify the areas that require attention.

Contact: information@layer8security.com.au
Web: https://layer8security.com.au
Phone: 1300 536 706

The complete B.A.C.K.S program consists of much more than a questionnaire to the staff. We utilise the framework of understanding the following:

- Past behaviour – historical behaviour within the organisation and personally
- Current behaviour – simulated social engineering to ascertain their current behaviour, not just at a single point of time, but over a period and under certain stimuli
- Perceived behaviour – understanding how they think they behave
- Corporate impact on their behaviour – how the culture and policies are causing them to behave

It provides an excellent tool to plan the best methods of education as well as what else needs to be done to address the human factor.

Just creating awareness or knowledge alone, won't succeed in identifying the staff's understanding of:

- Security principles,
- Their attitudinal and Cultural issues,
- Their Knowledge and Understanding of the topics,
- Their Motivation, and Ego based concerns
- Which all ultimately lead towards changes in their behavioural components.

The B.A.C.K.S report also provides us with an excellent tool to focus the training components into where they are best needed. It's like using a scalpel rather than a shotgun approach. We can identify the topics, by department of down to individual users, if needed, that should be addressed.

These areas of concern are broken down into four specific areas:

- Behaviour – how are they behaving and how would they behave in certain circumstances.
- Attitude – what are their attitudinal contributors that are being impacted by internal and external factors
- Culture - How is the culture of TRC impacting attitudes and subsequently, behaviour
- Knowledge – Do your staff understand the information.
- For Security

Contact: information@layer8security.com.au
Web: https://layer8security.com.au
Phone: 1300 536 706

All these areas provide an invaluable tool and subsequent report to ensure the maximum success from the program to reduce the human risk associated with security.

The output of the extensive Baseline report is used to focus the training, measure the success of the program, and ensure that we can have a successful program with measurable ROI. Training and simulated phishing alone won't provide any real metrics of the success of the program.

The metrics that are ultimately used, leading to a change in behaviour are:

- Improvement in knowledge, understanding and retention, not just completion of the training course,
- Reduced susceptibility to social engineering attacks,
- Improved physical security behavioural change,
- Following of the security culture,
- Increase in reporting of suspicious activities
- Decrease in response to attacks,
- Increase in verbal communications about suspicious activities,
- Undertaking a more active role in acceptance of responsibility
- And ultimately, an improvement in behaviour towards security.

Layer 8 Security provides Australian built and focused training activities, reinforcement activities, games, articles, tools, security awareness week, ongoing measurement and tuning of the program, Australian built and focused email and SMS Phishing tools which provide actual localised and configures simulated attacks, and all of our services and tools