Layer 8 Security
B.A.C.K.S Program Overview

INTRODUCTION

All organisations today rely heavily on the internet, information systems, communications systems and collaboration in business, investing significantly in these resources to compete in today's global marketplace. This investment in these organisational systems exposes organisations to risks and threats that can result in major losses such as financial, intellectual property, customers and reputation.

To protect from these risks and threats, organisations often resort to purchasing security technologies to be implemented to protect the organisation.

Technology, people and process are the three core components necessary to address the increasing amount of risk associated with physical and cyber security. Technology alone isn't the answer to addressing security within the organisation. Technology and processes can usually stop around 95% of the threats. That still leaves 5% of attacks coming into your organisation through your people. People are responsible for more security breaches than the other two combined. More than 75% of all breaches are because of human activities or other insider threats.

We need to look at how people behave and how they respond to certain circumstances, stimuli, and situations. Knowledge / awareness alone won't change an organisations risk profile. Just because someone has knowledge doesn't mean that they will do the right thing. What motivates people to act in certain ways? What is their perspective on security as it relates to their personal lives? If their attitude is wrong, or the corporate culture is bad then their behaviour will be in conflict to their knowledge.

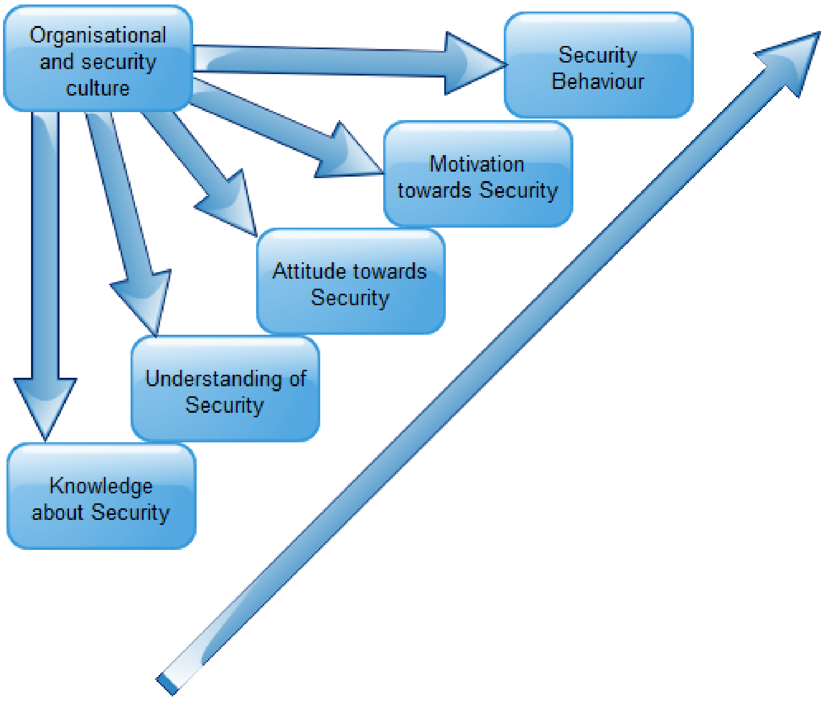
A change in behaviour is the only tangible way to address this component of security risk.

Behavioural change comes with knowledge through understanding, perception, attitude, motivation, impacted by culture towards behaviour.

What's even more important is, with knowledge / awareness alone, there is no way to measure the success of the campaign.

How can you measure your security awareness training program's return on investment when you have no metrics against how people react, respond, think, or feel?

To truly address the people component of security, measurements against attitude, behaviour, culture, and knowledge need to be made.


Organisational and security culture
Security Behaviour
Motivation towards Security
Attitude towards Security
Understanding of Security
Knowledge about Security

Incorporating knowledge through understanding, attitude, motivation, impacted by culture towards behavioural change

Until we all take Security Behavioural Programs seriously, where continuous measurements, refocusing, attitudinal encouragement and a focus towards positive culture based behaviour, human beings will continue to represent a significant component of security breaches.

It is important that Board and executive management are well-informed regarding cyber security risks and their organisation's preparedness to prevent, detect and respond.

To assist you in reducing your risk to security breaches, Layer 8 Security has developed a comprehensive framework utilising advanced methodologies, tools and systems to provide a comprehensive security knowledge, attitude and behaviour "awareness" program. As a component of the program, Layer 8 Security implements this security program in accordance with NIST and ISO27001 requirements.

OVERVIEW

This overview should hopefully assist your organisation to better understand how to address the need to reduce the impact of human error.

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.

The reasoning behind the Baseline report is to provide a gap analysis of the people within your organisation, their strengths and weaknesses.

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 entire Baseline process provides an excellent base for analysis of what human issues are being encountered now, and what level of controls and best practice we are aiming for.

The complete Baseline 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.

Behaviour, unlike awareness, is the ultimate objective of any campaign of this type.

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 Baseline 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:

- Knowledge – Do your staff actually understand the information.
- 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
- Behaviour – how are they behaving and how would they behave in certain circumstances.

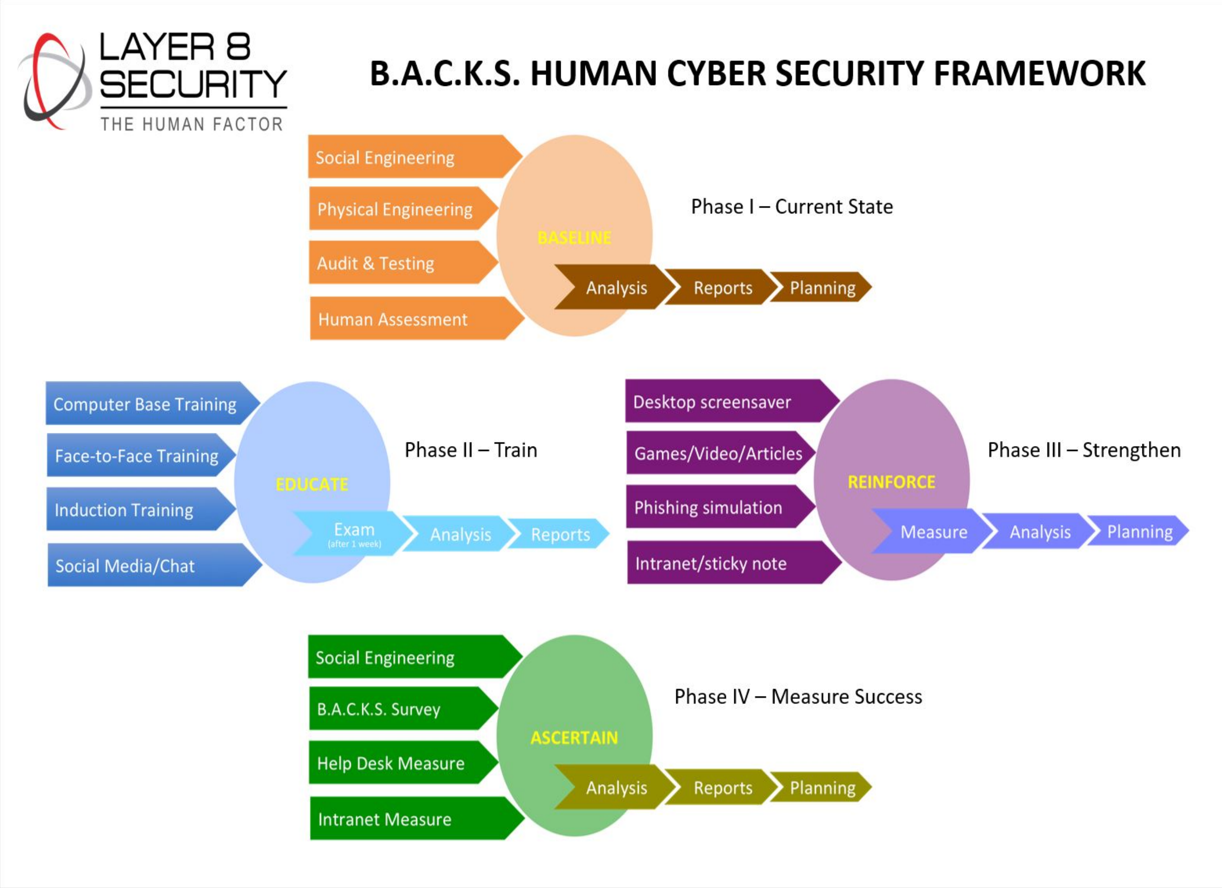
All these areas provide an invaluable tool and subsequent report to ensure the maximum success from the program to reduce the human risk associated with security.

A Baseline is used going forward to measure against for all activities in the future. Training 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 as a whole.

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,



B.A.C.K.S. HUMAN CYBER SECURITY FRAMEWORK

and all of our services and tools can be configured to your organisation with local voiceovers if you wish.

The Baseline is an initial measurement designed to ascertain where the organisation is now with regards to staff behaviour, attitudinal issues, knowledge and understanding of the specific topics, cultural impacts upon the staff, security policies, incident response processes, reporting processes, historical bad actors or behaviours and any other issues that may impact the human side of security.

The accuracy of the baseline measurement is entirely dependent upon the service items selected. The more items selected, the more accurate the results will be.

The results from these services being analysed, is to identify the issues as well as what topics departments require special attention to. It also addresses a complete understanding of the requirements / policies of the organisation and how well the behaviour of the staff maps to these policies.

Ultimately, the Baseline provides an initial measurement that can be compared to industry best practices as well as focus areas that require special attention.

Ongoing measurement throughout the program is undertaken every three months via various testing methods, (Exam results, Simulated attacks, Mini B.A.C.K.S and satisfaction analysis) to not only measure the success factors, but also any educational components that may not be showing the success required. This allows the educational program to be modified quickly to address the issue.

At the conclusion of each year, the ascertainment is undertaken to compare to the previous results to measure the growth and success of the program as it relates to the organisation.

BASELINE

This effectively allows us to undertake a Gap Analysis of your people, what they know, their average attitude towards security, how your current culture impacts their attitude and finally, their behaviour and how they respond to situations. This baseline / Gap Analysis allows us to start to measure the maturity of your staff and the success of the program. Attitudinal factors can be influenced by immediate changes in short term situations, but these are not often long-term influencers.

- Phishing
  - Email - General, Spear phishing & Whaling
  - SMS - General, Spear phishing & Whaling
- Social engineering,
- Physical risk analysis,
- Vishing – Social engineering phone Calls,
- USB drop,

- Wi-Fi risk audit
- Human social penetration test, human vulnerability assessment, human gap analysis, vendor human risk analysis
- Corporate Analysis Questionnaire
- Staff Assessment Questionnaire
- Cultural Analysis,
- Social Media analysis
- Compromised Password / dark web analysis
- Policy and Incident response analysis
- Industry Threat Profile analysis
- Analysis of previous issues relating to human errors, frequency, bad actors, severity, remediation time.
- Reporting of the combined results against NIST and ISO27001 best practices, as well as reporting of the departmental specific requirements
- Planning for addressing the educate components.

The B.A.C.K.S Assessment explained

The B.A.C.K.S user questionnaire is a specially developed analytical tool designed to ascertain the critical components of your staff behaviour.

Behaviour, unlike awareness, is the ultimate objective of any campaign of this type. Just performing awareness or knowledge training alone, won't succeed in identifying staff understanding of security principles, their attitudinal and Cultural issues, their Knowledge and Understanding of the topics, their Motivation, Moods, Emotive and Ego based concerns which ultimately leading towards changes in their behavioural components.

When the 4-minute B.A.C.K.S user questionnaire is undertaken by all staff, the results allow us to ascertain an accurate baseline measurement (where are we now), especially if this is incorporated with the results from other tests like the corporate threat profile and the social engineering simulated attacks. This baseline provides an excellent base for a Gap analysis of what Human issues are being encountered and what level of best practice we are aiming for.

The B.A.C.K.S user questionnaire also provides us with an excellent tool to focus the training components into where they are best needed. Its 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 three specific areas:

- Knowledge – Do your staff actually understand the information.
- Attitude – what are their attitudinal contributors that are being impacted by internal and external factors
- Behaviour – how are they behaving and how would they behave in certain circumstances.

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.

EDUCATE

This process starts with an exciting and engaging interactive session with your staff to help them better understand what the program is all about and why they should actively undertake a proactive approach to cyber security awareness.

We also undertake executive and board level engagement to ensure that there is not only executive buy-in into the program, but also a good understanding of the responsibilities, and consequences of their actions.

Every person learns in different ways, so your standard Computer Based Training (CBT) course isn't going to have the results that you really need.

We then offer to maximize learning and retention with a broad set of focused interactive training modules or even face to face training. Ongoing modules are designed to not impact their busy workload or home life.

- Short assessments are conducted two weeks after any training. Through our research, we have found that if people are presented with a test at the end of training, they utilize short term memory recall to address the test. Unfortunately, cognitive memory is short term, and often doesn't relate to behavioural change.

By advising people at the start of training that the exam is two weeks away with an 80% pass mark required, encourages the students to pay closer attention to the subject matter to ensure that they pass the assessment. This enforces the building of memories and subsequent habits around knowledge and behaviour.

To further enhance the experience, this is then followed up with regular engagements to discuss security and to update them on their progress

CYBER ESCAPE
ROOM

and any new attack vectors being encountered around the world. The components may consist of all or some of the following:

- CBT training - Fully customizable security training portal which provides course packages that are SCORM compliant and can be utilized from any standard LMS.
- Face to Face sessions conducted as discussion groups, lunch and Learn or training sessions.
- Induction training incorporating simplified security awareness training as well as interactive instructor led sessions
- Physical team building games, like escape rooms to address solving security challenges.
- Discussion groups, these sessions are expected to comprise 1-hour sessions of interactive presentations and discussions. Staff team building and encouragement sessions to increase communications and the willingness to openness and collaboration
- Hacking demonstrations, with discussions with the experts to understand how the criminals undertake the attacks.
- Executive and Board discussion groups tailored to the specific requirements of the business and the threats.
- LMS delivery is available if desired

The results of any training is analysed for results, attendance, and improvements.

REINFORCEMENT

Reminding your employees about best practices is essential and can be undertaken by bringing messaging into the workplace and providing methods for them to report suspicious activity, providing positive feedback for each reporting instance.

- Screen savers,
- Reinforcement materials,
- On-line Games,
- Desktop Wallpapers,
- Animated videos,
- Posters if required,
- Monthly articles and updates,
- Postit campaign
- Intranet program
- Security Awareness Week
- Cyber Escape Rooms

These items are configured to exactly fit your corporate standards and culture.

ASCERTAINMENT

To further assist our customers, we also offer a service to measure the success of your Program. This program is best combined with our Baseline service which would provide a strong measurement of the success of your program.

To ensure the success of your program, measurement of the success of the participants needs to be undertaken and compared to the results from the baseline assessment done earlier.

Just looking at the quantity of help desk tickets is unlikely to provide any insight into the success of the awareness training program. We often find that after the program, the quantity of tickets addressed via the help desk increases as the employees are now more aware of what to look for and hence, what they report to the help desk.

The assessment needs to address such issues as the severity of the help desk tickets, remediation times, how easily employees are fooled by new simulated attacks, a comprehensive analysis survey, as well as the quantity and quality of issues reported to the help desk. We also need to look at the changes in attitude, motivation and ultimately, behaviour.

As users are completing their training assignments, we can monitor the results and look back over the data that was gathered throughout the assessment and training steps. You'll be able to review employees' interactions with the Security knowledge, Attitude and Behaviour Risk profiler. You'll have access to detailed information about who completed which assignments, who fell for specific simulated attacks, which concepts employees understand well, how your culture is impacting their attitude, topic areas of weakness, and improvements over time and finally the change in behaviour and the impact that is having on reducing your risk.

At any point in the cycle, we can provide reports as a summary of results to managers, human resources, executives, and any other interested parties.

Components of ascertainment are:

- Phishing – at 3-month intervals and then again at 12 months – looking for trends – Email & SMS
- BACKS Assessment Questionnaire at 12 months – ascertain if it has it improved
- Help Desk assessment – issue quantity, severity, and time to remediation
- Password / dark web analysis – 12 months – has it been reduced
- Data collection of
    1. Data analysis
    2. Gap Analysis against Baseline
    3. Risk determination
    4. Report built
    5. Report presented