LAYER 8 SECURITY
THE HUMAN FACTOR

COMPANY NAME
YOUR SAMPLE TEXT HERE

Human Security Risk & B.A.C.K.S BASELINE Report

Report compiled by
Layer 8 Security
Date:

Contents

Introduction to the Baseline Report 3
Synopsys 4
SAMPLE COMPANY Summary 7
- Completion rate 10
- SAMPLE COMPANY user questionnaire Average Scores 10

Behaviour, Attitude, Culture and Knowledge for Security user Questionnaire 11
- Attitude 12
- Knowledge 14
- Behaviour 16

Departmental Breakdown 17
Corporate Threat Profile 19
Topics 20
Recommendations 21
- Topic 22

Introduction to the Baseline Report

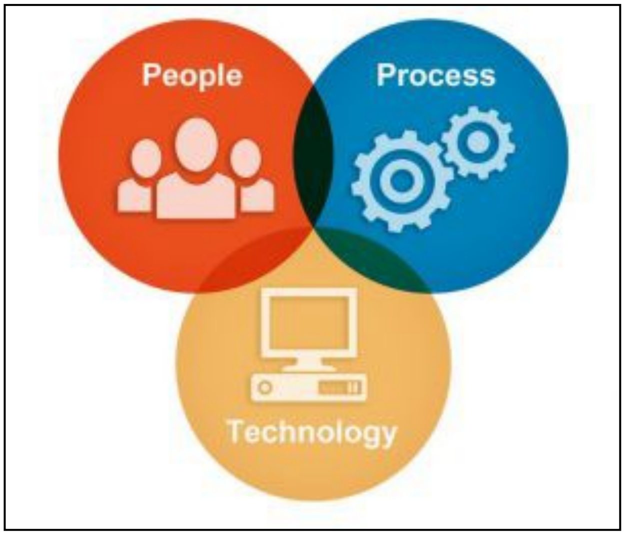
SAMPLE COMPANY engaged with Layer 8 Security to undertake an initial program of work to perform an analysis of staff behaviour as it pertains to security awareness and identify areas that require further attention.

This report is identified as the "Human Risk and Baseline Report" under which controls can be put in place to address the areas that are identified as high risks to SAMPLE COMPANY.

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 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 any organisations. Fully updated and perfectly configured technology can usually stop around 95% of the threats. That still leaves 5% of attacks coming into your organisation through your people.

As identified by the recent OAIC report, people are responsible for more security breaches than technology and processes combined. More than 75% of all breaches are due to human error or other insider threats. People are the first line of defence, not the last. If a person makes a mistake, we can only hope that the technology will prevent a breach, not the other way around.

This report is designed to be the initial piece of documentation outlining the issues within SAMPLE COMPANY as well as a breakdown of the issues and areas that require focus during the planning stage going into the educate phase.

Synopsys

The Baseline stage is designed to look at the staff behaviour as well as basic attitudes, cultural impact as well as an understanding of the topics.

The current program is designed to identify behavioural issues incorporating historical activities and current behaviour.

Like any project, a Baseline needs to be established to ensure that the current state is identified and measured prior to attempting to address any issues. Understanding the Gap between where you are now and where you desire to be is critical.

The Baseline uses a culmination of components, simulated attacks, questionnaires, organisation al components as well as analysis of past and present behavioural activities.

The foundation of the Program is to analyze staff behaviour, the factors that contribute to their behaviour and to then formulate a program to address these issues.

This B.A.C.K.S user questionnaire is designed to be an initial analysis of the components of staff perception of their behaviour. Staff complete the questionnaire, providing an insight into what they understand, how they feel about certain aspects of security, how the culture impacts their behaviour as well as their behaviour as it relates to security.

The B.A.C.K.S questionnaire and subsequent report are combined with the results from the social engineering attacks, historical data from the help desk analysis and other Baseline components. The results from these activities are collated, collaboratively analysed and assessed to formulate a report that will provide indicators of behavioural problems, attitudinal issues, cultural impact as well as understanding of the subject matter.

The corporate analysis also allows for a focus to be placed on areas that may be counterproductive to the corporate requirements and the staff behaviour. E.g., this could encompass the password policies and the way staff address their methods of addressing password changes.

The Corporate Threat Profile provided by the CISO or CIO is also utilised to better understand the corporate perspective of staff and this is then married to the B.A.C.K.S to get a two-sided view of the human component within the organisation.

The report can be presented at a departmental level or, if mandated by the organisation, drilled down to the individual users.

Attitudinal issues are often identified at a broad level, but further testing, including individual discussions will provide more in-depth understanding as to the actual attitudinal issues. Historical data pertaining to specific department is utilised to further provide in depth details around specific departmental concerns.

Comprehensive measurement metrics are utilised to ensure that the program always stays on track as well as provides the optimum results desired by the organisation.

The program is built to provide a measurable, continuous program, over the minimum of one year, to address security awareness, behavioural modification and education.

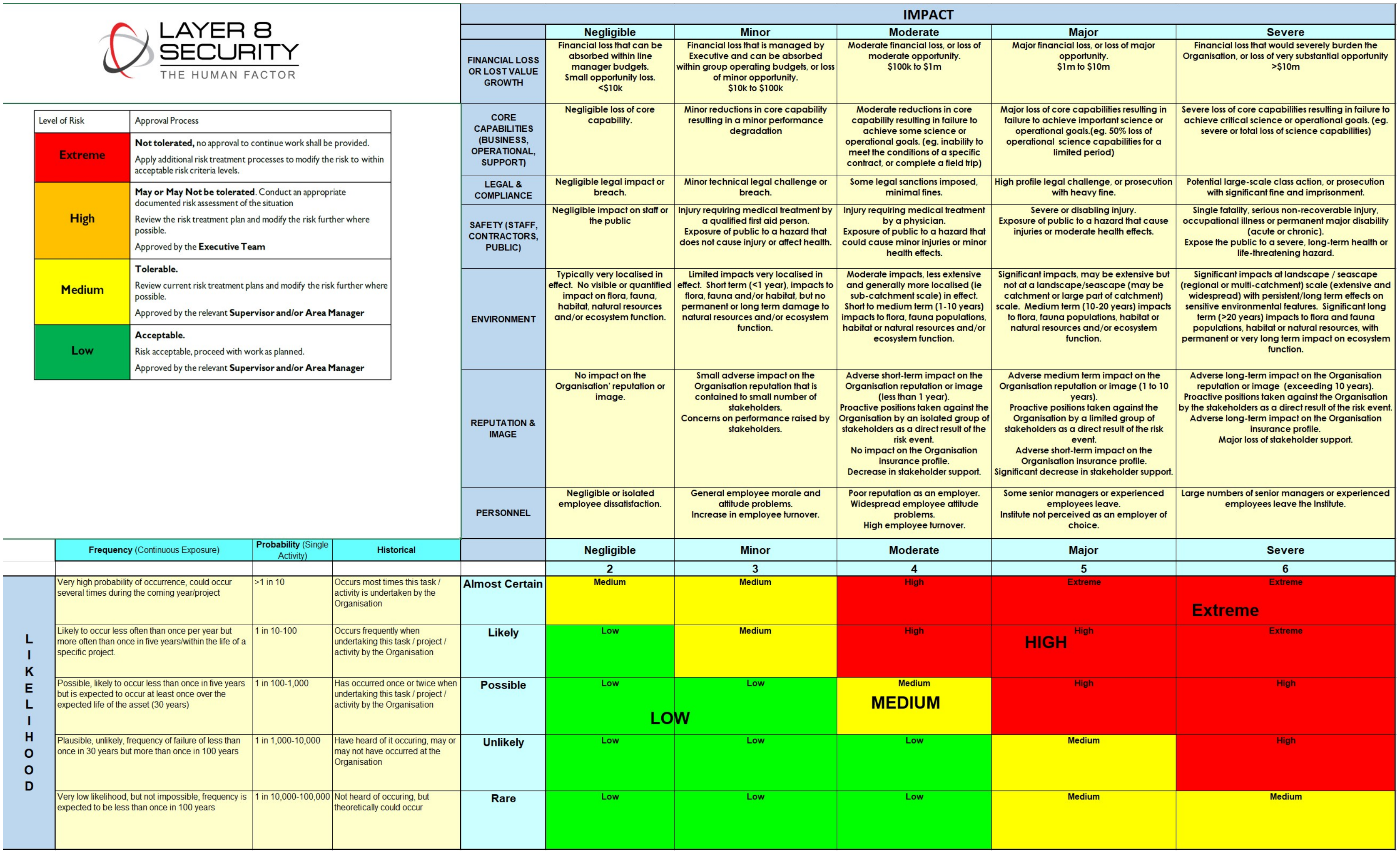
The final Baseline report provides comprehensive analysis of individuals, teams as well as corporate wide areas that require attention.

The final report also provides an insight into the areas that require specific focus in the education area. These may be certain courses to address certain departments, or maybe areas to address certain behavioural or attitudinal issues.

At the end of the Baseline, a comprehensive planning session is undertaken to ensure that the program is addressed to achieve the maximum success factors.

The risk rating was calculated from the chart below.

See last page for a clearer version.



Level of Risk	Approval Process
Extreme	**Not tolerated,** no approval to continue work shall be provided. Apply additional risk treatment processes to modify the risk to within acceptable risk criteria levels.
High	**May or May Not be tolerated**. Conduct an appropriate documented risk assessment of the situation Review the risk treatment plan and modify the risk further where possible. Approved by the **Executive Team**
Medium	**Tolerable.** Review current risk treatment plans and modify the risk further where possible. Approved by the relevant **Supervisor and/or Area Manager**
Low	**Acceptable.** Risk acceptable, proceed with work as planned. Approved by the relevant **Supervisor and/or Area Manager**

IMPACT					
	Negligible	Minor	Moderate	Major	Severe
FINANCIAL LOSS OR LOST VALUE GROWTH	Financial loss that can be absorbed within line manager budgets. Small opportunity loss. <$10k	Financial loss that is managed by Executive and can be absorbed within group operating budgets, or loss of minor opportunity. $10k to $100k	Moderate financial loss, or loss of moderate opportunity. $100k to $1m	Major financial loss, or loss of major opportunity. $1m to $10m	Financial loss that would severely burden the Organisation, or loss of very substantial opportunity >$10m
CORE CAPABILITIES (BUSINESS, OPERATIONAL, SUPPORT)	Negligible loss of core capability.	Minor reductions in core capability resulting in a minor performance degradation	Moderate reductions in core capability resulting in failure to achieve some science or operational goals. (eg. inability to meet the conditions of a specific contract, or complete a field trip)	Major loss of core capabilities resulting in failure to achieve important science or operational goals.(eg. 50% loss of operational science capabilities for a limited period)	Severe loss of core capabilities resulting in failure to achieve critical science or operational goals. (eg. severe or total loss of science capabilities)
LEGAL & COMPLIANCE	Negligible legal impact or breach.	Minor technical legal challenge or breach.	Some legal sanctions imposed, minimal fines.	High profile legal challenge, or prosecution with heavy fine.	Potential large-scale class action, or prosecution with significant fine and imprisonment.
SAFETY (STAFF, CONTRACTORS, PUBLIC)	Negligible impact on staff or the public	Injury requiring medical treatment by a qualified first aid person. Exposure of public to a hazard that does not cause injury or affect health.	Injury requiring medical treatment by a physician. Exposure of public to a hazard that could cause minor injuries or minor health effects.	Severe or disabling injury. Exposure of public to a hazard that cause injuries or moderate health effects.	Single fatality, serious non-recoverable injury, occupational illness or permanent major disability (acute or chronic). Expose the public to a severe, long-term health or life-threatening hazard.
ENVIRONMENT	Typically very localised in effect. No visible or quantified impact on flora, fauna, habitat, natural resources and/or ecosystem function.	Limited impacts very localised in effect. Short term (<1 year), impacts to flora, fauna and/or habitat, but no permanent or long term damage to natural resources and/or ecosystem function.	Moderate impacts, less extensive and generally more localised (ie sub-catchment scale) in effect. Short to medium term (1-10 years) impacts to flora, fauna populations, habitat or natural resources and/or ecosystem function.	Significant impacts, may be extensive but not at a landscape/seascape (may be catchment or large part of catchment) scale. Medium term (10-20 years) impacts to flora, fauna populations, habitat or natural resources and/or ecosystem function.	Significant impacts at landscape / seascape (regional or multi-catchment) scale (extensive and widespread) with persistent/long term effects on sensitive environmental features. Significant long term (>20 years) impacts to flora and fauna populations, habitat or natural resources, with permanent or very long term impact on ecosystem function.
REPUTATION & IMAGE	No impact on the Organisation' reputation or image.	Small adverse impact on the Organisation reputation that is contained to small number of stakeholders. Concerns on performance raised by stakeholders.	Adverse short-term impact on the Organisation reputation or image (less than 1 year). Proactive positions taken against the Organisation by an isolated group of stakeholders as a direct result of the risk event. No impact on the Organisation insurance profile. Decrease in stakeholder support.	Adverse medium term impact on the Organisation reputation or image (1 to 10 years). Proactive positions taken against the Organisation by a limited group of stakeholders as a direct result of the risk event. Adverse short-term impact on the Organisation insurance profile. Significant decrease in stakeholder support.	Adverse long-term impact on the Organisation reputation or image (exceeding 10 years). Proactive positions taken against the Organisation by the stakeholders as a direct result of the risk event. Adverse long-term impact on the Organisation insurance profile. Major loss of stakeholder support.
PERSONNEL	Negligible or isolated employee dissatisfaction.	General employee morale and attitude problems. Increase in employee turnover.	Poor reputation as an employer. Widespread employee attitude problems. High employee turnover.	Some senior managers or experienced employees leave. Institute not perceived as an employer of choice.	Large numbers of senior managers or experienced employees leave the Institute.

	Frequency (Continuous Exposure)	**Probability** (Single Activity)	**Historical**		Negligible	Minor	Moderate	Major	Severe
					2	3	4	5	6
LIKELIHOOD	Very high probability of occurrence, could occur several times during the coming year/project	>1 in 10	Occurs most times this task / activity is undertaken by the Organisation	Almost Certain	Medium	Medium	High	Extreme	Extreme Extreme
	Likely to occur less often than once per year but more often than once in five years/within the life of a specific project.	1 in 10-100	Occurs frequently when undertaking this task / project / activity by the Organisation	Likely	Low	Medium	High	HIGH High	Extreme
	Possible, likely to occur less than once in five years but is expected to occur at least once over the expected life of the asset (30 years)	1 in 100-1,000	Has occurred once or twice when undertaking this task / project / activity by the Organisation	Possible	Low LOW	Low	Medium MEDIUM	High	High
	Plausible, unlikely, frequency of failure of less than once in 30 years but more than once in 100 years	1 in 1,000-10,000	Have heard of it occuring, may or may not have occurred at the Organisation	Unlikely	Low	Low	Low	Medium	High
	Very low likelihood, but not impossible, frequency is expected to be less than once in 100 years	1 in 10,000-100,000	Not heard of occuring, but theoretically could occur	Rare	Low	Low	Low	Medium	Medium

SAMPLE COMPANY Summary

SAMPLE COMPANY contracted Layer 8 Security to conduct the Baseline analysis on all SAMPLE NUMBER staff.

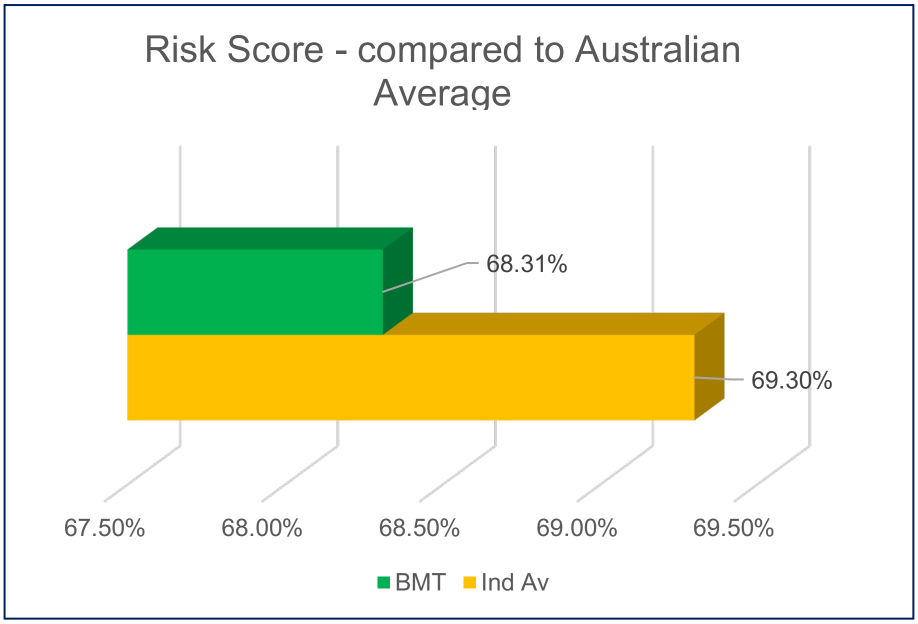
Percentage
>80% = LOW RISK
70% to 80% = MEDIUM RISK
55% to 70% = HIGH RISK
<55% = EXTREME RISK

The program was focused on all the staff of SAMPLE COMPANY. Due to the makeup of the company, we were able to test and analyze most of the staff to the level desired, and the testing completed has provided an excellent insight into the organisation.

The testing encompassed Corporate Threat Profile as well as the B.A.C.K.S staff questionnaire and some simulated Spear Phishing.

This questionnaire was sent out on SAMPLE DATE and remained open until SAMPLE DATE to all staff. The results obtained from the SAMPLE NUMBER of staff who completed the questionnaire was subsequently analysed to determine the risk level per person, and as a company overall as well as to pinpoint specific issues within them, along with SAMPLE COMPANY's overall level of risk as a company.

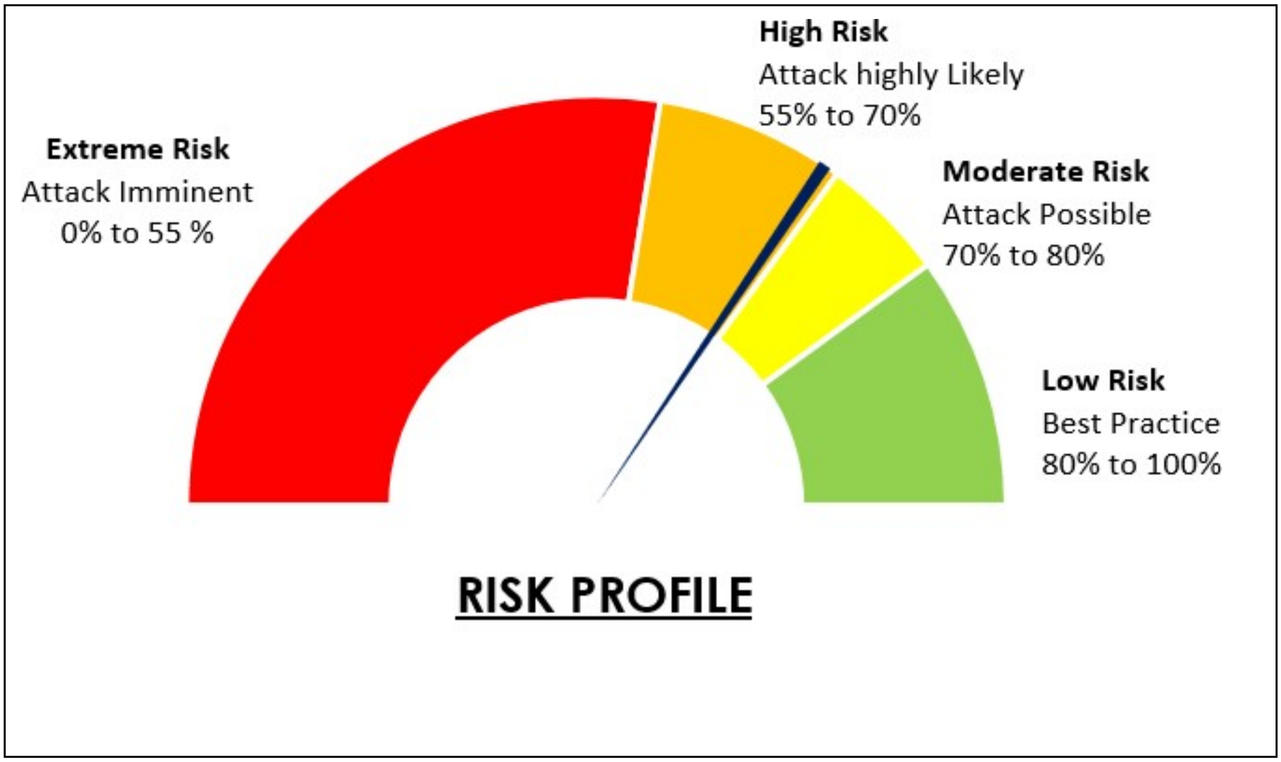
We have confidentially identified individuals to aid SAMPLE COMPANY in the efforts to monitor certain people who may pose a greater risk to the organisation.



This data is available upon request.

Total Overall risk score was 68.31%, incorporating all staff who completed the B.A.C.K.S questionnaire. It is understood that certain people were unable to complete the questionnaire due to other commitments

Compared to the industry average score, SAMPLE COMPANY compared on an equivalent level, and this score is considered a moderate to high risk.



This report incorporates the results from the "Corporate Threat Profile" as well as the "B.A.C.K.S (Behaviour, Attitude, Culture, Knowledge for Security) questionnaire.

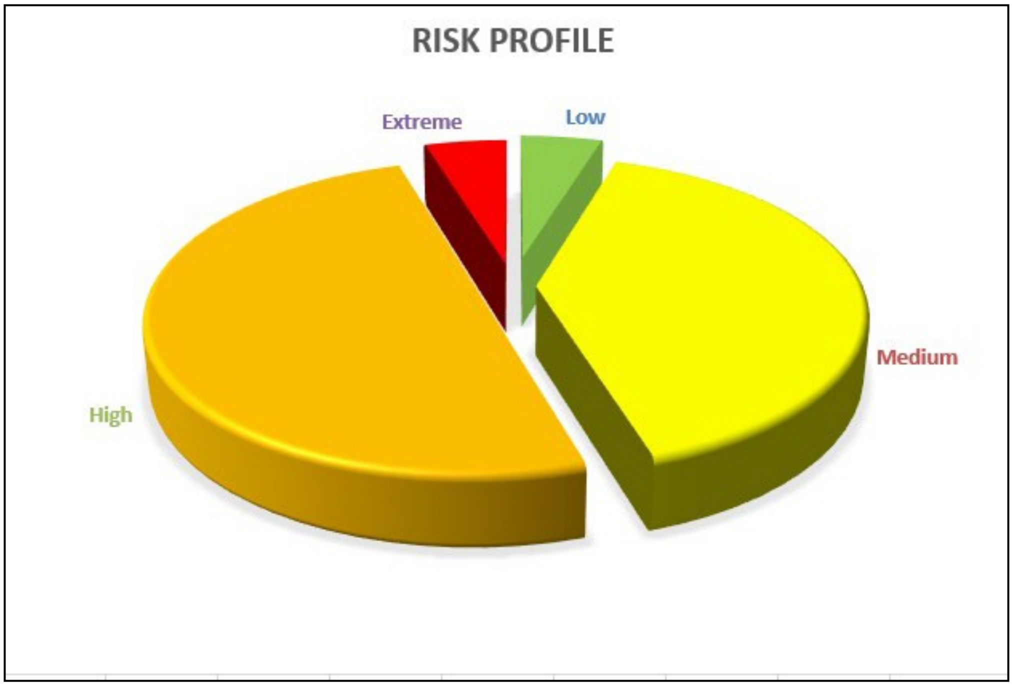
More in-depth analysis can be undertaken utilizing additional components like help desk ticket analysis to provide historical data, and current behaviour patterns against certain operational stimuli.

Overall, SAMPLE COMPANY performed quite well from a risk perspective against the Australian industry.

SAMPLE COMPANY was compared to other Australian manufacturing organisations as well as the Australian Industry (government and corporate) as a whole.

The industry average is calculated utilising data from government organisations, ASX listed companies, healthcare, financial services industry, critical infrastructure, and other organisations.

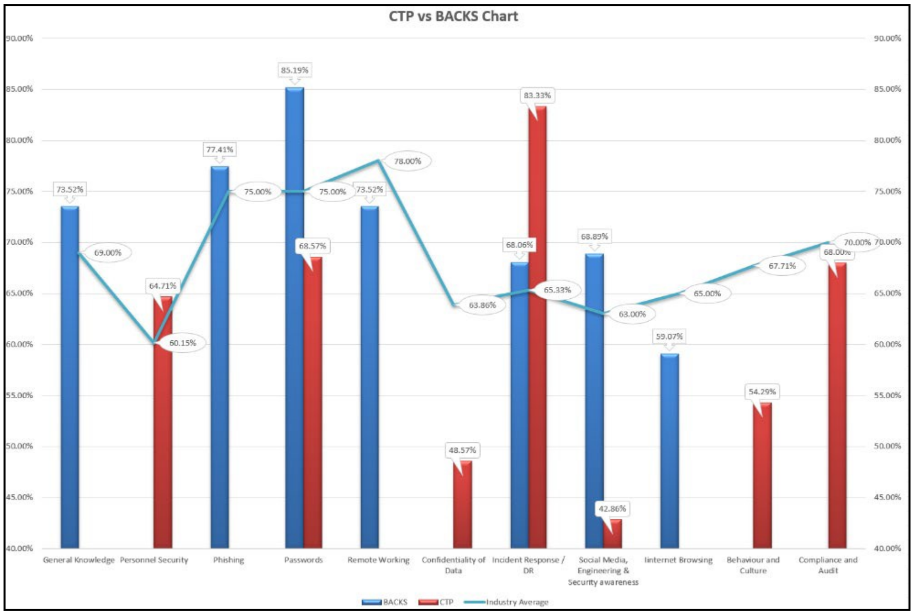
When the social engineering exercise was undertaken,SAMPLE NUMBER people failed this exercise. This represented SAMPLE PERCENT of SAMPLE COMPANY and as such was considered an extreme risk. Notwithstanding, SAMPLE PERCENT of phishing exercises didn’t undertake the B.A.C.K.S questionnaire which places these people in the Extreme risk category.



If we take all staff into account, attributing a higher risk value to the staff who didn’t undertake the questionnaire we can see a risk profile as depicted by the pie graph.

This data is comprised of all staff, the ones who completed the questionnaire, the two who partially completed the questionnaire, and the ones who didn’t, as well as factors correlated from the social engineering attacks.

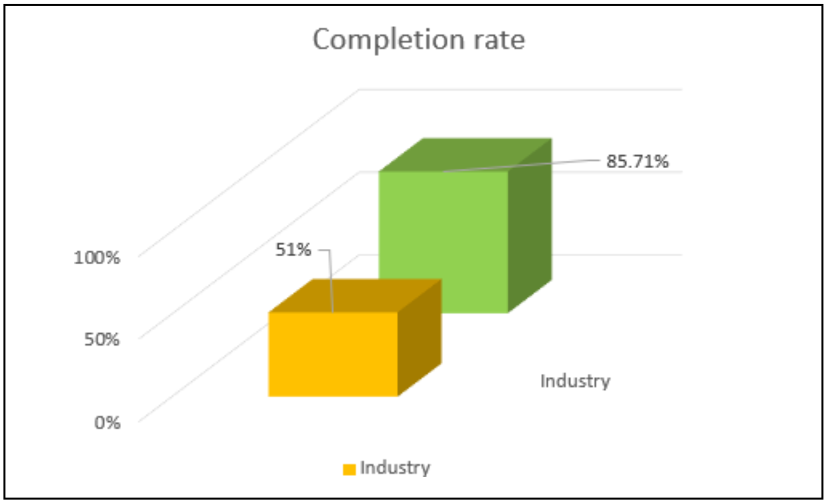
The graph shows the BACKS and CTP measured against the industry average.



Completion rate

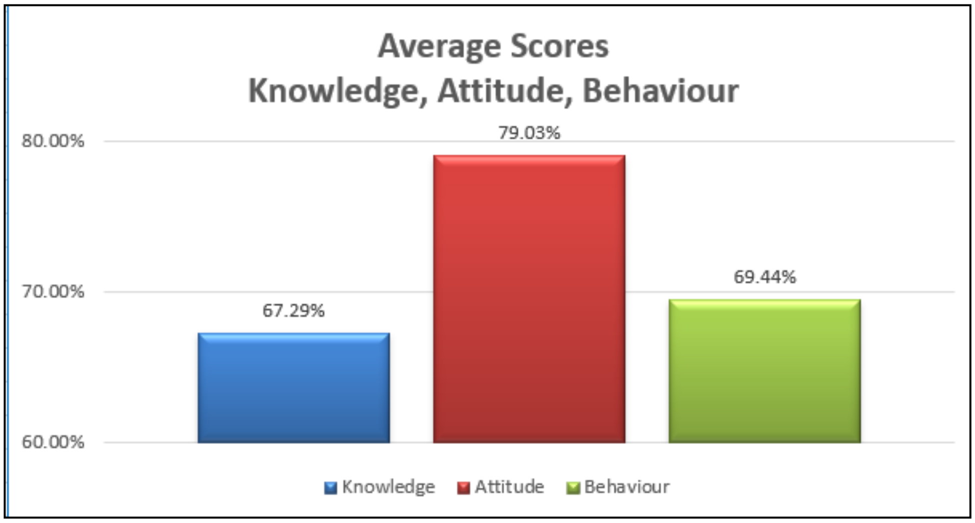
Another factor that we analyse is the actual completion rate of the questionnaire.

The normal completion rate for this questionnaire is measured at 51%, whereby SAMPLE COMPANY achieving a completion rate of 85.71%, which is considered excellent. This reflects well on the culture within SAMPLE COMPANY.



SAMPLE COMPANY user questionnaire Average Scores

As can be seen from this graph, the scores for the participants who completed the B.A.C.K.S was quite good. Attitudinal factors were within the best range that we have seen to-date.



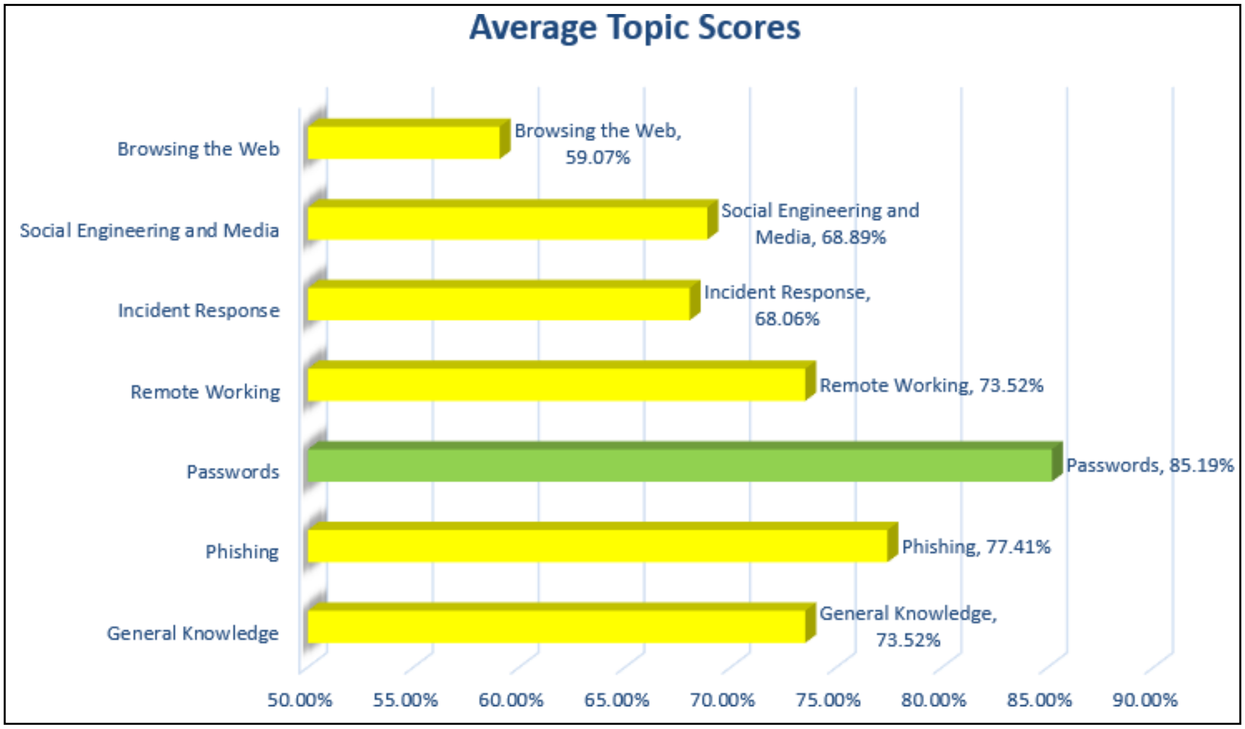
The company average indicates overall performance. Further breakdown is undertaken later in this document.

- Attitude is very good with a score of 79.03%.
- Behaviour as also reasonably good with a score of 69.44% which is a good reflection of how the staff are currently behaving around security.
- Knowledge is not too bad with a score of 67.29%

Overall, SAMPLE COMPANY did very well from the people that completed the questionnaire.

Behaviour, Attitude, Culture and Knowledge for Security user Questionnaire

The table below provides an interesting insight into the related score from the B.A.C.K.S questionnaire subjects. These scores were compiled utilising algorithms and data achieved using industry analysis in accordance with NIST and historical data.



The average scores are the average for the specific topics incorporating knowledge, attitude and behaviour.

As can be seen from the subject graph above, there are a few specific areas where further attention needs to be placed, Internet Browsing and Social Engineering (High risk topics).

Passwords achieved a very high score and subsequently would be considered a low risk to SAMPLE COMPANY.

Attitude

Attitude average
79.03% Low to Medium Attitude Risk

We have identified from the current research that employee attitudes towards cybersecurity were negatively correlated to the frequency with which they engaged in risky cybersecurity behaviours.

The capacity to instill good cybersecurity behaviour should be viewed as being of paramount importance for all organisations, irrespective of their size and complexity.

However, it is apparent that from the responses to the attitude scale this is not always the case, with pockets of individuals appearing to be disengaged or ill equipped to act appropriately.

In many organisations, staff devolved responsibility of company cybersecurity to management or IT, with more indicating that they did not know how they could protect the company from cybercrime.

Historically, we have seen more issues with attitude than with awareness.

Fortunately for SAMPLE COMPANY, the results from the people who completed the B.A.C.K.S questionnaire, there seems to be a very good attitude. This can often be attributed to a caring and collaborative culture within the organisation.

As indicated earlier within this document, 21% of these people were caught during the social engineering exercises, didn't complete the B.A.C.K.S user questionnaire which indicates a poor attitudinal focus for these people and an extreme risk for SAMPLE COMPANY.

Just because people know what to do, or have been made aware, it doesn't correlate to their behaviour. Some of the reasons given by people within other organisations are:

The attitudinal issues that often impact Security behaviour are:

- Aggressive – I don't have time for this rubbish.
- Arrogant – I know what to do, you can't tell me.
- Devolved – It's an IT responsibility to protect us, not mine.
- Dishonest – Malicious intent – I want to cause damage!
- Distant – I am too busy.
- Hostile – I don't want someone telling me what to do.
- Ignorance – It's just a job to me.
- Indifferent – I just don't care.
- Intolerant – Nothing seems to make a difference.
- Irresponsible – It's not my problem.
- Pessimistic – What difference will it make?
- Prejudiced – We employ idiots, they can't do anything right.
- Prideful – I already know better than they do.
- Salary – I'm not paid enough to care.
- Selfish – What's in it for me?
- Skeptical – This won't have any impact on my life.
- Suspicious – Why do they want me to do this?
- Thoughtless – It's not my problem.
- Untrusting – I don't trust the company to keep me safe.

The problem is not knowledge, but attitude. Understanding a person's attitudinal issues and reluctance to actively participate in a security program can open the success rate of these programs and subsequently reduce the risk of human error.

Knowledge

Knowledge Average
67.29% High Risk

The knowledge score for the staff that completed the questionnaire was fair with a score of 67.29% putting SAMPLE COMPANY into the medium risk category with some room for improvement.

This showed a fair level of understanding and acceptance of the basic principles of security.

Our recommendation here is to build specific training materials for specific departments, as well as incorporating a more in-depth reinforcement program and possibly incorporating a team building, collaboration learning exercise like the "Cyber Escape Room". © Layer 8 Security

This can be easily addressed via a comprehensive and regular education campaign encompassing training focused in the specific areas that require attention, workshops showing staff how they can easily be compromised, face to face training, and reinforcement materials such as screen savers, posters, articles, games, and security awareness week annually encompassing onsite activities.

Developing a Strong Security Awareness and Training Program

An effective security awareness and training program begins with establishing clear and enforceable policies. Since policies are essentially the laws of the company and their role is to influence behaviour, they should be:

- Clear, concise, role-based and enforceable;
- Developed at a high level, with input and consensus from senior management; and
- Reflective of business requirements.

Procedures, standards and plans are linked to policies because they describe the steps required to achieve compliance with the policy.

For security concerns such as acceptable use and remote access, companies should have one or two-page policy documents so that they understand how their responsibilities play a vital part in the overall security strategy.

Keep in mind that users tend to pay less attention to issues that don't directly affect them. You should take time to educate users on the negative consequences their poor security practices and behaviours can have on the company and themselves.

Ensure that security awareness and training is completed by all workforce members, including employees and part-time personnel.

Initial and annual awareness training should be mandatory and followed up with ongoing education about new and emerging security issues.

Training programs should focus on issues such as:

- Acceptable use of information assets;
- Password protection;
- How to handle sensitive information in both paper and electronic form;
- Validating requests for information about the company, business partners or other stakeholders;
- Legal and regulatory responsibilities and consequences;
- Safe computing practices;
- How to recognize a threat or security incident; and
- Who to call in the event of a suspected or actual security incident?

Behaviour

Behaviour Average
69.44% Medium to High Risk

The average behaviour profile for the staff at SAMPLE COMPANY that completed the questionnaire is okay with a score of 69.44 % putting SAMPLE COMPANY barely into the medium-risk profile.

Behaviour, as it pertains to Security Behaviour, is a complex matter.

How people react to security threats, how they protect themselves, how they acknowledge the threats and undertake an active role within the community or workplace to protect themselves and the organisation.

What are the contributing factors to behaviour?

Most people seem to believe that behaviour is controlled by raising awareness. Undertaking an awareness program to teach people what to look for and how to address it.

This probably won't change the desired behaviour. It only assists the people who may have forgotten about what to do and reminds them. It doesn't change behaviour for people with attitudinal issues.

Overall, staff at SAMPLE COMPANY showed a reasonable level of behaviour, understanding risk and responding in an appropriate level, yet still rated at a high risk.

Behavioural change needs to be addressed via educational campaigns and further addressing the attitudinal issues.

Behaviour, as it pertains to Security Behaviour, is a complex matter. How people react to security threats, how they protect themselves, how they acknowledge the threats and undertake an active role within the community or workplace to protect themselves and the organisation.

What are the contributing factors to behaviour? Most people seem to believe that behaviour is controlled by raising awareness. Undertaking an awareness program to teach people what to look for and how to address it.

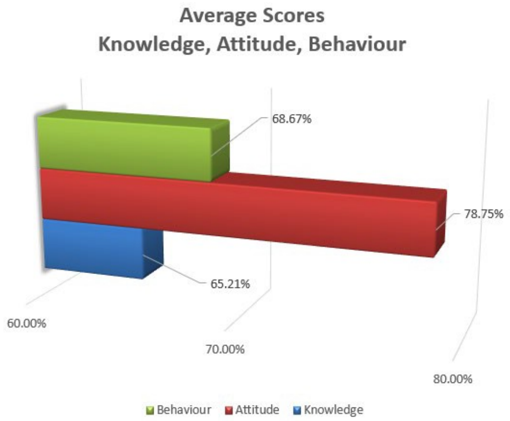
This probably won't change the desired behaviour. It only assists the people who may have forgotten about what to do and reminds them. It doesn't change behaviour for people with attitudinal issues.

Behavioural change comes via knowledge through attitude, impacted by corporate culture to behaviour.

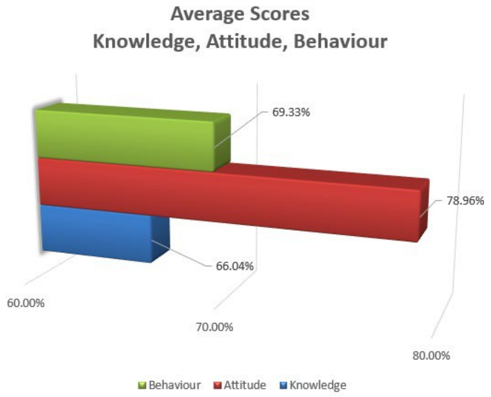
The impact of a change within the culture at SAMPLE COMPANY incorporating behavioural consequences and rewards, policies, and procedures can help to mitigate the staff risk.

Departmental Breakdown

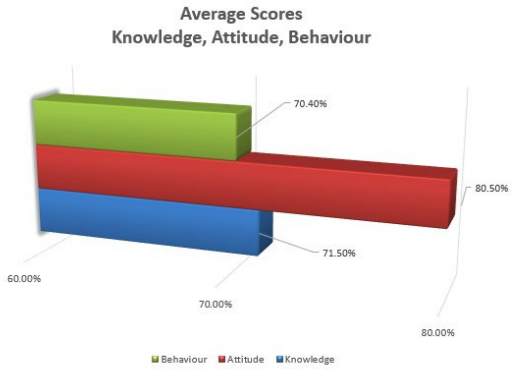
Breaking the results down into the relative departments, we find a consistent theme, that the attitude and culture within SAMPLE COMPANY shows a very high score, the focus going ahead seems to be to increase the level of knowledge within the organisation.



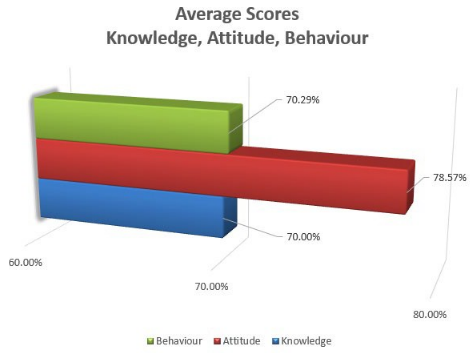
OPERATIONS



CONSULTING

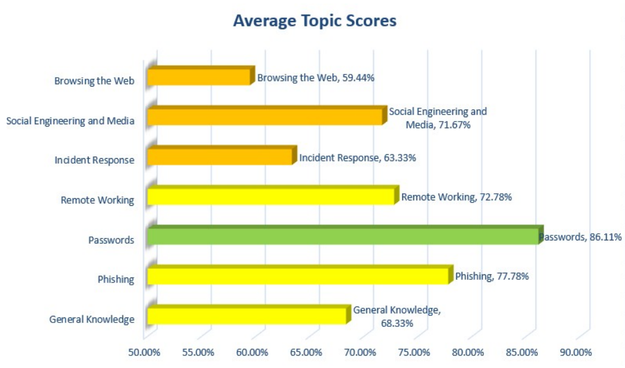


SALES

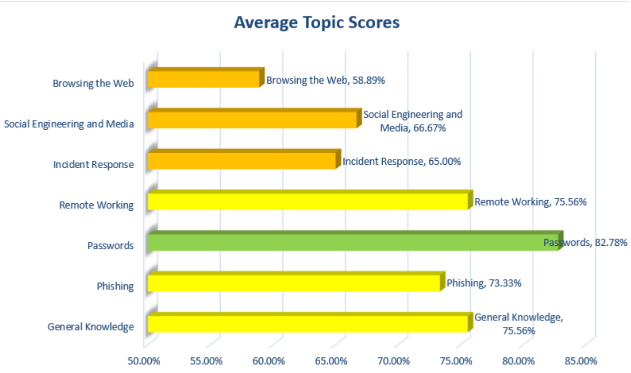


R&D

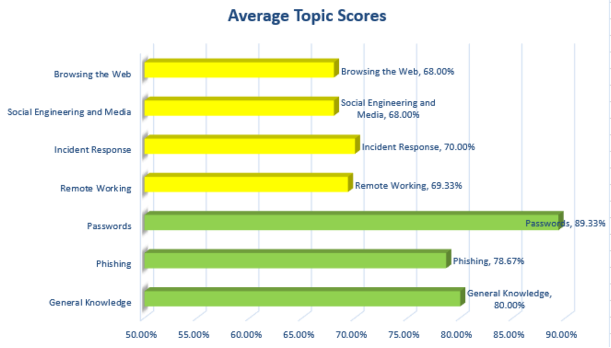
With attention needed on the training side, we see below the departmental breakdown showing the areas of focus needed, Internet Browsing and incident reporting being the topics that require the most attention, but we also noticed that some departments require training in other areas, more specific to them.



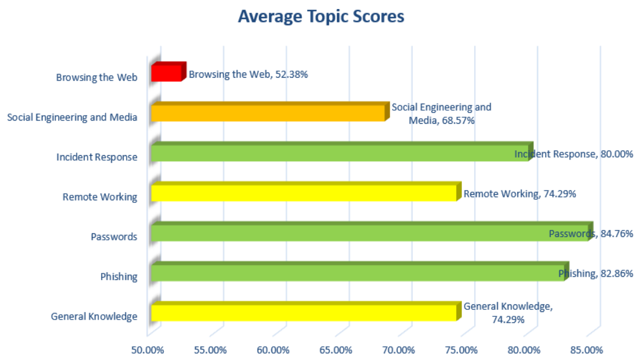
OPERATIONS



CONSULTING



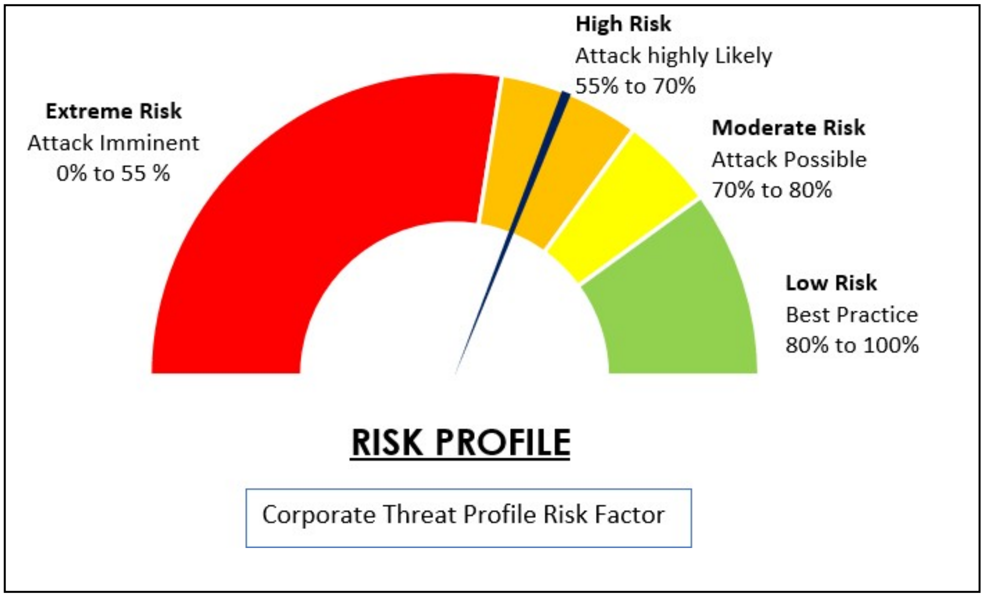
SALES



R&D

Corporate Threat Profile

The corporate threat profile (CTP) is filled out by an executive to identify the corporate perspective of the security. Unlike the B.A.C.K.S score, the Corporate Threat Profile score is quite low, shown as being a High risk.



Further details are provided later in this document, notwithstanding, a score average of 61.47% for the CTP should be addressed in the areas that require attention.

Topics

The topics analysed were typical of the areas that are often encountered as issues within security. This section addresses the combination of the B.A.C.K.S questions as well as the CTP questions.

Percentage
>80% = LOW RISK
70% to 80% = MEDIUM RISK
55% to 70% = HIGH RISK
<55% = EXTREME RISK

As can be seen from the table below, SAMPLE COMPANY have some areas, like confidentiality of data, social engineering and behaviour and culture that could do with some attention.

Further details are provided later in this document.

TOPIC	BACKS	CTP	TOTAL	RISK LEVEL	Industry Average	Notes
General Knowledge	73.52%		**73.52%**	Moderate	69.00%	Above Average
Personnel Security		64.71%	**64.71%**	**High**	60.15%	Above Average
Phishing	77.41%		**77.41%**	Moderate	75.00%	Average
Passwords	85.19%	68.57%	**76.88%**	Moderate	75.00%	Average
Remote Working	73.52%		**73.52%**	Moderate	78.00%	Below Average
Confidentiality of Data		48.57%	**48.57%**	**Extreme**	63.86%	Below Average
Incident Response / DR	68.06%	83.33%	**75.69%**	Moderate	65.33%	Above Average
Social Media, Engineering & Security awareness	68.89%	42.86%	**55.87%**	**High**	63.00%	Below Average
Internet Browsing	59.07%		**59.07%**	**High**	65.00%	Below Average
Behaviour and Culture		54.29%	**54.29%**	**Extreme**	67.71%	Below Average
Compliance and Audit		68.00%	**68.00%**	**High**	70.00%	Average

Recommendations

With relatively good scores received from the staff at SAMPLE COMPANY who completed the BACKS questionnaire, it is recommended that these people be educated around the topics previously mentioned and mentioned on the following page.

Reinforcement of the message is also a good idea, as is the aligns the message of security,

Running a "Security Awareness Week" in SAMPLE TIME FRAME, aligned to reinforce the message as well.

Cyber Escape Room training should be undertaken to not only promote security awareness, but also team building, communication and establishing a higher retention rate.

Other ideas can be discussed in the next planning session as well as the following section on the various topics

Topic

- Personnel Security by corporate
  - Access rights of staff after termination
  - Background checks for staff and contractors
- Phishing – Staff Knowledge enhancement
  - Identifying indicators of Phishing attacks
- Disaster recovery by Corporate
  - Undertaking a tested continuity plan
  - Communication of Incident response to staff
  - Breach notification to the authorities and customers
- Security Awareness by Corporate
  - To be addressed within this engagement with Layer 8 Security
- Internet Browsing by staff
  - Improve knowledge and subsequent bahaviour with appropriate education
- Behaviour and Culture by corporate
  - Address the culture of consequences and rewards as it pertains to security behaviour.

TOPIC	BACKS	CTP	TOTAL	RISK LEVEL	Industry Average	Notes
General Knowledge	73.52%		**73.52%**	Moderate	69.00%	Above Average
Personnel Security		64.71%	**64.71%**	**High**	60.15%	Above Average
Phishing	77.41%		**77.41%**	Moderate	75.00%	Average
Passwords	85.19%	68.57%	**76.88%**	Moderate	75.00%	Average
Remote Working	73.52%		**73.52%**	Moderate	78.00%	Below Average
Confidentiality of Data		48.57%	**48.57%**	**Extreme**	63.86%	Below Average
Incident Response / DR	68.06%	83.33%	**75.69%**	Moderate	65.33%	Above Average
Social Media, Engineering & Security awareness	68.89%	42.86%	**55.87%**	**High**	63.00%	Below Average
Internet Browsing	59.07%		**59.07%**	**High**	65.00%	Below Average
Behaviour and Culture		54.29%	**54.29%**	**Extreme**	67.71%	Below Average
Compliance and Audit		68.00%	**68.00%**	**High**	70.00%	Average

LAYER 8 SECURITY
THE HUMAN FACTOR

Level of Risk	Approval Process
Extreme	**Not tolerated,** no approval to continue work shall be provided. Apply additional risk treatment processes to modify the risk to within acceptable risk criteria levels.
High	**May or May Not be tolerated**. Conduct an appropriate documented risk assessment of the situation Review the risk treatment plan and modify the risk further where possible. Approved by the **Executive Team**
Medium	**Tolerable.** Review current risk treatment plans and modify the risk further where possible. Approved by the relevant **Supervisor and/or Area Manager**
Low	**Acceptable.** Risk acceptable, proceed with work as planned. Approved by the relevant **Supervisor and/or Area Manager**

	IMPACT				
	Negligible	**Minor**	**Moderate**	**Major**	**Severe**
FINANCIAL LOSS OR LOST VALUE GROWTH	Financial loss that can be absorbed within line manager budgets. Small opportunity loss. <$10k	Financial loss that is managed by Executive and can be absorbed within group operating budgets, or loss of minor opportunity. $10k to $100k	Moderate financial loss, or loss of moderate opportunity. $100k to $1m	Major financial loss, or loss of major opportunity. $1m to $10m	Financial loss that would severely burden the Organisation, or loss of very substantial opportunity >$10m
CORE CAPABILITIES (BUSINESS, OPERATIONAL, SUPPORT)	Negligible loss of core capability.	Minor reductions in core capability resulting in a minor performance degradation	Moderate reductions in core capability resulting in failure to achieve some science or operational goals. (eg. inability to meet the conditions of a specific contract, or complete a field trip)	Major loss of core capabilities resulting in failure to achieve important science or operational goals.(eg. 50% loss of operational science capabilities for a limited period)	Severe loss of core capabilities resulting in failure to achieve critical science or operational goals. (eg. severe or total loss of science capabilities)
LEGAL & COMPLIANCE	Negligible legal impact or breach.	Minor technical legal challenge or breach.	Some legal sanctions imposed, minimal fines.	High profile legal challenge, or prosecution with heavy fine.	Potential large-scale class action, or prosecution with significant fine and imprisonment.
SAFETY (STAFF, CONTRACTORS, PUBLIC)	Negligible impact on staff or the public	Injury requiring medical treatment by a qualified first aid person. Exposure of public to a hazard that does not cause injury or affect health.	Injury requiring medical treatment by a physician. Exposure of public to a hazard that could cause minor injuries or minor health effects.	Severe or disabling injury. Exposure of public to a hazard that cause injuries or moderate health effects.	Single fatality, serious non-recoverable injury, occupational illness or permanent major disability (acute or chronic). Expose the public to a severe, long-term health or life-threatening hazard.
ENVIRONMENT	Typically very localised in effect. No visible or quantified impact on flora, fauna, habitat, natural resources and/or ecosystem function.	Limited impacts very localised in effect. Short term (<1 year), impacts to flora, fauna and/or habitat, but no permanent or long term damage to natural resources and/or ecosystem function.	Moderate impacts, less extensive and generally more localised (ie sub-catchment scale) in effect. Short to medium term (1-10 years) impacts to flora, fauna populations, habitat or natural resources and/or ecosystem function.	Significant impacts, may be extensive but not at a landscape/seascape (may be catchment or large part of catchment) scale. Medium term (10-20 years) impacts to flora, fauna populations, habitat or natural resources and/or ecosystem function.	Significant impacts at landscape / seascape (regional or multi-catchment) scale (extensive and widespread) with persistent/long term effects on sensitive environmental features. Significant long term (>20 years) impacts to flora and fauna populations, habitat or natural resources, with permanent or very long term impact on ecosystem function.
REPUTATION & IMAGE	No impact on the Organisation' reputation or image.	Small adverse impact on the Organisation reputation that is contained to small number of stakeholders. Concerns on performance raised by stakeholders.	Adverse short-term impact on the Organisation reputation or image (less than 1 year). Proactive positions taken against the Organisation by an isolated group of stakeholders as a direct result of the risk event. No impact on the Organisation insurance profile. Decrease in stakeholder support.	Adverse medium term impact on the Organisation reputation or image (1 to 10 years). Proactive positions taken against the Organisation by a limited group of stakeholders as a direct result of the risk event. Adverse short-term impact on the Organisation insurance profile. Significant decrease in stakeholder support.	Adverse long-term impact on the Organisation reputation or image (exceeding 10 years). Proactive positions taken against the Organisation by the stakeholders as a direct result of the risk event. Adverse long-term impact on the Organisation insurance profile. Major loss of stakeholder support.
PERSONNEL	Negligible or isolated employee dissatisfaction.	General employee morale and attitude problems. Increase in employee turnover.	Poor reputation as an employer. Widespread employee attitude problems. High employee turnover.	Some senior managers or experienced employees leave. Institute not perceived as an employer of choice.	Large numbers of senior managers or experienced employees leave the Institute.

	Frequency (Continuous Exposure)	**Probability** (Single Activity)	**Historical**		**Negligible**	**Minor**	**Moderate**	**Major**	**Severe**
					2	3	4	5	6
LIKELIHOOD	Very high probability of occurrence, could occur several times during the coming year/project	>1 in 10	Occurs most times this task / activity is undertaken by the Organisation	**Almost Certain**	Medium	Medium	High	Extreme	Extreme **Extreme**
	Likely to occur less often than once per year but more often than once in five years/within the life of a specific project.	1 in 10-100	Occurs frequently when undertaking this task / project / activity by the Organisation	**Likely**	Low	Medium	High	High **HIGH**	Extreme
	Possible, likely to occur less than once in five years but is expected to occur at least once over the expected life of the asset (30 years)	1 in 100-1,000	Has occurred once or twice when undertaking this task / project / activity by the Organisation	**Possible**	Low **LOW**	Low	Medium **MEDIUM**	High	High
	Plausible, unlikely, frequency of failure of less than once in 30 years but more than once in 100 years	1 in 1,000-10,000	Have heard of it occuring, may or may not have occurred at the Organisation	**Unlikely**	Low	Low	Low	Medium	High
	Very low likelihood, but not impossible, frequency is expected to be less than once in 100 years	1 in 10,000-100,000	Not heard of occuring, but theoretically could occur	**Rare**	Low	Low	Low	Medium	Medium