LAYER 8 SECURITY
THE HUMAN FACTOR

Layer 8 Security Baseline Pack

Comprising:

- Spear Phishing,
- B.A.C.K.S staff questionnaire
- Corporate Threat Profile
- Help Desk Historical Analysis
- Compromised Account Analysis
- Physical Security Analysis - where possible
- Baseline Report
- Planning Session

Short Descriptions

Spear Phishing (401 Program)

- A spear phishing campaign to better understand the level of vulnerability staff have with dedicated spear phishing attacks.

B.A.C.K.S – Behaviour, Attitude, Culture and Knowledge for Security

- User based question assessment tool to provide Knowledge level, Attitudinal issues and behavioural issues

Corporate Threat Profile

- Corporate based Risk Assessment Questionnaire to ascertain the corporate perspective towards humans and the possible impact this may have on staff behaviour

Help Desk Historical Analysis

- Human perspective using Help desk ticket analysis:
    - Analyse previous human related incidents of tickets raised
    - Determine breaches encountered
    - Assess remediation time

Physical Security Analysis

- Analysis of the physical security components including attempting tailgating, disposal of documents, secure storage and policies relating to these.

Compromised Account Monitoring Service

- Identify if passwords have been compromised and are currently being sold on the Dark Web as well as identify written down passwords that are stored insecurely

Baseline Report and Planning Session

- Analysis of the results of the Baseline and a planning session for the future.

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

LAYER 8 SECURITY
THE HUMAN FACTOR

Extended Descriptions

401 Spear Phishing Campaign

Layer 8 Security (401 - Authorization required) Simulated Email spear phishing attacks, identify users with regards to their susceptibility to cyber criminal phishing attack methods and the number of people who fall victim to a phishing attack.

These attacks replicate the very same types that cyber attackers are using.

The goal is to measure who falls victim to such attacks as well as who opens the email on different devices to try and achieve a different result.

It is also important to identify the number of people who detect and report an attack of any type.

B.A.C.K.S staff questionnaire

Behaviour, Attitude, Culture and Knowledge for Security Questionnaire. To understand the Behaviour, Attitude and Knowledge of staff within the organisation and how it relates to cybersecurity culture.

This is undertaken via a questionnaire, focusing on knowledge, attitude and behaviour with special focus on specific topics such as phishing, passwords, remote working and many other topics.

The measurement is twofold. It allows us to identify departmental areas of concerns as well as identify the departmental requirements for later education.

Corporate Threat Profile (CTP)

This is a checklist designed to identify and document the existence and status for a recommended basic set of cyber security controls (human, policies, standards, and procedures) for an organisation.

The questions asked here are used to identify any potential issue from a corporate perspective that may have an impact on the staff attitude, behaviour or culture.

The measurement of this questionnaire is to align with the user's responses undertaken within the BACKS questionnaire and to identify any areas / gaps in the policies, controls and standards.

Help Desk Historical Analysis

Identification of issues relating to: Previous 6 months incidents caused by staff, Severity of incidents, Breaches, Remediation times of incidents, Are staff reporting incidents.

Identify areas for improvement that should be addressed through guidance for measuring the performance of an entity in implementing the Cyber security Framework.

These measurements are used to ensure that the amount of reported / suspicious issues increases and subsequently that the amount of breaches decreases.

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

LAYER 8 SECURITY
THE HUMAN FACTOR

Compromised Account Monitoring Service (CAMS)

Security team does an analysis of compromised passwords for specified domain that are available on the dark web as well as a walkthrough of organizational facilities, checking each work environment and looking to ensure that individuals are following organizational policy

This can also include the number of staff locations with passwords or confidential information written on Postit Notes or pieces of paper left on the desk

Physical Security Analysis

This is undertaken onsite to identify vulnerabilities and risks associated with the physical aspects of security, people and policy.

Confidential document management and destruction, workplace / desk security with a walk through - identify security breaches, unattended devices, etc., secure storage of documents and trash and Physical - tail gating, unaccompanied access

Report and Planning Session

Baseline Analysis and Report encompassing collection and combination of results from phishing, SMS, Questionnaire, Knowledge, Culture, Attitude and Behaviour

A report that provides the information as a Gap analysis identifying the areas, issues and people that represent risks to the organisation.

It also provides the ability to efficiently plan the way forward without wasting people's time and money

Baseline Analysis and Report encompassing collection and combination of data from Social Engineering, Physical, Historical, B.A.C.K.S and CTP Questionnaires,

With this, and any other information provided by the customer, we undertake a planning session to address the best way forward to address the security behaviour risks.

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