LAYER 8 SECURITY
THE HUMAN FACTOR

What does Layer 8 Security provide?

Staff Cyber Security Baseline

Know and measure your staff risk. The Baseline© provides you with an understanding your staff security behaviour, what are their strengths and weaknesses pertaining to cyber security awareness.

The output of the Baseline report allows you to target your training to exactly the staff that need it most.

Know where your organisation stand sand how best to progress forward with mitigating the risks posed by the Human Factor, incorporating behaviour, corporate and cultural impact on behaviour, external influence, and the corporate maturity towards the Human Factor.

Analysing staff attitudes, behaviour, knowledge, and the corporate impact to:

- What do your staff really understand about cyber security?
- How do they feel about your policies and the corporate requirements?
- What does their behaviour tell you about how they may respond to a cyber-attack?
- Ensure accurate focused training, and not waste time and resources
- Measure, where are you now and measure the progress of the program
- Show significant "Return on Investment"
- Report and plan your program of work

Cyber Security Maturity Audit

To truly understand your organisational maturity, we have developed the "Human Cyber Security Maturity Audit".

This audit Integrates the "Staff Cyber Security Baseline" with Incident Response handling, Security Culture and Policies, this program allows you to fully understand the Maturity of your organisation pertaining to Human Cyber Security and what is needed to ensure that your human risk program will succeed.

Security Cultural Audit

Security culture refers to the set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security. Getting security culture right will help develop a security conscious workforce and promote the desired security behaviours you want from staff.
Better knowledge of your security culture enables a better chance to address any issues and improve the organisational risk profile.

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

LAYER 8 SECURITY
THE HUMAN FACTOR

Corporate Threat Profile Audit

The impact that the corporation has upon the staff can have a significant impact upon the manner in which they respond to threats. This program is a great way to identify any holes within your security posture as well as any areas that may have adverse impact upon staff.

3rd Party / Vendor Security Audit

3rd Party Vendor assurance is the process of analysing and controlling risks associated with outsourcing to third-party vendors or service providers. We not only undertake a thorough analysis of the technology and processes, but also the human impact of the vendor.

Physical Cyber Security Audit

This audit looks at the physical components of Policy alignment, as well as the impact of incorrect disposal of documents, passwords left in plain view, conversation security, tailgating and other physical security procedures.

Incident Response Audit

Understanding the incident response plan ensures that in the event of a security breach, the right personnel and procedures are in place to effectively deal with a threat. How staff identify and respond to perceived incidents, the analysis and remediation procedure and the possible reporting of a breach, is essential in building a strong plan to incident response.

Compromised Account Audit

The risk associated with compromised credentials lies not only in the threat of easy to obtain, unauthorised entry into organisations from the outside. The risk is magnified because compromised credentials upend many of the traditional risk mitigations organisations typically use and rely upon to bring assurance.

Historical Incident & Response analysis

Understanding how staff have previously behaved when presented with a security incident, allows us to better understand their behavioural and attitudinal characteristics. This in turn becomes a critical component of analysis of their behavioural patterns and likelihood to reoffend.

Social Engineering

Social engineering ranges from Phishing attacks where victims are tricked into providing confidential information or downloading Malware, Vishing attacks where an urgent and official sounding voice mail convinces victims to act quickly or suffer severe consequences, or physical Tailgating attacks that rely on trust to gain physical access to a building.

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

LAYER 8 SECURITY
THE HUMAN FACTOR

Security Awareness Training

Technology alone doesn't provide your organisation with perfect protection from cyber-attacks. Australian built for Australian regulations and requirement, our Security awareness training turns users into cyber heroes and cultivates a security mindset and culture that prioritises the protection of your organisation's data.

Facilitated Learning and Games

Layer 8 security has developed interactive courses and games utilising the services of a facilitator to run scheduled courses with your staff for any learning content.

Security Workshops & Live Hacking Sessions

Layer 8 Security sessions highlight security and how the criminals hack staff. These are interactive sessions to encourage full participation and learning.

Games and Team Building

Team building and games encourage your staff to participate actively in the learning experience and allows them to have an enjoyable experience. Knowledge retention is increased from traditional learning method of 5% to 75% using these tools.

Cyber Security Knowledge Reinforcement material

Reinforcing the messages taught during the education phase increase staff knowledge retention and helps to encourage a culture of security.

Cyber Escape Room

Improve knowledge retention, encourage active participation, build collaboration, and team building, and finally, enhance cyber security knowledge and ultimately, change behaviour. By participating in these games, your staff will not only enhance their knowledge, but they will have fun doing it as well.

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