



# Are your users human firewalls or potential security breaches?

Human Element IT is a specialist provider of unique security solutions.

We believe protecting your valuable assets isn't just an IT Department problem solved with technology.

Unlike other traditional IT providers, we focus on leveraging your existing investment with processes and education of users. Our consulting services will help you identify gaps in your organisation's security posture and make suggestions to resolve those issues – we empower you with best practice tools.

Our bespoke services are designed around:

## Cyber Security Awareness & Culture

Educate your users about the ever changing security landscape and empower them to help mitigate risk. This can be achieved by:

- Assessment of current user awareness
- User Risk Analysis report.
- Education Strategy (includes Presentation and Phishing campaigns)

## Security Consulting

Your current cyber security management products and solutions are only effective if they are configured correctly and reviewed on a regular basis. Human Element IT can help you by providing the following:

- A non-intrusive cyber threat assessment of your network
- Analysis of your current security infrastructure
- Review potential security risks & vulnerabilities
- Review and enhance existing security configurations
- Develop and review policies

## Client Testimonial

The MMA engaged Human Element IT to provide on-site cyber awareness training to our staff members. It was profoundly insightful and staff thoroughly enjoyed the training. It was one of the best decisions to make as it gave staff the tools, knowledge and self-awareness to detect threats and the actions to take in the event of one. It was a great session and got staff talking. We would recommend this training to other organisations.

- IT Systems Manager, Melbourne Market Authority



## Cyber Security Awareness Training

Training can be chosen as a presentation or on-line content. This service is designed to educate your users of the risks caused by malware, phishing and other threats. It is an essential component to any organisations security posture as we know technology can only stop what it has seen before.

## Phishing Education Campaign

This service delivers a baseline understanding of potential phishing campaigns that could target your organisation. These exploits can cause maximum disruption or loss of data. We will help you better evaluate user risk profiles as a once off or ongoing service.

## Policy Review

The purpose of a Policy is to set guidelines and rules for processes. Policies should be reviewed on a regular basis to maintain and enhance the quality of all activities. These days all organisations should have an Acceptable Use policy to ensure all users understand their responsibilities and operate computer systems in an effective, safe, ethical and lawful manner.

## Vulnerability Assessment

A vulnerability assessment is a risk management process used to identify, quantify and prioritise the possible threats in a given system. Leveraging both internal and external scanning and validation to cover all of an environment's devices and endpoints. Our report provides an impact loss rating and the system's vulnerability to that specific threat.

## Penetration Test

A PenTest is an authorized simulated attack to evaluate the security of your infrastructure. Penetration testers can leverage the list of vulnerabilities found during a vulnerability assessment as a starting point to prove internal weakness. Their experience and intuition enables them to look for potential unauthorized access to your Networks (including wireless), Web Applications and your Website.