TRUSTMARQUE
Part of Capita plc

THE HUMAN FACTOR OF CYBER SECURITY

To err is to be human

By focussing on your people, you can improve your organisation's security posture exponentially.

We believe that Cyber Security tends to be focussed on technology and securing the organisation against outside threats. It can often be forgotten that a significant proportion of breaches come from your own internal employees or "malicious insiders".

Cyber criminals actively work to exploit your people rather than your technology - as this is easier. And if your users demonstrate poor cyber security awareness, then it doesn't matter how much you spend on technology, you'll always be at risk.

How you successfully improve the cyber awareness levels of your users, monitor risky and malicious behaviours to prevent any damage, by mistake or otherwise, is critical to a modern security strategy.

Common tactics

Phishing – in the broadest sense, phishing is any attempt to persuade someone to interact with an unsafe email. Phishing emails are used to trick recipients into opening unsafe attachments, clicking unsafe URLs, handing over account credentials or sensitive information, transferring money, and more.

Email Fraud – these attacks can consist of an email, or series of emails, purporting to come from a senior person in your organisation asking the recipient to transfer money or send sensitive information. It does not use malicious attachments or URLs, so it can be hard to detect and stop.

Technology alone isn't enough

Cyber Security solutions in the main look to secure organisations using technology. In addition, those technologies are too often designed to only detect threats which originate from outside the organisation.

We now know that technology alone isn't enough - employee awareness about cyber security and the threats they are susceptible to are critical to successful cyber security. New tools can help you understand which of your users are demonstrating risky behaviours and need help, as well as those looking to deliberately damage your organisation.

Malicious insiders could be an employee or user that has criminal intent to defraud or maliciously damage your organisation. Research by the Ponemon Institute found that 23 percent of incidents involved an insider.

TRUSTMARQUE
Part of Capita plc

Cyber Security's human element

Cyber Security Awareness Training

We can help you develop your security awareness training for your employees. This includes phishing simulations that use real-world tactics to see who's most at risk. It teaches people how to recognise attacks via email, cloud apps, mobile devices, the web and social media.

User Entity and Behavioural Analytics

We will implement and deploy tools that monitor normal behaviour in both your users and machines to create a baseline. This can then be used to track when a user or machine starts to behave maliciously.

Business Email Compromise (BEC) prevention

By deploying email fraud defence tools you can use technologies to stop many attacks that replicate your trusted brand to trick employees, partners, vendors, and customers.

Why Trustmarque?

Trustmarque helps you understand your organisation's true risk and exposure. Our experts will recommend the best solution for your organisation by understanding your unique requirements. We have a fine-tuned portfolio of services and partners that gives you access to the most relevant and advanced solutions. In addition, we have invested highly in staff training and are proud of our expertise as well as our relationships and certifications with the industry's leading vendors. We are uniquely placed to leverage both the strength of our strategic ecosystem partners and Microsoft.

Founded in 2004, acquired by Capita in 2013 and now a part of Trustmarque, our team is a multiple award-winning practise that has been in operation for 17 years. We have over 55 in-house engineers and a customer facing Security Managed Service manned 24x7x365 providing industry leading support coverage for our strategic security vendors.