Why VOSO Lite for training?

90% of security incidents are traced back to human errors.

The human firewall is your first line of defense. Four out of five of the data breaches the ICO investigates are down to human error.

All government and industry standards state that continuous training of employees is the only way to prevent unauthorised disclosure of protected personal information and to avoid to negligently allowing cyber criminals access to corporate systems.

VOSO Lite neutralizes that human risk by:

- Establishing the board director responsible for cyber security. Questions 17, 18, 19 and 67 of the IASME GDPR Governance questionnaire.
- Issuing a Cyber Essentials compliant information risk policy that tells employees their roles and responsibilities in keeping your company safe from a cyberattack and protecting data from unauthorized disclosure. Questions 69, 70, 73, 74, 76 through 90, 120 of the IASME GDPR Governance questionnaire.
- Providing regular reminder training videos that keep employees aware of how they might be tricked into allowing cyber criminals into your organization and what they are required to do to prevent it happening.
- Creates an event schedule that sends out a video at least once a month. VOSO can be configured for more frequent training as per your organizations policy.
- Provides a status dashboard, audit trail and report that contains a time stamp, record and affirmation of all of the videos and security policy, members of the workforce have watched and read.

Within minutes VOSO lite address the biggest risk and major cause of a data breach – human error.

VOSO Lite answers 24 or the 147 policy and process questions of GDPR (16%). It also completes sections 6,8 and 10 of the ICOs guide to cybersecurity for small and medium business therefore helping to mitigate the risk of regulatory action by the ICO.

Questions

We do a phishing exercise and training once a year so why do we need VOSO Lite?

That is good but all standards recommend continuous training to offset social media campaigns. Cyber criminals are inventing new and clever ways to trick members of the workforce into giving them access to systems. Also, we are all human and forget or ignore what we are supposed to be doing.

- If your phone is running out of power do you think twice about plugging it into your workstation to charge?
- If you need to surf the web for some information do you think twice about the sites you are visiting?
- How do you ensure that new employees who join after your training session receive training so you maintain a consistent standard or awareness?

These are some very obvious ways that malware gets into an organization.

We do not have the time for this?

Training all members of the workforce, having an information risk policy and a board member in charge of security are requirements of GDPR. Not doing this is breaking the law but also puts your lively hood and your employees' job at risk. It takes less than five minutes to do this with VOSO because we have done all of the work for you and it is the lowest cost solution in the market today … less than you spend on coffee in a week.

CySure

CySure Limited

2, Printer's Yard, 90A The Broadway,
Wimbledon, London, SW19 1RD

D : +44 (0) 20 8412 1106 | W: www.cysure.net