MOBIUS APPROACH TO SECURITY AWARENESS

Due to ever-increasing information-sharing and heightened awareness of the value and risk associated with information, user awareness has become an essential step in improving information security within organisations. Many organisations are asking themselves the very relevant question of how best to raise awareness relating to information security within their organisation and how to create a culture whereby employees act with security in mind. No organisation is exactly the same as another; therefore differing methods to communicate knowledge and create a security aware culture are appropriate.

Security awareness refers to the sharing of information relating to information security, and the educating and training of users about the risks associated with organisational data – including the confidentiality, integrity, and accessibility thereof. It is generally acknowledged that the weakest (and most difficult to control) link in organisational security is the human factor. This factor can sometimes be overlooked in security programmes, but it forms the base of a successful organisational information security programme. Many organisations have identified this and are moving towards the goal of empowering every employee to contribute towards an effective level of information security.

This increased focus on information security awareness has resulted in the need for a formalised organisational security awareness programme to ensure effective and efficient implementation of such a programme. A security awareness programme focuses on the value an organisation applies to its assets, products, and information and the risk associated with that information. The security awareness programme assists organisations in protecting critical assets from theft and misuse by maintaining the correct level of control over the assets. The information security programme is closely associated with organisational information security policies which detail how assets should be used and protected.

> A recent survey conducted by Mobius Consulting concluded that information security awareness as being one of the top 5 projects for corporate information security officers

By creating awareness regarding security and a security culture within an organisation it is possible to provide employees with the knowledge they need to act in a secure manner, thereby greatly reducing 'people oriented' vulnerabilities, and mitigating risk to the organisation. The Mobius Consulting approach to developing and implementing a security awareness programme provides a practical approach that encompasses an end-to-end lifecycle to ensure that security awareness is effectively embedded into the organisation as part of its culture. Our approach is continuous and flexible and can be applied to any organisation based on their maturity level with regard to managing information risk.

For more information, contact Mobius Consulting on +27 21 20 111 20 or +27 10 590 6111
email info@mobiusconsulting.co.za or visit our website www.mobiusconsulting.co.za

mobius
ACTUALISING CHANGE

PHASE 1. Set Security awareness goals and objectives

- Set security awareness goals that are SMART (Specific, Measurable, Action-orientated, Realistic, Time-delimited) by considering factors such as timelines for completing execution, audience coverage, etc.
- Determine the objectives or drivers for implementing a security awareness programme, e.g. meeting regulatory requirements and becoming compliant
- Define the scope and strategy of security awareness and training

PHASE 2. Design and develop Security awareness Ppogramme

- Obtain buy in and endorsement from executive management
- Identify stakeholders who will be key in making the programme a success and assign roles and responsibilities
- Design a focused programme based on specific risks identified in a risk assessment
- Develop the programme in line with project management disciplines

PHASE 3. Execute Security awareness programme and training

- Execute the programme through:
  - Security awareness which focusses on the end-user and senior executives and;
  - Security training which focusses on IT operational staff responsible for implementing security.
- Use a variety of delivery techniques such as presentations, structured workshops, virtual environments, videos, computer-based training (CBT), e-learning and competitions
- Supply customised security awareness material, such as brochures, newsletters, booklets, posters and intranet-based electronic documents
- Update information security messages regularly using a broad range of communication methods
- Deliver material as part of an on-going information security awareness programme

PHASE 4. Monitor and sustain

- Measure the effectiveness of security awareness activities on a periodic basis
- Identify the overall benefits derived from the security awareness programme
- Obtain feedback from users
- Revise and update the programme in line with organisational needs

For more information, contact Mobius Consulting on +27 21 20 111 20 or +27 10 590 6111
email info@mobiusconsulting.co.za or visit our website www.mobiusconsulting.co.za