secarma®
CYBERSECURITY EXPERTS

SERVICE OVERVIEW

Virtual Information Security Manager

Developing and maintaining a robust cybersecurity posture can be challenging for organisations who either don't have the necessary skills, time internally or the budget to employ a full time, in house Security Manager. Secarma can provide a Virtual Information Security Manager (vISM) who will be embedded within an organisation for a selected period of time to assist in meeting security objectives.

WHO IS IT FOR?

A service of this nature can benefit a range of companies, who are looking for extra support managing and performing security tasks within their organisation.

For example, small companies might simply not have the resources for a full-time security manager but require the capabilities that one brings. Additionally, organisations may want security guidance from an independent source, not tied to their current hierarchy.

HOW CAN WE HELP?

Secarma's vISM Consultancy can offer a solution to these issues, providing bespoke security support to suit a business's requirements.

Our experienced consultant will provide an organisation with an independent view of their security posture, as well as the additional benefit of acquiring a security capability on a consumption-based pricing model.

WHAT WE TEST

Whilst some organisations may require support in all areas, others may have certain aspects of security competently covered, only requiring assistance in specific areas. With this in mind, this service is broken down into 'modules' which can be utilised in any combination – or in their entirety.

- **Risk Management**
  Assisting in compliance work working towards Cyber Essentials, policy review, and building a strong security culture.
- **Security Protection**
  Assisting in the development of implementation plans for vulnerability management, penetration testing, and secure workstation builds.
- **Incident Detection**
  Assisting in the deployment of log management capabilities, as well as developing an in-house monitoring capability or threat-hunting team.
- **Minimizing Impact**
  Developing incident response plans, incident

secarma®
CYBERSECURITY EXPERTS

SERVICE OVERVIEW

Virtual Information Security Manager

The consultancy can be available as security guidance-only or technical hand-on assistance, depending on the organisation's requirements. Whilst we typically embed a dedicated consultant with customers for long term engagements, we can bolster their capability by bringing in additional experienced consultants where required.

The types of activities our vISM can provide are:

INFORMATION SECURITY GUIDANCE

Whilst an organisation may have all the staffing they may require for daily tasks, they could benefit strongly from independent security guidance for board-level meetings, interpretation of security testing reports, appraising an organisations security stance, or simply keeping up to date with new threats and potential remediations.

ORGANISATION SECURITY MATURITY REVIEW

Some organisations desire to improve their overall security but simply don't have enough insight into their current level of security maturity. In order to improve security you have to understand where you are, where you're struggling, and where you would like to be. A maturity review is a solid foundation for developing a security improvement action plan.

VULNERABILITY MANAGEMENT PROGRAM DEVELOPMENT

Vulnerability management is much more than simply running an automated vulnerability scanner. It is critical to ensure that all company assets are discovered, assessed, and issues remediated in a controlled and auditable way.

INCIDENT RESPONSE PLANNING AND PROCEDURES

Whilst many organisations have great knowledge of their internal systems they may not have experience dealing with large scale incidents, such as mass ransomware infections, data breaches, or simply data unavailability due to infrastructure issues.

The dedicated consultant can offer either guidance on writing processes and procedures for an incident, or can develop a contextual incident response plan for your organisation and work to gain board-approval for the developed plan.

INCIDENT RESPONSE TESTING ("WARGAMING")

Wargaming is the process of performing a table-top test of an incident response plan, against a realistic incident scenario. This involves key response staff members sitting down to discuss the steps they would take to deal with an incident, and then guidance being drawn up to improve the efficiency and effectiveness of the in-place plan.

SECURITY AWARENESS TRAINING

Security Awareness Training is designed to highlight key security issues that regular members of staff will face, and ways they can reduce their personal risk.

Risks that should be considered for training are phishing and social engineering, weak and reused passwords, insecure wireless networks, and reporting security incidents. However, training packages can be tailored to organisational requirements.