Security Assessment Review

Introduction

How secure is secure? A silly question but one that is not often asked. One is never totally secure but there must be a point at which the level of security processes, tools and technologies is sufficient to mitigate the main business risks as well as taking into account the ability of the organisation to manage the technologies, maintain process adherence and respond to security incidents. This capability of the organisation to monitor, manage and enhance security methods is a factor based upon many things. This 'maturity' is fundamental to the effectiveness of the organisation's ability to respond and adapt.

Guardian Technologies has identified this need to match the risk mitigation activities with the ability to use layers of technology and process complexity through many client projects. Clients need a straightforward methods to assess the security processes and technology and match them against the maturity of the organisation. There is no point implementing complex technologies if there is insufficient skills to operate and interpret them. For example perhaps a cloud service may be a solution but then these can be expensive, compromise security through the use of third parties and may not provide the protection promised. In addition it may not be clear which technology or service is needed next based upon risk to the organisation.

Guardian Technologies has introduced a Security Maturity Model to help. There are many security maturity models but these either are focussed on one area of security or are so complex to prevent the visualisation of the next steps.

Basic

Advanced

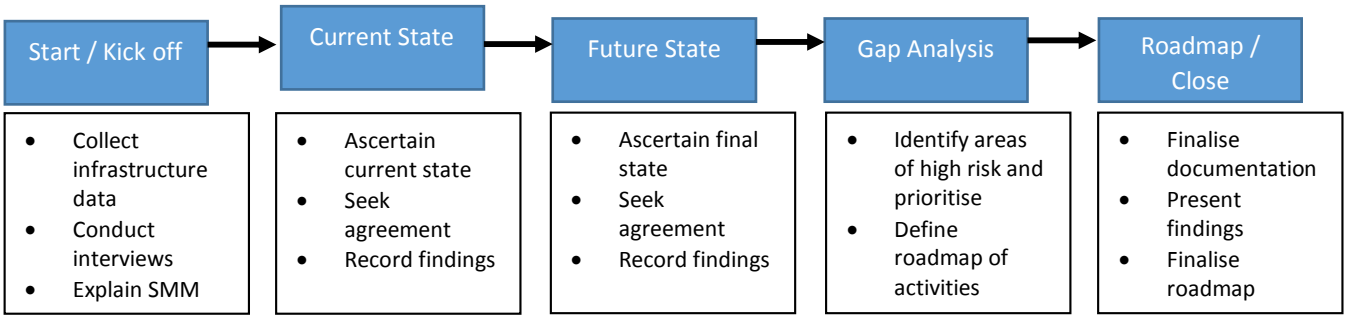
Security Aspect	Initial	Developing	Defined	Managed	Optimised
Patch Management and Anti-Virus	Inconsistent, Automatic updates, No reporting	Some automation & reporting	Documented & consistently applied	Measured and Reported. Enforced by end-point management tools	Continuous improvement and innovation
Firewalls & Network Segmentation	Simple firewall at internet boundary, ad hoc use of desktop firewalls	Dedicated firewall appliance and/or DMZ	Multiple firewalls and network segmentation	Centralised firewall configuration mgmt.	Continuous improvement and innovation
Identity & Access Management	Ad hoc with no process	Domain users & computers, some access restrictions / structure	Documented repeatable change control processes and JML processes	Analysis, visualisation and reporting tools	Continuous improvement and innovation
Asset and Configuration Management	None	Register of assets and deployment documentation	Asset discovery and reporting	Configuration Change Management and License Management tools deployed	Continuous improvement and innovation
Information Classification and Protection	None	Ad hoc file / disk encryption, inconsistent visual labelling	Structured & unstructured data classification, defined meta-data / templates	Discovery, Data Loss Prevention / Rights Mgmt.	Continuous improvement and innovation
Monitor, Alert and Incident Response	None	Some logging, inconsistent monitoring	Basic SIEM deployed Embryonic continuity plans	SIEM tools integrated with most areas. Regular reviews, response and recovery tests	Continuous improvement and innovation
Risk Management and Governance	None	Ad hoc risk assessments, developing security policies	Regular risk assessments and mitigation planning, ad hoc awareness training	Regular policy reviews. Training and compliance tracking	Continuous improvement and innovation

Benefits and Features

Guardian Technologies has developed a security assessment to take clients through the process of understanding what are the key areas of security protection that are required for a structured security stance, where the organisation is actually positioned on the model and where the organisation would like to move to for increased maturity of security capability. So a review of the security systems and processes are taken based upon the maturity model. The model is non-threatening and simple to use. Benefits include:

- Client quickly understands the difference between technology vendors and Guardian security consulting
- Demonstrable process of steps
- Complete security components are covered
- Define a roadmap including next steps and projects

Structured Approach

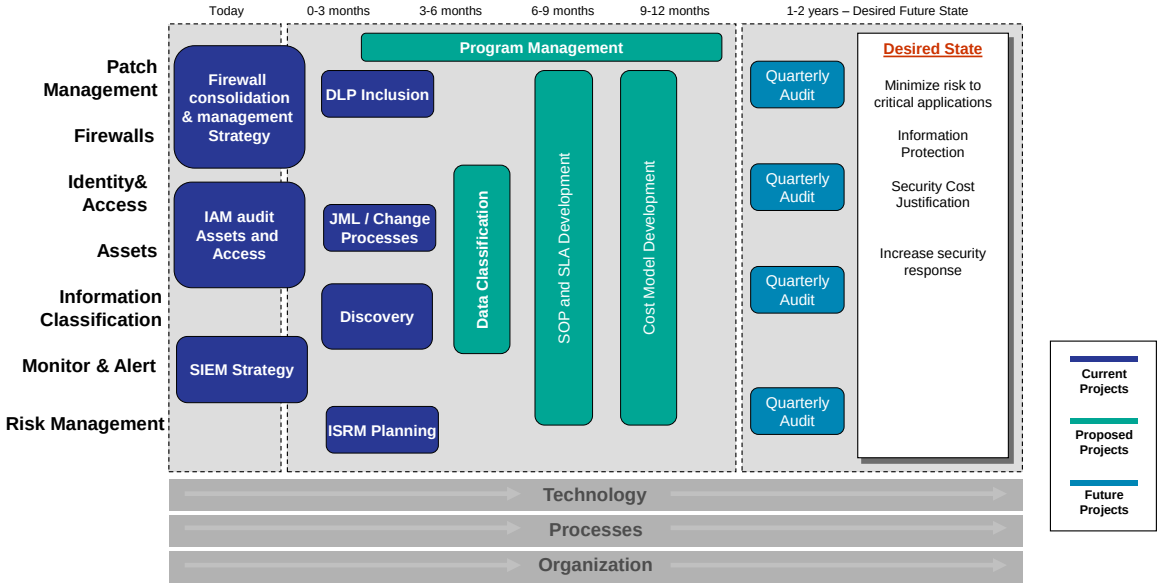


Phases

Guardian consultants will engage with the client personnel in the respective security disciplines to establish the current state of security and where the priorities for the client exist. Following a kick-off workshop to lock down the engagement plan, the roles and individuals required and the scope of the engagement, then a current state, future state and gap analysis will be performed. With agreement from the client for the focus areas and priorities then a roadmap of activities will be provided. It is up to the client to engage with the appropriate parties to execute the roadmap. Guardian has been engaged to oversee the execution of the plan whilst the individual work packages are completed by third parties. Alternatively, Guardian would be delighted to execute the required works.

Workshop Phases	Tasks	Deliverables
Workshop Kick-off	Agenda, Introductions	Roles, Planning, scope, costs
Current State Discovery	Conduct interviews and discussion on each current state situation using SMM framework. Test and verify. Write up data.	Documented minutes. Current state summary
Final State Discovery	Conduct collective discussion on final state aspiration and the benefits of final state using SMM framework. Write up data	Documented minutes. Future state summary
Gap Analysis	Review information and ratify across interviewees. Develop short term and long term recommendations.	Roadmap
Documentation and knowledge transfer	Document and test with client	Final Report Final Presentation Next steps

Example Roadmap



The above roadmap is an example – it can be expanded to more detail for the seven areas of review from the Guardian Security Maturity Model. It is to give a method to communicate the areas required for projects and can be prioritised. Some activities may be combined into a program for firewall and AV as an example. The project impact on technology, processes and people would also be mapped out.

Summary of Assessment

This assessment gives a method to clearly understand the required work areas and why those areas need to be addressed. Breaking down security into the seven focus areas helps to divide up tasks into more manageable parts. Maturity is mapped from left to right to allow technologies to be gradually extended or layered as ability to use those tools is gained. Processes can be modified over time to avoid rapid changes. People or users can be trained or made aware as different areas of security become important.

The assessment should take no more than a week for a small to medium company but this depends on the scope and resource availability. A charge will made for this service.

For more information contact Guardian Technologies (UK) Ltd on +44 (0) 330 223 0261
or visit our website at www.guardiantechnologies.co.uk