Cyber Security Maturity Assessment

Organizations are subject to increasing amount of regulatory, legislative and corporate requirements to demonstrate that they are managing and protecting their information systems and data appropriately.

As a cyber and data security specialist, Techpro Global Group can work with your team to benchmark your security practices, processes and technology, against established industry best practices. We can help assess your security capabilities, identify potential risks and help develop a positive approach to managing cyber risk.

Cyber Security Maturity Assessment

Techpro Global Group's Cyber Security Maturity Assessment (CSMA) provides an in-depth review of an organization's ability to protect its information assets and its ability to respond to cyber threats.

Our assessment looks beyond pure technical competency. It takes a balanced view of how prepared the organization is for cyber threats across people, process and the technologies deployed to counter vulnerabilities. Specifically, The Cyber Security Maturity Assessment service is designed to help you:

- Align cyber security practices to your organizational objectives and policies
- Identify areas for remediation and suggest priorities based on risk and organizational requirements.
- Demonstrate both corporate and operational compliance
- Priorities any existing or future investments according to both risk and security practice 'maturity' aspirations

Our Approach

In developing the assessment Techpro Global Group has combined best practice benchmarks set out in international security standards, the National Cyber Security Centre's (NCSC) 10 Steps to Cyber Security and guidelines from the Centre for the Protection of National Infrastructure (CPNI). These form the framework of the service and are key pillars of the assessment.

The areas covered in the service include:

- Information Risk Management Regime
- Secure Configuration
- Network Security
- Managing User Privileges
- User Education & Awareness
- Incident Management
- Malware Protection
- Monitoring
- Removable Media Controls
- Home & Mobile Working Information Risk Management Regime

Cyber Security Maturity Assessment

Service Methodology

The CSMA service is provided over a fixed number of days. The number of days is determined by organizational complexity and scale. An initial scoping call can estimate this.

The CSMA service follows the following steps:

- Security scoping questionnaire and fact-finding survey
- On-site working session with relevant stakeholders
- Stakeholder and key personnel interviews
- Maturity assessment development
- CSMA findings, maturity score and recommendations report
- Stakeholder de-brief

Maturity Levels

The insight gained from hundreds of separate security customer engagements, and input from our security testing practice, has helped us develop our cyber security maturity assessment that help our customers de-risk and accelerate their cyber security improvement plans.

The maturity level used align with Capability Maturity Model Integration (CMMI) and ITIL.

The 5 Maturity Steps

1. START UP

At this level either nothing exists or is very embryonic in nature. It could also include initial discussions about cyber security development, but no concrete actions have been taken.

2. FORMATIVE

Some features of a cyber security process have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply "new".

3. ESTABLISHED

Key elements of a cyber security plan are in place, and working. There is not, however, a well-thought out consideration of the relative allocation of resources against a strategic cyber security plan for the medium to long term.

4. STRATEGIC

Choices have been made about which parts of the cyber security plan are important, and which are less important for that particular organization. The strategic level reflects the fact that these choices have been made in the context of the organization's objectives, risk profile and compliance obligations.

5. DYNAMIC

At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances: for example, the technology of the threat environment, cyber-attack profiles, a significant change in one area of concern (e.g. Cybercrime or privacy). Dynamic organizations have developed methods for changing strategies in stride, in a “sense-and-respond” way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this level.

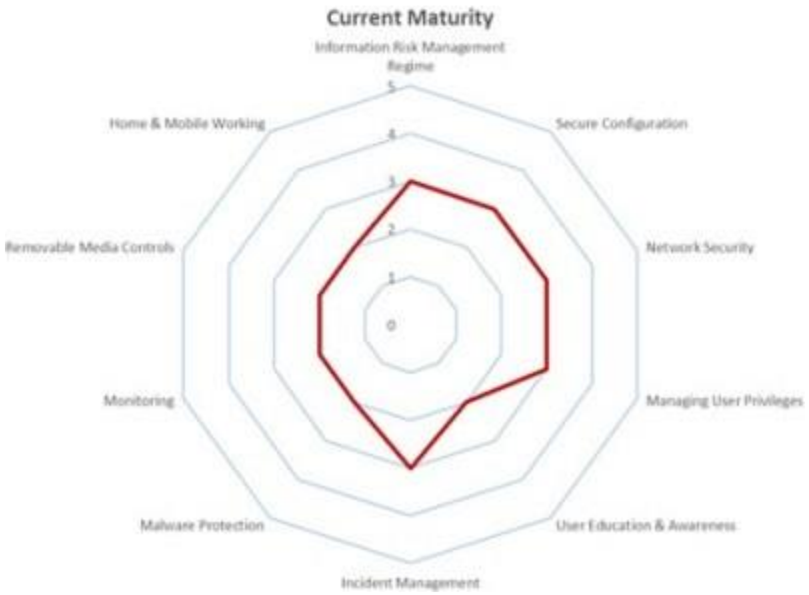
CSMA Report and Recommendations

The purpose of the CSMA is to help customers identify risks, prioritize them and provide advice on appropriate measures and controls in order to better protect the organization and improve our customers overall cyber resilience.

We provide a written report that includes:

- Executive summary
- Key recommendations
- Visual representation of maturity score against the key category
- Detailed assessment of each key metric
- Recommendations for remediation or opportunities for improvements within each category

Example fig for maturity score:



Next Steps

Speak to one of our CSMA experts.

Contact Us