CyberTek™ Security Maturity Model				
Maturity Level	Policies & Procedures	People	Process	Tools/Controls
1: Initial	Informal P&P	Staff with minimal or no formal security training or experience	Basic security processes are performed informally	Minimal to none
2: Managed	Basic, formalized P&P in place	Existing IT staff trained in security	Basic security processes are planned and tracked. May or may not be risk-driven	Basic security related tools & controls are used on an as-needed basis
3: Defined	P&P well-defined and communicated throughout the organization	Experienced Secuity Practitioners at Corporate level	Well-defined and repeatable security engineering process based on a risk-driven methodology. Emphasis on Security Requirements Management and Definition	Security tools/controls are integrated as part of a security framework/architecture
4: Quantitatively Managed	Organization is trained on P&P	Experienced Secuity Practitioners are shared at Corporate and System level	Well-defined metrics exist to measure the effectiveness of the security engineering practices	Security information and event management (SIEM) leveraged for real-time analysis of security alerts generated by network hardware and applications
5: Optimizing	Organization trained on P&P. P&P refined/updated based on organization feedback and security landscape changes	Dedicated & Experienced Secuity Practitioners at Corporate and System level	Integrated Governance in place to ensure that security engineering processes are continuously refined based on metrics to optimize organizational value	Security architecture is refined based on intelligence gained from SIEM to pro-actively deter security threats