APEX Systems
A DIVISION OF ON ASSIGNMENT

Tech Notes

Risk Management for Antiquated Corporate Green IT Practices Impacting HIPAA, HITRUST and NIST

By Erik Lucas, Security and Compliance Consultant

Since its inception, the Green IT movement has lost a good amount of momentum. Consequently, Corporate Green IT processes and polices created several years back, are currently being ignored. The lack of attention to these polices have created compliance vulnerabilities. Proper Risk Management techniques are required to develop a sustainable, pragmatic solution.

The following guidelines highlight the necessary framework required to manage and mitigate the threats from antiquated corporate Green IT practices:

- Risk Management for GreenIT practices from a Business Perspective
  - Ensure qualified personnel are assigned to risk management roles and responsibilities, and unqualified personnel are assigned to risk management functions, leading to the acceptance of inappropriate risk levels and tolerance.
  - Identify new business risks associated with technology and implement them into the risk management framework to ensure that risk events are managed and incorporate into a risk profiling process.
  - Assess the risk posture of a specific entity or item for potential risk impact. Risk: Risk events are not assessed and evaluated leading to a lack of risk mitigation or unacceptable risk acceptance.
  - To ensure that risk events are assessed in compliance with policies, standards, best practices, or other guidelines identified throughout a risk framework.
  - Communicate the organization's risk position to relevant stakeholders.
- Risk Management for GreenIT practices from a Technical Support Perspective
  - Create AES-256 FDE(Full Disk Encryption) Standards, and follow the NIST SP 800-11–Storage Encryption Technology Planning and Implementation guidelines
  - Ensure Disk Drives policies follow the DoD 5220.22-M data sanitization method
  - Establish an inventory tracking system which includes a log to identify where, when, and by whom a drive was formatted

Reference Links:
http://www.hitrustalliance.net/
http://www.hhs.gov/ocr/privacy/index.html
http://www.nist.gov/

About Erik Lucas

Erik Lucas is a Security and Compliance Consultant for a large Non-for-profit healthcare company. He has over 15 years of experience in information technology, with an 8 year emphasis on corporate security compliance working across broad regulatory landscapes, impacting business in the areas of: NIST, HIPAA, HITRUST, COBIT, PCI, and SOX for non-for-profit healthcare organizations, Fortune 50 Corporations and federally funded lending conglomerates. He is the owner and founder of CDM Technology Consulting, a data infrastructure security company.