A.R.T.I.S. Assessments of Risk and Technical Infrastructure Security

Centre TECHNOLOGIES

PREMIER BUSINESS SOLUTIONS

A.R.T.I.S. SECURITY ASSESSMENT

Your comprehensive audit of security and compliance across your entire IT infrastructure.

Security and compliance regulations are continuously in flux based on world events and threat trends. Ensure your organization's technology is in compliance with required regulations and mandates. Centre's Assessment of Risk and Technical Infrastructure Security (A.R.T.I.S.) is available as a recurring service that provides you a detailed view of the security posture of your organization.

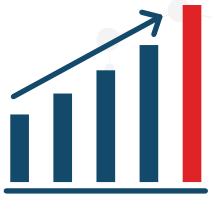
- In-depth view of current vulnerabilities across your environment
- Access to seasoned IT security experts knowledgeable of current and potential threats, providing advisory-level consultation

Bring your security roadmap and compliance plan to life utilizing a Virtual CIO.

ASK US ABOUT vCIO IT RESOURCING

U.S. COMPANIES
will experience a breach

NEARLY $8M
AVERAGE COST OF BREACH
in U.S. following security incidents*



GLOBAL RANSOMWARE
increase of 176% over 5 years

BUSINESS IMPACT ANALYSIS (BIA)**

- Creates detailed inventory of all assets in your current environments
- Defines how critical assets (people, processes and technology) are to your organization based on individual impact scores
- Gathers data to perform full risk assessment and develop IRP/DRP/BCP

RISK ASSESSMENT (RA)

- Conducts security audit and reviews current processes and procedures
- Provides ranking of risks based on potential impact and likelihood
- Recommends response plan to reduce potential threats and mitigate risk, taking into account the BIA

INCIDENT RESPONSE PLAN (IRP)

- Develops and delivers supporting documentation on chain of command for dealing with security incidents
- Provides script for initial response to major incidents most likely to happen

DISASTER RECOVERY PLAN (DRP)

- Outlines plan for short-term recovery of critical information systems immediately following a security incident or natural disaster
- Provides script for specific major events, such as fires, floods or other critical asset downtime incidents

BUSINESS CONTINUITY PLAN (BCP)

- Outlines plan for conducting business in the long term if disaster recovery windows are unable to be met
- Provides scenarios for most critical processes and assets, based on the impact scores from BIA
- Documents tasks that must be completed after an incident in order to return to normal business operations

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) POLICY

- Creates foundation for information security and aligns workflows
- Ensures compliance with external requirements
- Provides guidance for protection, detection, response and recovery controls

RECURRING IT + SECURITY SERVICES

- Develops IT policies
- Reviews current IT policies
- Executes regular vulnerability scans
- Conducts annual A.R.T.I.S. assessment

ADDITIONAL AVAILABLE SERVICES***

- Cybersecurity Operations Center (CSOC) for threat detection and response with 24/7/365 active monitoring and threat intelligence
- Security training targeting areas of weakness, including email phishing and real world scenarios

Penetration testing is not included in A.R.T.I.S. and available at additional cost.

* *The Average Cost of A Data Breach is Highest in U.S.*, Forbes, 2018

** Includes (1) Confidentiality, Integrity and Availability (CIA) of each process or asset; (2) Recovery Point Objectives (RPO) frequency of backups; (3) Recovery Time Objectives (RTO) desired uptime after an event.

***Optional services not included in A.R.T.I.S. and available at additional cost.

centretechnologies.com

v01212019-0241PM