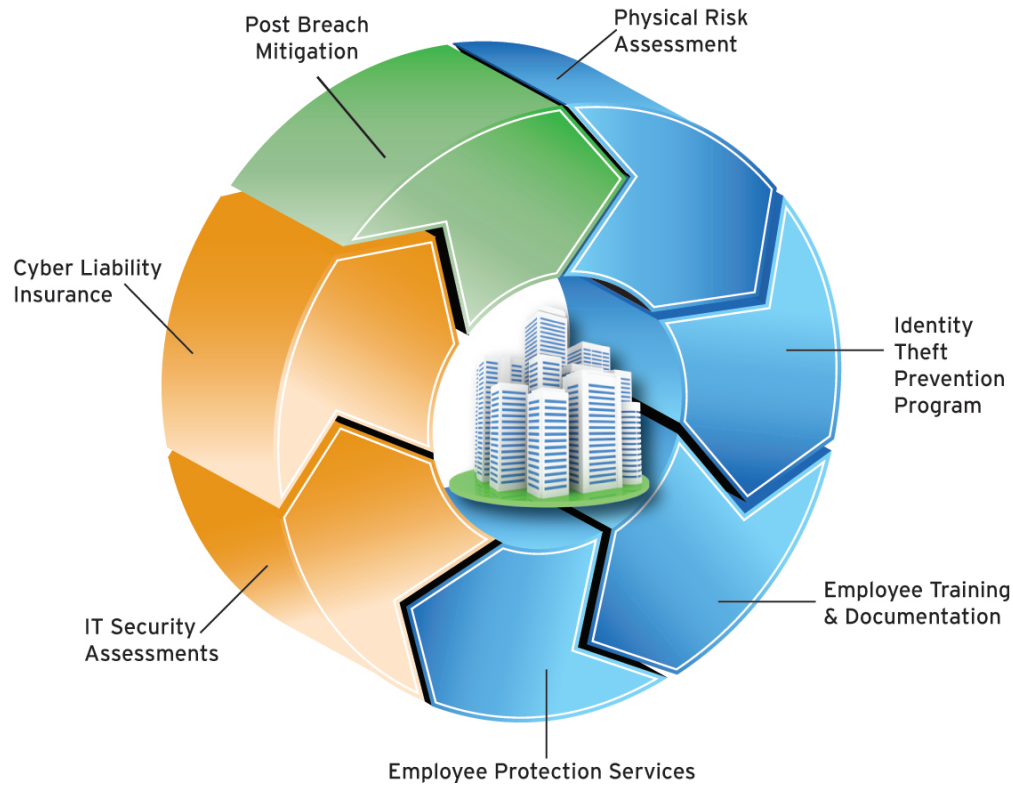




Data Breach Prevention Program



Creating a Culture of Security to
Defend, Protect and Restore your information

Proactive is less expensive than reactive! In 2011*:

- 545,000,000 is the number of lost or stolen records since 2005
- \$56.6 Billion annually is the cost to business from data breaches
- 96% of data breaches are avoidable through simple and immediate controls
- 89% of victims have not achieved compliance
- 68% of breaches occurred within companies under 1,000 employees
- 78% of breach cases last year involved in-person contact
- \$200 is the average cost of a lost record

* Verizon Data Breach Report, 2011

The message for corporate America on privacy and security is simple: "You only need to worry about privacy, security laws and rules if you have customers or employees."

-Kirk J. Naha is a partner with Wiley Rein LLP

Services Overview

DATA BREACH PREVENTION PROGRAM (DBPP) – (Available at NO COST)

- Onsite physical risk assessment
- Documented appointing of an I.R.O. (Incident Response Officer)
- Design and delivery of a Data Breach Prevention Policy Bank:
 - HIPAA Privacy and Security
 - HIPAA Breach Notification
 - IT Security
 - Document Destruction and Retention
 - Non Public Information (NPI)
 - Red Flags amendment
 - Social Media
 - Portable Electronic Device
 - Patient Privacy Notice
 - Business Associate Agreement and addendum
- Employee training and documentation
- Employee ID theft / legal protection program
- Notification to all B.A. and vendor agreements
- Creation of a Breach Response Task Force

POST BREACH RESPONSE PROGRAM

- Forensics – Identifying the type of data lost (IT Analysis)
- Documentation and audit trail preparation
- Notification to affected individuals – Custom mail, email, website
- Annual credit monitoring for victims
- Corrective measures program – Updating policies, employee training, risk assessments

ELECTRONIC RISK ASSESSMENT – (HITECH / Meaningful Use)

- IT Infrastructure – servers and operating systems
- Network Infrastructure – routers, firewalls, workstations, and e-mail
- Internal & external vulnerability testing –network and systems
- User access – online applications or PII / PHI in records
- Compliance status related to the “minimum necessary” required standards

CYBER LIABILITY INSURANCE

- Breach notice costs
- Damages and defense costs
- Service provider breach
- Business interruption and data restoration
- Denial-of-service attack
- Cyber extortion

Our program is customizable to meet your industry-specific needs. Whether you are looking for a complete program or adding an additional layer of protection, we can help. Fee-based solutions provided at a reduced rate when combined with DBPP.