propel
INSURANCE®

DATA SECURITY SELF-ASSESSMENT

For Corporate Executives

INTRODUCTION

It should come as no surprise that companies of all sizes are taking data security more and more seriously. Similarly, in recent years, Cyber Liability Insurance has become more commonplace which has allowed the insurance industry to gain important experience with regard to how various companies organize and prepare themselves for the inevitable data breach.

The following self-assessment is designed for corporate executives, not Information Technology staff. It highlights areas upon which senior executives should focus in order to minimize the impact of a breach, strengthen their company's response, and avoid costly claims.

The self-assessment is divided into four categories:

1. Data Practices Overview
2. Policies and Procedures
3. Controls and Safeguards
4. Ongoing Measures

1. DATA PRACTICES OVERVIEW

□ Does your company own, license, store, or maintain

- ○ Personally Identifiable Information (“PII”)
- ○ Protected Health Information (“PHI”), or
- ○ Payment Card Industry (“PCI”) information?
- ○ Other records that may or may not contain some of the above?

□ Where is the PII, PHI or PCI information stored?

- ○ Paper records?
- ○ Computer systems?
- ○ Portable devices?
- ○ Vendors / service providers (cloud)?

□ What are the threats to data security?

- ○ Computer hackers
- ○ Burglars and thieves (physical break-in)
- ○ Employee errors
  - □ Lost laptop or cell phone
  - □ Fraudulent e-mail / malware
- ○ Rogue employees – intentional theft

□ Is the amount of data and length of time data is stored limited to what is reasonably necessary or required by law?

□ Is the effectiveness of current data protection measures and data storage practices regularly reviewed?

□ Do you have Cyber Liability Insurance?

- ○ Data breach response costs (first party)
- ○ Liability for coverage of claims (third party)

2. POLICIES AND PROCEDURES

□ Written Information Security Program (WISP)

  - ○ All employees sign confidentiality agreements
  - ○ Device usage policy – cell phones and laptops
  - ○ Social media policy
  - ○ Procedure to report data breaches to management
  - ○ Meets state regulations

□ Data and document destruction policy

□ Agreements with business partners to maintain data security

□ Procedure to provide access to individuals who request personal data (Subject Access Requests)

□ New business projects include provisions for data security at planning stage

□ Disaster response and business continuity plans include secure data transfer provisions

□ Specific responsibilities are assigned to staff members:

  - ○ Information systems design and implementation (IT)
  - ○ Designated Privacy Officer
  - ○ Manager of records
  - ○ Risk manager – regular review of data security risk
  - ○ Trainer of employees regarding security systems and protocols
  - ○ Data breach response team
    - □ Team leader
    - □ Leaders within specific business units
    - □ Legal compliance (often external cyber counsel)
    - □ Public relations or crisis management firm
    - □ Forensic computer analysis
    - □ Notification to victims
    - □ Credit monitoring

3. CONTROLS AND SAFEGUARDS

- □ Is access to records limited to employees with legitimate business purposes?
- □ Is data stored in a physically secure location with controlled access?
- □ Is electronic communication of sensitive data encrypted?
- □ Does the computer network have appropriate firewalls?
- □ Do all computers have virus protection and regular virus scans?
- □ Are staff prevented from storing data on portable devices (e.g. USB drives)?
- □ Are data backup systems secure (encrypted)?
- □ Does you require multi-factor authentication for customer/vendor access?

4. ONGOING MEASURES

- □ Is the effectiveness of current data protection measures and data storage practices regularly reviewed?
- □ Are all employees trained as to security procedures?
- □ Are training materials regularly updated?
- □ Is employee access to records terminated when no longer necessary?
    - ○ Are terminated employees denied access immediately after termination?
- □ Are employees who violate security procedures disciplined?
- □ Are policy and procedure changes effectively communicated to employees?
- □ Must passwords be changed regularly (at least every 90 days)?
- □ Do you regularly test or audit for compliance with security procedures?
- □ Do you regularly perform simulations of data breach events?
    - ○ Technical simulations to recognize and flag data breaches
    - ○ Table-top exercises with data breach response team
- □ Do you regularly purge or dispose of data no longer needed?
- □ Is system vulnerability testing done regularly?
- □ Is the movement of records from location to location tracked and recorded?
- □ Is data routinely backed up (securely)?
- □ Are decisions related to data sharing recorded and maintained in logs?