

## TECHNOLOGY COMPANIES



### PROFILE OF CLIMATE

Over the past 5 years, numerous legislation has affected how companies use and protect proprietary information. Data storage and transportation security concerns have changed the climate and exposure in the technology industry. Errors and omissions can no longer simply be corrected by technology companies.

Legislative mandated breach reporting and compliance is now an extremely costly business expense - A security breach costs an average of \$202 per record with an average claim of \$6.6 million (*Ponemon Institute Study*). Legislative mandated costs for both the technology firms and companies contracting with them can virtually put a firm out of business.

Breaches can be a result of insufficient employee background checks, lack of standards of care, non conformity in software updates, lack of encryption processes and wireless networks, to name a few. No matter what the reason, all can lead to enormous exposures for your technology firm.

### COVERAGE OVERVIEW

Claims made policies with Premiums ranging from \$1k to over \$100k for more complex coverage typically requiring world-wide coverage. Limits range from \$250k to \$25million and deductibles from \$1k upward to \$100k.

### COVERAGE AVAILABLE

*Note that many ISO exclusions exist for electronic information including explicit exclusions on almost all CGL and GL coverage forms.*

**Cyber coverage** for 1st and 3rd party malicious code

**Secure Data** coverage for breaches of GLB 401c, HIPAA, and states secure data laws

**Business Interruption** for loss of revenue during security breach crisis

**Crisis Management** reimbursement to remediate and control the incident including PR spin and media costs

**Intellectual Property** for perils like trademark, copy write and patent infringement

**Errors and Omissions** for malfeasance of the technology implementation team and their subcontractors associated with any professional technology service for a fee

**Personal Injury** to cover defamation, invasion of privacy or related perils

**Call Center Support** for costs associated with Q&A load from breached clients

**Legislative Compliancy** for certain fines and costs associated with investigations and penalties associated with HIPAA, GLB etc

**Cyber Extortion** perils associated with malicious demands for pay off or threats in exchange for not releasing propriety or sensitive data.

## CLASSES OF TECHNOLOGY COMPANIES

Software developers, ASP, ISP, Package Software firms, consulting firms, network support and implementation, Software Security firms, programmers, hardware support and repair,

## QUESTIONS ABOUT YOUR INSURED'S

- Any secure data breaches or incidents in last 5 years?
- Do they use release control software such as "source safe" etc?
- Do they have a well defined implementation and development methodology such as Rational Rose etc?
- Do they use independent contractors or subcontractors?
- Do they require E&O coverage for subs and independent contractors?
- Do their contracts have hold harmless or limits of liability in them?
- Do they have any compliance certificates (PCI, HIPAA, etc)?
- Do they work with companies that collect and keep any proprietary info such as (SS#, Credit card info, Financial info, account numbers, maiden names, pets names etc)?
- Do they encrypt data on laptops, back ups, emails etc.?
- Do they use and or implement any wireless networks?
- Do they have any policy or procedures for identity theft or secure data breaches?
- Do they have any patents, copy writer, trademarks or intellectual property?
- Do they have a transactional website in any way?
- How often do they change passwords for their systems and do they contain a combination of letters and numbers?
- Do they do business in multiple states and or worldwide?
- Do they have a minimum of 2 locked doors with FOB or pass card protection at minimum and explain more complex security measures?

## CLAIMS EXAMPLES

### **Claim #1 - Technology Consultant**

Programmer was an Independent contractor born in India and employed by a technology company building a CRM system for a bank. Contract called for the bank to not provide any proprietary information to programmers in populating the data base. The programmer in lieu of the contract was given private information. After completing the project the programmer wanted to show his mother back in India what he had built. He posted on his personal website a link to the software he built so his mother could see. An executive from the bank saw the link and followed to their bank website where the contents showed social security numbers of bank personnel, account #'s and other specific secure data, protected by law.

Bank sued the technology company for assorted breach of contract and secure data law malfeasance. The technology company had only GL, no E&O nor secure data, privacy law coverage.

Costs ran in the multi million dollar range for notification and compliance of states secure data laws.

### **Claim #2 - Cyber Claim and Secure data**

A woman purchased a used computer from a pharmacy. The computer still contained the prescription records, including names, addresses, social security numbers and medication lists of pharmacy customers.

### **Consequence:**

The cost of notifying affected parties per state law totaled nearly \$110,000. Two lawsuits have been filed: one alleges damages in excess of \$200,000 from a party who claims she lost her job as a result of the disclosure; the second alleges that the plaintiff's identity was stolen, and that costs of correction and emotional distress will exceed \$100,000. A HIPAA investigation is also underway.