Contact Information

Ralph Vanner , Jr.
CEO & Director of Development
Vanner Insurance Agency
11 Pinchot Court, Suite 100
Amherst, NY 14228
rvanner@vannerinsurance.com

Privacy/Security Liability

The question is no longer will a company have a security breach but rather when!! There are first party costs as well as legal liabilities in the event your client's information is compromised because of their security failures.

In addition to the costs below insured's are at even greater risk for the cost associated with lost business from a breach or "churn" of existing or future customers resulting from the publicity.

Statistics:

- In 2011 there were 31,016,310 breaches recorded (2010 there were over 12,000,000!)
- Average notification costs $204 – per record
- 40% of data breaches are from negligence – human error
- 24% are from a malicious attack
- 36% are from a system glitch – human error

Triggers of a Breach that Create Exposures:

- Lost/stolen portable computers or media device
- Lost/stolen backup tapes/devices
- Improper disposal of paper records and computer equipment
- Computer hacking
- Employee misuse
- Vendor negligence

Cost to Handle Privacy / Security Breach

Consider this – if a breach occurred that affected 1,000 records the anticipated reasonable costs would be

Internal Investigation
- Cyber Crime Consulting: $ 6,900
- Attorney Fees: $ 6,996

Regulatory / Compliance
- Credit monitoring for affected customers: $ 57,840
- Regulatory investigation defense: $ 21,396
- State/Federal Fines/Fees: $ 45,384

Notification/Crisis Management
- Customer Notification: $ 12,720
- Call Center Support: $ 9,000
- Crisis Management Consulting: $5,040
- Media Management: $ 996

Area's the policy can respond:

- Expenses associated with an incident such as:

Privacy:

- Unauthorized acquisition, identity theft, mysterious disappearance, release, distribution or disclosures of personal and corporate information
- Breaches by third parties as well as **rogue employees**
- Civil fines and penalties and consumer redress
- Violation of federal, state or local privacy laws

Privacy Breach Containment:

- Costs of notification – may be a $ amount or number of individuals affected
- Crisis management expenses
- Credit monitoring costs
- Costs of breach investigations

Technology Security:

- Failure to prevent a party from unauthorized access including denial of service attacks
- Malicious code coverage
- Inability of a third party to gain access

Web-Media Services:

- Personal injury coverage for the insured's website
- Intellectual property coverage for website the insured maintains

Technology Extortion:

- Extortion payments to a third party related to a technology threat
- Expenses to investigate the cause of the extortion
- Expenses the insured incurs to pay the extortion, including travel expenses and the cost of a third party to make a payment

Restoration Loss:

- Costs to restore, recover or replicate data that is damaged
- Costs to recollect unrecoverable data
- Cost to determine the ability to recollect data

2012 Privacy "Real Life" Breaches

May 30, 2012 American Advertising Federation (AAF)

A **hacker** or hackers posted member names, email addresses, and contact information online.

May 29, 2012 Investacorp, Inc.

A vendor of the broker-dealer, National Financial Services (NFS), used by Investacorp was involved in a data security breach. On or around March 12, 2012, Investacorp learned that an NFS vendor had **accidently** shared electronic files with another federally regulated broker-dealer that also uses NFS's services. The incident occurred on November 29, 2011 and was first noticed on February 13, 2012. The information included client names, Social Security numbers, and certain types of account data. Five Investacorp clients from California may have been affected, but the total number of affected individuals nationwide was not reported. The vendor responsible for the mistake worked with the other broker-dealer to delete the client files from their system. Investacorp then received an executed affidavit from the broker-dealer certifying the destruction of the electronic files.

May 25, 2012 Phoebe Putney Memorial Hospital

On April 9, 2012, Phoebe Putney Home Health Care (PPMH) learned from law enforcement officials that a **former employee had improperly accessed** patient information with the intent to file fraudulent tax returns. The dishonest employee may have accessed the names, Social Security numbers, and dates of birth of patients some time between June 2010 and April 2012. Patients who were treated through PPMH between July 2005 and April 2012 may have been affected.

May 25, 2012 Duane Reade

Employees at two Duane Reade stores were caught participating in a credit card fraud ring. One employee at each store was found to have used an unauthorized device to scan customer credit cards prior to processing them through the store's system. People who made purchases at the stores between October 1, 2011 and February 16, 2012 may have been affected.

May 24, 2012 Physicians Automated Laboratory

An office **burglary** on or around March 26 resulted in the exposure of patient information. Patient files containing names, phone numbers, dates of birth, addresses, and lab work were stolen from a laboratory. It is unclear why affected patients were not notified until two months after the incident.

May 23, 2012 Boston Children's Hospital

Buenos Aires, MED PORT 2,159 (No SSNs or financial information reported) A Boston Children's Hospital employee **misplaced** an unencrypted laptop during a conference in Buenos Aires. It contained the names, dates of birth, diagnoses, and treatment information of patients were exposed.

VANNER
INSURANCE AGENCY
Managing Risk. Maximizing Results.

Privacy Ballpark Application

Notice: This indication sheet is for a **non-binding indication** for privacy insurance only. A contract of insurance cannot be confirmed with this alone.

Please include subsidiary companies (companies in which you directly or indirectly own more than 50% of the assets or outstanding voting shares or interests).

1. Applicant details

Name:

Address:

Website:

2. Cover required

Please indicate cover required:

US $1,000,000 ☐ US $2,000,000 ☐ US $3,000,000 ☐ US $5,000,000 ☐

3. Business Activities

Please describe business activities of your company and include the revenue from any subsidiaries that you want covered:

4. Types of personally identifiable information (PII) held

Social security numbers ☐ credit card numbers ☐ personal health information ☐

bank account details ☐ Driving licenses ☐ Other. Please specify _____

5. Amount of personally identifiable information held

Number of Social Security numbers, credit cards numbers, drivers license numbers, etc.

_____

5. Gross revenue

Past year ending / /	Current year	Estimated for coming year
$	$	$

		Yes	No
6. Written policies	Do you have a written privacy policy?	☐	☐
7. Privacy audit	Has a third party audited your privacy and IT Security practices in the last 2 years?	☐	☐
8. Encryption	Do you encrypt PII at rest (on a database or laptop) and in transit (email or file transfer)? If no, please describe any compensating controls: _____	☐	☐
9. Network Security and Monitoring	Have you installed and do you maintain a firewall configuration to protect data?	☐	☐
10. Access Control	Do you restrict access to data by business need-to-know?	☐	☐
11. Regulatory issues	Have you ever been investigated in respect of the safeguards for personally identifiable information, including but not limited to credit card information, or your privacy practices?	☐	☐