How to Protect Your Firm Against Cyber Liability

Most businesses collect or hold **personally identifying information (PII)** about customers, employees, or business partners. If this PII is lost or stolen, this places not just these persons at risk of identity theft but the PII custodian and controller at risk of civil liability and criminal sanctions, too.

Various States have enacted laws:

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Identifying & Addressing your Exposure

What confidential information does your business handle?

It is critical for you to understand your exposure and take specific steps to reduce risk. Your first action should be to establish a policy that addresses information security and cyber liability within your firm. Determine what confidential information your company handles, stores sells and/or shares (considering the legal implications of doing this) and for how long it is needed. Reducing what you retain reduces your exposure.

Establish a record retention policy and stick to it. This should include data that can be destroyed or redacted and password protected. For instance, when checks are received, your accounting department should record receipt and never store a copy of the check in the client file or other location

Where do you store confidential information?

- Do you store information off site?
- Do company laptops contain confidential information?
- Are your server backups housed away from the office?
- How do you treat paper files that may contain sensitive information?

Keep a record of any place, equipment or other media devices that may have confidential information. Limit access on an as needed basis and minimize the amount of offsite data storage.

Set up and maintain a policy, subject where possible to audit, of password protecting, information culling and restricting laptop stored information.

Where third parties, such as contractors, are employed to look after hard and soft copies of PII clarify your contractual arrangements with them and more specifically look at your respective contractual liabilities and indemnities.

What security steps have you taken to safeguard release of this data?

What internal controls do you employs:

- Are passwords regularly changed?
- Are server rooms locked?
- Are all firewalls updated regularly?
- Do you have the ability to track who has data access remotely?
- Are paper files that contain sensitive information kept locked after hours?
- Is the office manager's room locked?
- Does the firm have procedures for dealing with incoming and outgoing mail to prevent security leaks?
- Are detailed personnel checks undertaken of involved staff prior to their employment.

What additional steps can I take to improve data protection?

A review of the response to the foregoing questions will provide a guideline. Survey all employees and departments to request suggestions. Create an internal team of senior staff to develop a Cyber liability policy; train and educate staff about the impact of a data breach; implement your policy; and meet regularly to update, review and implement planned risk management ideas; to implement a series of annual or more frequent internal seminars highlighting cyber security and its developments as they impact upon your own business.

Does your firm have the external resources to protect itself from Cyber liability?

Most small companies do not have the internal resources to manage and maintain relevant cyber exposures. The Cyber team should consider external IT help to provide key components of their cyber liability strategies. The outside IT consultant should initially provide an assessment of your company's existing cyber protection. In addition, it is beneficial to inquire about "best practices" of other similar businesses as yours. The IT consultant should be responsible for ensuring that all areas of protection are regularly updated including:

- Firewalls

- Anti-virus software
- Regular security patches
- Software updates

Do you have written guidelines and procedures for lost files, media storage devices and other electronic equipment?

Don’t keep confidential information on a laptop or other portable media, including portable memory discs, vulnerable to loss or theft. Use laptops to review information only on a protected server. Use USB, or similar storage devices to store data and kept them separate from the laptop. Every portable device should be protected with both password and hard drives encryption. Backup data backups via the web and back-up files stored remotely. Taking storage tapes home is antiquated and creates exposure, and should be avoided.

How long could your company stay in business without website, email or server access?

Depending upon your business disruption of web access can be a minor annoyance or significant loss of income. Regardless of this, you should have a system to regularly back-up a copy of your websites and consider a ghost site. Consult with your web hosting company about techniques to deal with a denial of service attack.

Electronic-mail is integral to the efficient running of your business. When it goes down, business grinds to a stop. A good solution is to set up a remote back-up for email, which allows for continued access if your server is down. Your email server should be back-up to this site regularly. Establish a formal email usage policy for all staff to minimize your exposure to spam and computer viruses.

Do your employees have remote access to your servers?

Employees’ remote access to your servers exposes your business to a security breach. Make sure you control the access. Vigorous password security is essential coupled with automatic password expiry. You should use complex passwords with 8 or 10 characters with alpha numeric sequencing. Maintain an access log permits to screen usage and identify hackers and non employees who may attempt access.

Does your firm have disaster recovery plan in place? Have they been tested?

Prepare a disaster recovery program. If your office space is closed down what steps are in place to keep the business open? Test your backups

systems thoroughly. Do not assume that an installed recovery system works effectively until you have actually run through the process. Think extensively of the possible disasters that your business could face and test against several scenarios that may arise.

Has your firm compiled a written information security plan?

A written information security plan (WISP) will avoid potential data breaches and assist you if a data breach does occur. The format is suggested by certain State departments of Consumer Affairs, eg.: http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf

Consider the following:

You suffer a data breach that compromises Personal Identifiable Information of clients.

By state law, you are required to formally notify all current and past clients that your firm had a significant data breach and it is possible that their personal confidential data may have been exposed to third parties.

What impact would this have on your business, your reputation, your long term stability?

If you can advise your clients that you have developed and implanted a written plan to protect their information you will reassure your clients and reduce the possibility of a lawsuit. If all data and data on hard drives is encrypted and protected it will minimize the impact on your operations and reassure your clients that you are taking all actions to protect their PII.

Cost of a Data Breach

In addition to your potential legal liability exposure, there are specific notification costs that may be payable in the event of a data breach. Many states have enacted consumer legislation that impose actions in the event of a security breach. Most of these laws require notification, and in some States, you must offer of credit monitoring to effected clients.

Estimated cost of notification per client: **$1.00 to $5.00**

If your firm has 2,000 clients (this may include previous and current clients), your cost just to notify them of a data breach may run **$10,000**.

Estimated cost of credit monitoring: **$10.00 to $50.00**

Although it appears that most individuals that receive data breach notifications do not elect to receive the credit monitoring, this trend may change dramatically.

With 2000 clients you are potentially facing **$20,000 to $100,000** in credit monitoring costs.

Insurance

Cyber Liability and Identity Theft Insurance is a relatively new insurance product that has been made available for both first party (your direct costs) and third party (legal liability) exposures. Securing a policy that pays for the legal defense, notification, and reimbursement of a data breach costs could significantly reduce the financial impact on your business.

The ability to demonstrate to Insurers that you have undertaken reasonable steps managing cyber and information liability risk may help reduce insurance premiums.

First Party Exposure

First party exposures are expenses incurred directly / internally by your firm for Cyber liability. This may include loss of hardware, loss of data, and damage to your internal systems. Cost can also include consequential losses (or business interruption) suffered while your business is closed. First Party coverage also includes the cost of client notification and/or credit reporting and regulatory defense and penalties. Some policies also include coverage for public relation services in the aftermath of a data breach.

Third Party Exposure

Third party exposure is the cost settlement and of lawyers fees to defend a legal action arising made by client that was financially harmed by a cyber attack or data breach caused by your failure to provide adequate safeguards to protect their PII. Claims generally involve a civil lawsuit or threat of suit, although some claims may be adjudicated in Mediation or other forms of alternative disputes resolution.

Conclusion

Cyber security should have a high priority in your office. Taking the steps to identify your potential exposures and creating a policy that assists your employees with the protection of your client data is now a necessity.

The identification of exposures and development of an Information Security plan will not only mitigate potential exposures, but provide peace of mind to your clients should a data breach occur.

Our suggestions and general recommendations in this article are not exhaustive, but illustrative only of possible good practice to adopt. Best practice would be dependent upon your specific needs which would need to be determined by yourselves and in consultation with others.

About the Authors

Gary Sutherland, CIC, MLIS is Chief Executive Officer, North American Professional Liability Insurance Agency, LLC – NAPLIA, a specialist in accounting and financial services firms.

Rickard Jorgensen, FCII, ACIArb, ARM. President of Jorgensen & Company, managers of **CPA***Gold*™, **Law***Gold*™, **Advisers***Gold*™, *The Firemark*™, InstantE&O™ and DentistSmartPlan™ professional liability insurance programs.

Gary Marshall, Solicitor at law, is an Arbitrtor and International Claims Consultant & Legal Consultant based in London.