Buyers Guide to Cyber Insurance

Currently no business is safe from privacy breaches and cyber attacks. Hackers have grown more sophisticated each day and as a result the demand for cyber insurance has grown significantly within Financial Institutions. Estimates vary but the average cost of a breach ranges anywhere from 300K to 5M. The market is very dynamic with coverages that vary from Insurer to Insurer.

We have developed unique partnerships with a variety of carriers that give us access to the best Network Security and Privacy Insurance solutions available within the USA. Understanding that each financial institution has different needs we have the ability to tailor your policy and its limits to minimize your cyber exposure/risk.

Insurers offer both first- and third-party insurance for cyber losses. First-party coverage insures for losses to the policyholder's own data or lost income or for other harm to the policyholder's business resulting from a data breach or cyber attack. Third-party coverage insures for the liability of the policyholder to third parties — including clients and governmental entities — arising from a data breach or cyber attack.

Available third-party coverages include:

- **Litigation and regulatory**. Covers the costs associated with civil lawsuits, judgments, settlements or penalties resulting from a cyber event.
- **Regulatory response**. Covers the legal, technical or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, investigations or other regulatory actions.
- **Notification costs**. Covers the costs to notify customers, employees or other victims affected by a cyber event, including notice required by law.
- **Crisis management**. Covers crisis management and public relations expenses incurred to educate customers concerning a cyber event and the policyholder's response, including the cost of advertising for this purpose.
- **Credit monitoring**. Covers the costs of credit monitoring, fraud monitoring or other related services to customers or employees affected by a cyber event.
- **Media liability**. Provides coverage for media liability, including coverage for copyright, trademark or service mark infringement resulting from online publication by the insured.
- **Privacy liability**. Provides coverage for liability to employees or customers for a breach of privacy.

The types of first-party coverage available include:

- **Theft and fraud**. Covers destruction or loss of the policyholder's data as the result of a criminal or fraudulent cyber event, including theft and transfer of funds.
- **Forensic investigation**. Covers the legal, technical or forensic services necessary to assess whether a cyber attack has occurred, to assess the impact of the attack and to stop an attack.
- **Business interruption**. Covers lost income and related costs where a policyholder is unable to conduct business due to a cyber event or data loss.
- **Extortion**. Provides coverage for the costs associated with the investigation of threats to commit cyber attacks against the policyholder's systems and for payments to extortionists who threaten to obtain and disclose sensitive information.
- **Computer data loss and restoration**. Covers physical damage to, or loss of use of, computer-related assets, including the costs of retrieving and restoring data, hardware, software or other information destroyed or damaged as the result of a cyber attack.

Ted Keller
561-235-7222 – Office
561-596-1619 – Mobile
tkeller@finrsk.com

Financial Risk Management

Recommendations for Buying Cyber Insurance

1. ***Identify Your Unique Risks.*** The first step in buying cyber insurance is to understand the nature and the extent of the risks facing your company. For some businesses, like banks or credit unions, the primary concern is the theft of personal financial information.

2. ***Understand Your Existing Coverage.*** Your company's standard first- and third-party policies may provide some protection from cyber risks, and it is important to understand what coverage, if any, may be available under your existing policies. For example, standard financial institution bonds provide coverage for third-party claims arising from a fraudulent computer instruction to transfer customer funds. Understanding your existing coverage will enable you to purchase the type of cyber insurance that your company needs.

3. ***Buy What You Need*.** With the variety of coverages offered by insurers in the market today, it is important to focus on the basics. You should consider whether your business needs all the coverages being offered and decline to purchase those that you do no need.

4. ***Secure Appropriate Limits and Sublimits.*** Perhaps the most important step a company can take to assess the value of cyber insurance is to compare the anticipated costs associated with a data breach with limits of liability available and the related costs.

5. ***Consider Coverage for Acts and Omissions by Third Parties*.** Many companies outsource data processing or storage to a third- party vendor. It is important that your cyber insurance policy provide coverage for claims that arise from misconduct by one of your vendors.

6. ***Evaluate Coverage for Data Restoration Costs*.** Many cyber insurance policies do not provide coverage for the costs to replace, upgrade or maintain a computer system that was breached. Data restoration costs are potentially prohibitive. Any company that faces the risk of a data breach should take steps to ensure that its policies provide coverage for the costs of putting the company back in the position it was in before the breach.

7. ***Involve All Stakeholders.*** As you consider the purchase of cyber insurance, be certain to involve all the potential constituencies within the company, including IT, treasury, finance and risk management. You are more likely to purchase the right policy with the right limits if you include all the divisions within the company who should have input into the insurance-buying decision.

8. ***Take Advantage of Risk Management Services.*** Many insurers offer cyber risk management services; you should consider whether your company needs these services, and if so, whether you should work with a carrier that offers a robust risk management program.

9. ***Understand The "Triggers."*** It is important to understand what activates coverage under your cyber policy. Some policies are triggered on the date the loss occurs, while others are triggered on the date that a claim is made against the insured. In order to provide proper notice, you need to understand how coverage applies under each policy you purchase.

10. ***Consider Coverage for Loss of Information on Unencrypted Devices.*** Many professionals today work on computers and tablets outside the office. Although many firms encrypt company-owned laptops, personally owned computers and storage devices are not. It is important for firms facing a loss of data through personal computers to buy insurance that provides coverage for such losses.

11. ***Consider Coverage for Regulatory Actions.*** A data loss may cause not only the loss of information, but also could result in regulatory actions against your company. State and federal agencies have become more active in responding to data and privacy breaches. You should consider whether your company's insurance policy provides coverage for a regulatory investigation or a regulatory action arising from a cyber incident.