SENTINEL RISK ADVISORS

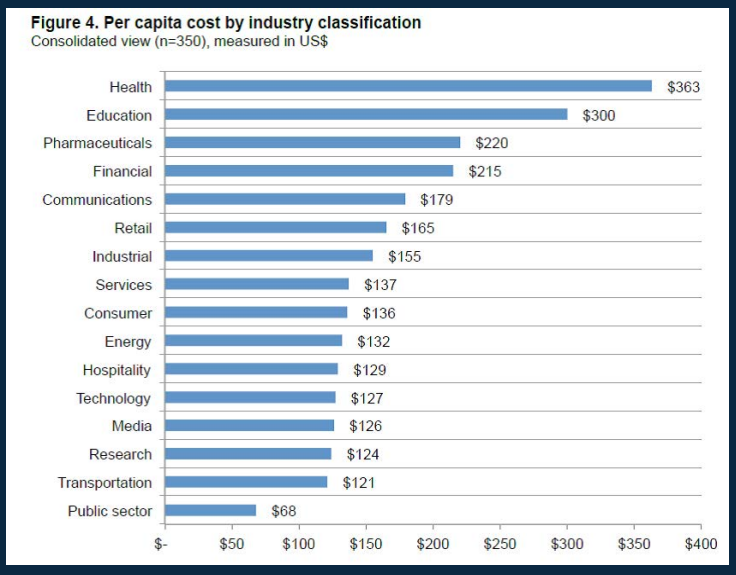
CYBER LIABILITY & INFORMATION SECURITY

In today's world, terms such as data breach and cyber liability are not new. With each year, it seems that these risks are becoming more and more prevalent both in our daily lives, as well as in our businesses. This publication will seek to bring you up to date on the current state of data breach, as well as attempt to unravel some of the complexities associated with proper risk management in this area.

One thing we know is that data breach is not slowing down. In the Poneman's 2015 Cost of Data Breach Study (Poneman Institute is considered the pre-eminent research center dedicated to privacy, data protection and information security policy) , it was reported that data breach is on the rise, continuing to escalate each year in both the number of breaches and the associated costs.

The United States has one of the highest per capita costs of data breach at an average of $217 per record (see chart.) This number contains both the direct costs, which may include utilizing forensic and legal experts and providing customer support and credit monitoring, as well as the indirect costs associated with in-house investigation, customer loss, and reputational harm.

In addition to understanding the costs of data breach, it is important to look at what industry segments are being targeted.
The short answer is all of them. What differentiates the industries is the cost associated with the breach.



When a data breach occurs, the repair process is more than just writing a check for $217 per record. Extraordinary coordination efforts must be deployed to handle the following:

1. Stop the breach (the forensic team will assess whether a breach occurred, work to stop the attack, and determine the impact)
2. Comply with individual state notification statutes and avoid fines and penalties (use of the legal team)
3. Protect your brand (use of the public relations team)
4. Address data loss/restoration needs (forensics and/or IT may be needed to rebuild computer systems and restore any lost data)
5. Mitigate/recover lost revenue (utilize internal resources and time)

Because of this, it is essential (and cost saving) to have a plan in place which will ensure a smooth facilitation.

Finally, the data breach arena is one that continues to evolve with each year. While notification for those whose information may have been compromised remains paramount, there are other areas of data breach which are concerning. 2015 saw an exponential rise in extortion, including ransomware and denial-of-service attacks. Another area of concern which has grown, and is now being addressed on many stand-alone crime policies, is targeted phishing scams. These are sometimes referred to as social engineering or spear phishing, but they all involve a cyber-criminal who attempts to impersonate a high ranking company official, usually through email, and instruct another employee to transfer what appears to be a legitimate wire transfer into the criminal's account.

Another increasing, and largely unresolved concern in the area of cyber liability is property damage resulting from a cyber incident. For the most part, cyber policies exclude property damage. For example, if through hacking, sprinklers are turned on and left on, most property polices will either exclude or significantly limit coverage for this risk; and general liability policies are typically going to exclude this risk. As we noted in the Sentinel '**2015 Market Review and 2016 Market Forecast**', there is an abundance of capacity and new markets being created; so while we are optimistic for a reasonable solution, there will likely be a lag.

When considering the potential of data breach and the costs that come with it, the most prudent measure a business can undertake is prevention. While not all breaches are preventable, we do know that those who have formulated a plan in advance of the breach suffer fewer damages when such an event occurs.

One of the first ways a business can mitigate risk from a potential data breach is to explore their own data retention plan. Failure to implement a data retention plan can be very costly if a data breach occurs. With notification to each record owner being required for each record that may have been compromised, it is imperative that records that are no longer needed be properly discarded. Each business should set guidelines for how long data (whether in the form of paper documents or electronic files) should be saved. In addition to this, there should be explicit instructions included for the destruction of data which is past its expiration. There have been a number of breaches that occurred because documents that were past their expiration were carelessly tossed in the dumpster. This can be a very costly mistake, and those employees who are tasked with the job of document destruction should be given the proper protocol for how it should be handled.

In addition to a document retention plan, having an incident response plan (IRP) in place is extremely important. An incident response plan should detail four key areas which include prevention, detection, response, and reporting:

1. **Prevention** - The IRP should include: a detection and response training schedule for employees (most insurers like to see this reviewed at least once a year), IT protocol and security safeguards which are to be in place, what type of security testing/monitoring will be performed and with what regularity.

2. **Detection** - Data breaches are not often detected at the onset, so it is important that employees be taught what it is they are to look for in hopes of stopping data breach. If issues like suspicious emails and viruses are reported right away, potential hackings can often be mitigated. For those companies with IT departments, the level at which IT should be monitoring for detection of potential breaches should also be laid out.

3. **Response** - Once a potential data breach is discovered, it is important that the person who made the discovery knows where to turn. An internal chain of command should be established so that employees know who to contact and in what manner (email, phone, face to face conversation). Once reported, there should be protocol for who is contacted next - whether it be IT, the insurance carrier, legal counsel, authorities, etc. This determination will help guide the response that follows: mitigation/remediation, forensic analysis, recovery, notification, and lessons learned.

4. **Reporting** - Because reporting in the event of a breach is necessary to avoid certain regulatory fines and penalties, the IRP should include a list of which entities should be notified of the breach. It is also important to detail who will be the one to provide these reports and in what timeframe.

One of the final components of data breach risk mitigation is contract review. Many businesses today utilize third party vendors to house and manage data. With these relationships come contracts, and it is important that these documents are reviewed carefully. You may be able to negotiate your own third party vendor contract, but it is also good to ask if your vendor is using other third parties to do your work. If so, a follow up detailing what requirements they have for their vendors is prudent. Some questions that should be addressed for vendors and any additional subcontractors are:

- Do they have cyber insurance? If yes, what limits / sublimits? What are the retentions?
    - If a subcontractor, does the vendor require cyber insurance?
- What do the indemnification provisions look like?
- In the event of potential breach, how soon is notification required to the parties of the contract?

One final method to mitigate the costs of data breach is through insurance. In addition to the cost, the time required for handling a data breach can be substantial, and insurance allows a business to streamline the process. When cyber liability insurance is in place, the Insured makes a call to their insurer or broker and the insurer will then deploy the pre-vetted team (which may include legal, forensics, public relations, etc.) to immediately begin assessing and managing the situation.

Cyber liability insurance has been in the news the last few years, but the fact of the matter is this is not a new coverage. Some carriers have been offering cyber coverage to their clients since the late 1990s. Since that time, there has not only been an evolution in coverage, but also in insurers who have entered the marketplace. Today there are more than 50 insurers that provide some type of stand- alone cyber insurance, and that number doesn't contemplate those insurers that are offering some type of cyber coverage enhancement to their package policies.

What this means for the consumer is there is great opportunity for those who are interested in adding this protective layer to their business. Insurance companies are not only willing to compete on pricing but coverage as well. It is very important to note that in this constantly evolving area of insurance, not all policies provide the same coverages. It is critical to make sure that your broker understands the market and coverages available to you so that you receive a carefully crafted policy that is priced appropriately.

When looking at coverage of a cyber liability policy, it is important to know what you need and what you are buying. The names of the different insuring agreements and coverage components may vary from carrier to carrier, but below is a summary of what to look for when examining a cyber liability policy:

- **Event Management** - Carriers often bundle legal billings, forensic services, and public relations into one insuring agreement. In the event of a breach, this insuring agreement is a crucial lifeline. It is very important to determine if this coverage is provided at full policy limits or whether it is sublimited. Depending on your business's needs, a sublimit in this area may not be adequate.

- **Network Security/Privacy Liability** - This area of coverage contemplates loss of data. Some policies provide first party coverage, some provide third party coverage, and others provide both. This distinction can be a crucial part building an appropriate cyber liability policy. Other items to note in these coverage sections are does the policy cover transmission of malicious code, does the policy cover hackings by rogue employees, and does the policy cover paper as well as electronic data.

- **Regulatory Fines and Penalties** - Data breaches can come with regulatory fines and penalties when data is not properly safeguarded or notification does not meet statutory requirements. Most cyber liability policies have some insuring agreement to address this, but one distinction that should be addressed is whether the coverage is for defense only or does it in fact cover fines.

- **Media Liability** - This area of coverage is meant to protect against claims of copyright infringement, libel/slander, etc. in media publications. It may also extend to other forms of media beyond a website and social media platforms.

- **Extortion** - As hacking becomes more prevalent, we are also seeing an increase in extortion claims. In these scenarios the hacker will demand a ransom for data which has been segmented out or access to a system which has been immobilized. This coverage provides monies that can be used for such payments, but only after such payment is authorized by the insurance carrier.

- **Business Interruption** - In certain industries, a data breach may leave a business unable to render services. Is this case, business interruption coverage may be available. Not all carriers offer this, and each carrier has a different waiting period before the coverage becomes available.

- **Property** - This is an area that is currently excluded on most stand-alone cyber liability policies. However, AIG is offering CyberEdge PC (first of its kind) providing excess and difference-in-conditions cyber insurance for property damage (first party). As a new product, the pricing, limits and deductibles may not be as competitive as a buyer may desire. London also offers difference-in conditions polices for cyber, but again, pricing, limits and deductibles may not meet a buyer's expectation. Larger businesses purchasing all-risk property program coverage may find that their insurers fully intend to cover property damage (first-party) from a cyber-attack. However, smaller and package policies must be carefully reviewed to understand the level of coverage being provided.

In addition to the different insuring agreements, it is also critical to be aware of the exclusions that your policy may contain. One of the most important exclusions seen on a cyber liability policy is failure to maintain certain controls. When an Insured completes a cyber application, they warrant that certain protocols are in place. Failure to maintain these controls can negate coverage. For this reason, if changes are being made to security controls, it is imperative that the Insured confer with their cyber liability provider prior to doing so. Another exclusion that many carriers like to utilize is a failure to encrypt data or failure to encrypt mobile devices. Carriers have made it known that they prefer to see their Insureds' data encrypted, and many will include an encryption exclusion of some sort on their policy. Because cyber liability coverage is one that is constantly evolving, it is important that these exclusions be reviewed at initial placement and also at renewal for any changes.

Business wide cyber activity and cyber losses are increasing beyond the loss of data. All companies, in all industries should review their exposures and evaluate various insurance options to mitigate or transfer their risks. Businesses that purchased cyber coverage should remain vigilant and review their insurance portfolio, not just the cyber policy.

Cyber threats are omnipresent and growing. We expect cyber insurance to continue to evolve to address the risks and issues of their insureds.

SENTINEL RISK ADVISORS

4700 Six Forks Road - Suite 200 - Raleigh, NC 27609

Phone: 919.926.4623 Fax: 919.926.4664 Toll Free: 855.490.2528

www.sentinelra.com