Cyber/Privacy Insurance
Talking Points for Clients

1. Breach Response Team and Breach Coach

The Breach Response team and coach are perhaps one of the more important things to consider when purchasing a Cyber/Privacy Policy. When a breach occurs, you will not know what to do and how to assess the risk and responsibilities. You will greatly appreciate being able to get in touch with a breach coach within hours of discovery. The ability to mitigate liability and further limit damages is critical in the first few hours of a breach. Many companies use outside vendors that refer claims to evaluate insurance coverage before responding and they lose critical time. There are only a couple of major firms that specialize in responding to a breach. The agent should make sure they know who the breach coach is and if there is a deductible for the breach coach.

The Breach Coach (law firm) should always hire the forensics team and not the insured. The reason is that if the law firm hires the forensics team, any reports and findings are privileged and not discoverable.

2. Pay on Behalf of

Similar to other insurance policies, Cyber/Privacy policies can be a "duty to defend" or "pay on behalf of" policy. This is important since it will determine whether the insurance company pays directly for the defense and indemnity or whether the insured has to arrange for and pay for their own, investigation, forensics and defense and then seek reimbursement from the carrier. Further, there may be parts of a policy that are paid directly by the carrier and other parts that must be paid by the insured first. Often business interruption and the first party costs are going to be "pay on behalf of" even if the rest of the policy is a "duty to defend" policy.

3. Primary and Non Contributory

Most insurance policies have an "other insurance clause." When placing a cyber policy, this can be problematic and lead to multiple deductibles and confusion at the onset of a claim as to who is to respond to a claim. Response time by the insured and their team is critical and you don't want to have to negotiate who is responsible for the claim. Many GL, D&O, and E&O policies have some cyber coverage. This can trigger "other insurance" clauses and lead to delays and unforeseen costs by the insured. Request that the Cyber/Privacy policy be primary and non-contributory.

4. PCI Fines and Penalties

PCI fines and penalties can be assessed by credit card companies for failure to have proper safeguards which can cause the credit card companies a financial loss. The fine and penalty can be included in the contract with the credit card company and therefore in the event of an assessment, the payment can be looked at as a contractual obligation rather than a covered liability. Further, as noted above, the liability may be deemed an "Assessment" which is neither a fine nor penalty. Some of these fines can be very hefty; as in the millions. Many of the newer policy forms will have full policy limits for PCI fines and penalties. The wording of a policy may not define an "assessment" as a fine or penalty.

Contact our experts today to find out how you can protect your business.

Axis Insurance Services, LLC
795 Franklin Avenue, Suite 206
Franklin Lakes, NJ 07417

www.axisins.com
P: 201-847-9175
F: 201-847-9174

5. Other Regulatory Fines and Penalties

The actual cost of a breach and unauthorized disclosure of confidential information can be significant even for small breaches. Additionally, many regulatory agencies can impose their own fines and penalties. Some carriers attempt to limit coverage for these fines and penalties since they are punitive in nature. If the data is Healthcare related, the fines can be even more significant. For example: HIPAA fines can be from $100 to $50,000 per record. Where the policy lists multiple acts such as HIPAA, ACA, etc., it should also include the words "or similar local, state or federal statute or regulation."

6. Third Party Cloud Data and Breaches

Most companies use third party "cloud" providers such as AMS, ADP, Amazon, Applied and Google just to name a few. The data entrusted to insureds by their clients is then entrusted to these third parties. What happens if the data is breached at the third party vendor site? In general, the insured is still responsible for liability, notifications and damages. Further, many of the cloud providers have indemnity agreements that limit their liability to fees paid. Additionally, if there truly was a breach at a third party vendor, they most likely would not have enough insurance to indemnify all of their clients. A properly structured Cyber/Privacy policy will cover your data in the event it is housed by a third party vendor and is breached. Some policies will even extend first party coverage to the third party vendor in order to mitigate damages.

7. First Party Costs

The major costs in a breach continue to be first party payments. Carriers try to mitigate this exposure by providing sub limits, limiting the number of records, or in other creative ways. Additionally, some carriers will provide these limits both inside and outside the limit of liability. These are the most important aspects of the coverage and where you will incur the most costs in the event of a breach. Data forensics is one of the largest costs as those professionals charge between $500-$1,000 per hour for their services. Keep in mind, your Breach Coach (attorney) should hire them so that their work is not discoverable.



Contact our experts today to find out how you can protect your business.

Axis Insurance Services, LLC
795 Franklin Avenue, Suite 206
Franklin Lakes, NJ 07417

www.axisins.com
P: 201-847-9175
F: 201-847-9174

8. Business Interruption

Business interruption for a Cyber/Privacy policy is no different than that for a Commercial Property policy or a BOP. A covered claim is the trigger for Business Income. One key difference between BI in a Commercial Property policy and BI in a Cyber/Privacy policy is that there is typically a waiting period of 8 to 10 hours. Meaning bringing a website down for an hour will not trigger a business interruption claim. Also, note that you will need to be able to prove a loss similar to a Commercial Property Business Interruption claim. So for example, many professional service firms couldn't document a loss in revenue for their server being down for a day, whereas a website selling widgets that can demonstrate what daily sales (and income) might have a claim.



In most cyber policies, the definition of the cyber business interruption is similar to the ISO standard time element definition: net profit (or loss) + ongoing expenses, during the period of restoration. Salaries may or may not be included. Some provide only a 30 day period of restoration, some up to 120 days. Some will also extend time element to an attack of a dependent provider network.

9. Encryption

Carriers have varying requirements as it relates to encryption (full disk, mobile device, standing data, cloud data, etc.) The carrier may require that all mobile devices be encrypted. The term mobile device may apply to laptops, cell phones and tablets, but may also apply to flash drives and portable hard drives, etc. Most insureds don't encrypt flash drives and cell phones. They may be password protected, but most are not encrypted. One issue relates to standing data. This means are backups encrypted, are servers encrypted and are all desktop units encrypted? You need to ask yourself these questions as the policy may be void as to any mobile device or standing device that is not encrypted as defined in the policy.

Encryption is also a vague term. Many encryption programs provide a shell (boot) encryption. You need to fully understand what is encrypted, how it is encrypted and how that relates to the coverage afforded in the Cyber/Privacy policy. Many policies will not respond unless the device is full disk encrypted.

Contact our experts today to find out how you can protect your business.

Axis Insurance Services, LLC
795 Franklin Avenue, Suite 206
Franklin Lakes, NJ 07417

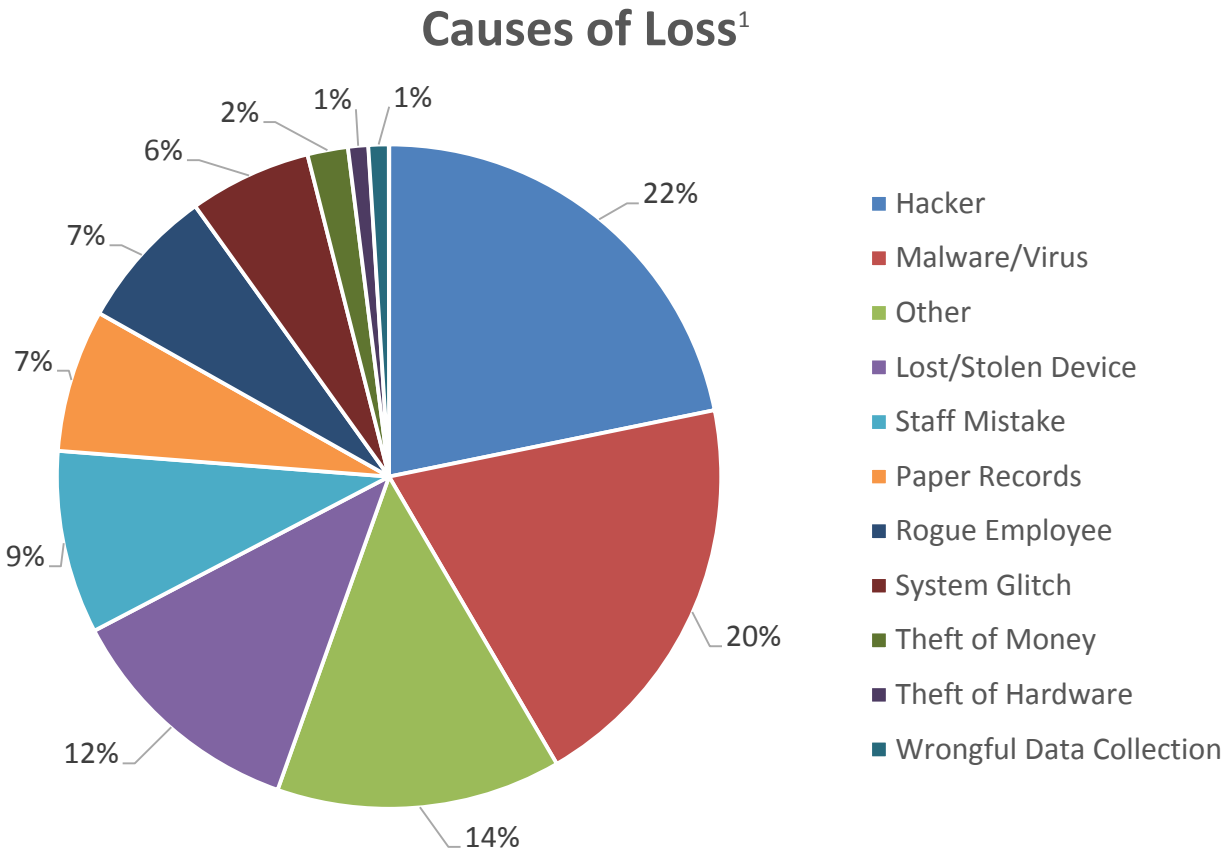
www.axisins.com
P: 201-847-9175
F: 201-847-9174

10. Social Engineering

Social Engineering is the buzz term of the year. Privacy and Crime Insurance companies fight as to who should pay for the loss. In most cases, a Privacy policy is concerned with loss of data and a Crime policy is concerned with loss of money and securities. The debate is what if there is a loss of funds as it relates to a hacking or breach event or a phishing or spear phishing event. Many of the Privacy carriers are beginning to offer a sublimit of $100,000 to $250,000 to cover the exposure of voluntarily parting with money due to fraudulent instructions through a spear phishing event. Most Privacy carriers at this point are not covering this exposure but there are several that do. Most Crime policies are evolving to cover voluntary parting of funds due to fraudulent instructions.

11. Other Issues of Note

- Class Action Exclusions
- Bodily Injury/Personal Injury Exclusions
- Media Liability
- Loss Sustained versus Loss Discovered



[1]Source: NetDiligence

9/1/16

Contact our experts today to find out how you can protect your business.

Axis Insurance Services, LLC
795 Franklin Avenue, Suite 206
Franklin Lakes, NJ 07417

www.axisins.com
P: 201-847-9175
F: 201-847-9174