



AXIS INSURANCE SERVICES, LLC

Cyber/Privacy Insurance

795 Franklin Ave, Suite 210

Franklin Lakes, NJ 07417

P: 201-847-9175

F: 201-847-9174

www.axisins.com

Security & Privacy Liability - Provides coverage for both defense expenses and damages from claims made against you for failing to provide adequate data security, or for failing to protect the personally identifiable information, in your custody.

Multimedia Liability - Provides insurance coverage for claims arising from your advertising, media, online media or social media material.

Technology E&O - Technology E&O provides coverage for claims against you arising from the information technology professional services your company provides.

Miscellaneous E&O - Miscellaneous E&O covers specifically described professional services that a company provides, which fall outside IT services.

Breach Expenses - Covers the typical expenses a company will incur, following a data breach event, such as data forensics, notification expenses and identity monitoring & restoration. Also included are legal and public relations expenses.

Privacy Regulatory Defense & Penalties - Provides coverage for the costs of defending a regulatory investigation following a data breach, along with any fines or penalties which result from that investigation.

Reputational Damage – This will reimburse you for a reduction in profit that you experience as a direct result of the loss of customers due to damage to your business reputation, caused by a data breach.

Cyber Crime - Provides coverage for the electronic theft of funds or other assets by a third party, including theft by fraudulent instrument or fraudulent transfer, or credit card fraud.

Social Engineering - Social engineering is theft by manipulation, where a third party masquerades as an employee, client or other business contact, in order to trick the insured into surrendering funds or other assets voluntarily.

System Damage - Provides coverage for the expenses the insured incurs to retrieve, restore or replace computer programs or data, which were damaged by a data breach or hacking event.

Cyber Business Interruption - Covers your company's lost profit, plus the extra expense you incur, following a data breach even which results in a system outage of longer than ten (10) hours.



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.

5. Other Regulatory Fines and Penalties

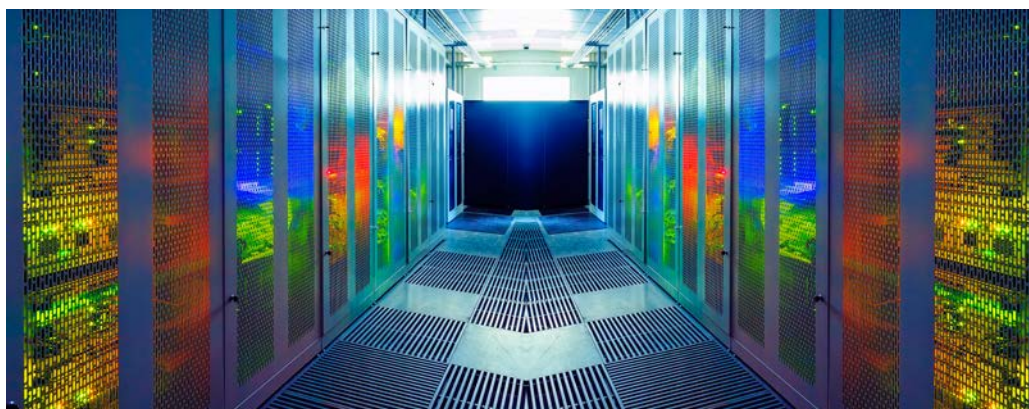
The actual cost of a breach and unauthorized disclosure of confidential information can be significant even for small breaches. Additionally, many regulatory agencies can impose their own fines and penalties. Some carriers attempt to limit coverage for these fines and penalties since they are punitive 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.



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.

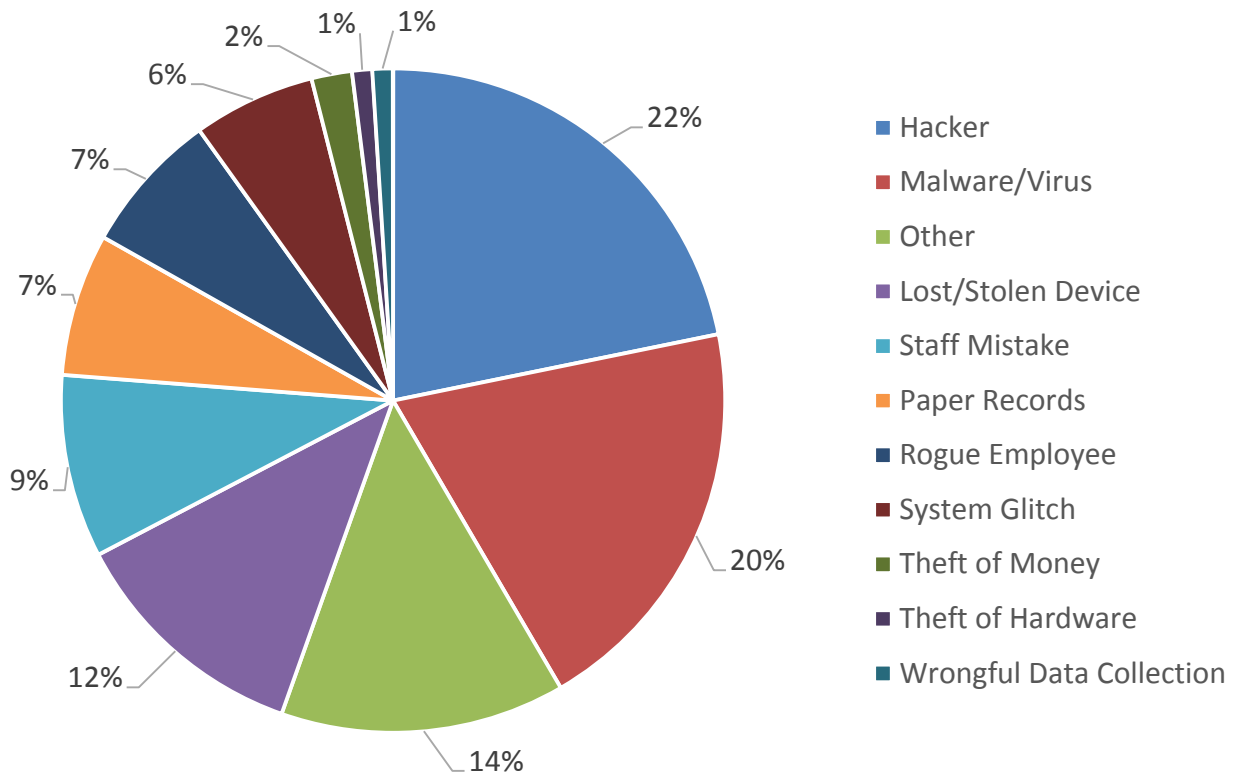
10. Social Engineering

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

Causes of Loss¹



¹Source: NetDiligence

3/1/17

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

- **Breach Discovery**
- **Experts**
 - Breach Coach
 - Forensics
 - Public Relations
- **Investigation**
 - How, when, who, what?
 - Is it over?
- **Notification Obligations**
 - State
 - Federal
 - Other (PCI, FDIC, OCR)
- **Notification Methods**
 - Written
 - Electronic
 - Substitute
- **Deadlines**
 - Can be from 48 hours to “without unreasonable delay”
- **Inquiries**
 - State/Federal Regulators (AG, OCR)
 - Federal Agencies (SEC, FTC)
 - Consumer Reporting Agencies
- **Litigation**
 - Subrogation
 - Class actions



A. “We are not Target or Home Depot. No one would care about us.”

- You are less sophisticated.
- You have less security.
- You are an easier target.

B. “We have a good IT department and a firewall.”

- So did Sony, Target, Home Depot, and PayPal.
- More claims relating to small businesses are related to employee error than hacking.
- IT individuals are like artists, take pride in their work, and often don't like others in their controls. It makes it difficult to see if there really are issues.

C. “We will get a breach team if we need one.”

- Once you have a breach, you are at the mercy of whoever is available and the costs. It's similar to buying a plane ticket on the last day.
- It has consistently been shown that costs related to an insured breach are less than 50% of other breaches. Insurance policies come with discounted rates, already assembled teams and knowledgeable resources.



D. “It's too much money.”

- Cyber is relatively cheap.
- An average breach of 10,000 records can cost in excess of \$1M.
- It isn't a matter of “if” you will have an issue, it is “when.”

E. “We don't have any PII.”

- Everyone has PII
- Recent issues involved PII
 - Theft of W-2s
 - Maliciously sent emails with malware
 - Crypto locker

F. “My data is at a third party vendor.”

- Those contracts have indemnity limitations.
- They can't indemnify all parties if they had to (40,000 agencies on AMS).
- You are still responsible for your data that is stored in the cloud.

What is Privacy & Network Security Liability Insurance?

Privacy & Network Security (Cyber) liability insurance provides coverage for the costs associated with the misuse, loss, or theft of data including personally identifiable information, sensitive health information, proprietary data and financial information stored in an electronic or physical format.

Why do I need a Privacy & Network Security Liability policy?

Business professionals need this protection to cover 1st and 3rd party costs arising from claims of a data breach or theft of personally identifiable information or information subject to HIPAA regulations. Privacy & Network Security insurance is a must for small and large firms to protect against this increasingly wide spread exposure.

What does a Privacy & Network Security Liability policy cover?

This policy covers the defense costs and other expenses for an insured's failure to protect confidential data stored in physical records or electronically on a computer network, data storage unit or device. This typically includes coverage for the following:

- **Network Security** – Covers claims made by 3rd parties arising out of a breach of their computer network and data storage units or devices. This includes coverage for both online and offline information, denial of service attacks, and for the failure to prevent the transmission of a virus or malicious code.
- **Privacy Breach Response Costs** – Includes coverage for the reasonable legal fees, public relations fees, advertising, IT/Data forensic services, credit monitoring, notification costs, identity theft restoration and postage expenses incurred by the insured in response to a privacy breach.
- **Network Asset Protection** – Coverage for the reasonable and necessary sums required to recover and/or replace data that is compromised, damaged, lost, erased or corrupted.
- **Regulatory Defense & Penalties** – Coverage for defense costs and fines or penalties for violations of privacy regulations, including, but not limited to, HIPAA, Red Flags Rule and the Hi-Tech Act.
- **Multimedia Insurance** – Coverage for both online and offline media, including claims alleging copyright/trademark infringement, libel/slander, false advertising, plagiarism and personal injury.
- **Business Interruption** – Coverage for income loss or expenses due to a computer system outage or repair.

Why choose Axis Insurance Services?

Unlike most brokers, our professionals specialize in professional liability and are nationally recognized. Our years of expertise in the industry allow us direct access to high-quality insurance carriers, extremely competitive rates and the ability to customize insurance solutions to meet the needs of our clients. Call us for a quick review of your current policy to ensure you and your business are properly protected.

Claim Scenarios:

Stolen Identities

A business was hacked by someone who steals the social security numbers and bank account details of its employees and customers. The information was sold to a website which uses the information to create false identities. The defense and damages resulting from the lawsuits exceeded \$900,000.

Lost Data

An employee's company laptop was lost on the train. The laptop contained files of private financial information of their customers. The company had to pay for notification to their customers that their private financial information was no longer secure. Their customers sued the company for damages resulting from their failure to protect their private financial information. The notification costs and settlement totaled \$350,000.

Troubled Employee

A problematic employee found out that he was about to be terminated and in response, stole personal account details that the business held on its clients, and published them online. When the clients find out about this, they sued for invasion of privacy and demand remediation. Total settlement and defense costs exceeded \$600,000.

Customer Privacy

An employee at an engineering firm found a way through his company's network security defenses and gained access to a customer's trade secret. The employee sold the trade secret to a competitor. The customer sued the engineering firm for the failure to protect the trade secret and was awarded for damages. The customer received over \$500,000.

Physical Files

Confidential paper files containing names and checking account information of an organization's donors were found in a dumpster in an organization's parking lot. The press gained access to the documents and published an article in the local newspaper. The organization needed to notify all affected donors and pay for advertising in the local newspaper. The notification and advertising costs added up to around \$50,000.

Network Security

An employee inadvertently downloaded a destructive computer virus onto the company's network, resulting in widespread data loss and transmission of the virus to a client's computer network. The client sued the company, contending they should have prevented transmission of the virus. Damages of \$750,000 were sought for the lost data and economic loss caused by the network security breach.

These are only claims examples: minor changes from actual suits have been made to protect the confidentiality of all clients.

6/1/15

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