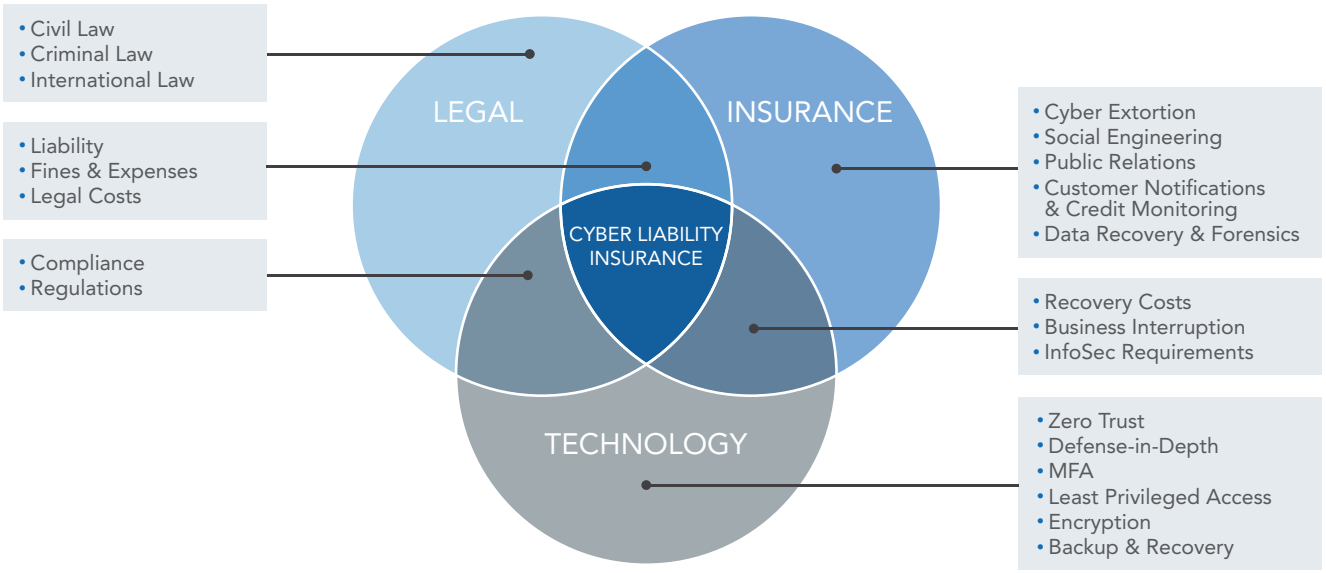
DESIGNING FOR Cyber Liability

Cyber Liability is both a hot button topic, and a rapidly evolving field that exists at the intersection of technology, law, and insurance. Cyber Liability is any liability relating to obtaining, storing, securing, authorized or unauthorized use, disclosure, or transmission of electronic data of any kind. The fast pace of change and intersection of business and technology functions creates a complex landscape for companies looking to navigate Cyber Liability.



> Any approach to Cyber Liability should move top to bottom, starting with legal, then moving through insurance to technology. This flow starts in the broadest terms defined within the legal domain, while considering compliance and regulatory requirements. This will allow you to define what Information Security (InfoSec) professionals often call 'Big P', the highest level of policy.

Big P policy defines broad stroke requirements your organization is required to, or chooses to implement within the Information Technology (IT) stack. An example component of Big P policy might be IT requirements for separating Payment Card Industry (PCI) regulated data from non-regulated data. Big P may go so far as to mandate encryption for that data in-flight (while being transferred), at-rest (while being stored), or both.

Big P will stop before defining how, where, and when this will be done. Big P focuses on the 'what' and 'why' of the "Five w's". This is often described as a declarative model. Big P declares an outcome that must be achieved, the implementation required to achieve that outcome is handled further down the stack. Big P operates like a General leading troops in battle. They may command a unit to secure and fortify a hill, the unit's leader is responsible for the tactical implementation of that command.

DESIGNING FOR Cyber Liability

A well-defined Big P will aid organizations in selecting the cyber insurance requirements they have. InfoSec is a constant exercise in risk assessment. The business must decide how the costs of exposure weigh against the costs of security measures and insurance costs. Big P helps define one side of those costs, the cost of noncompliance, while simultaneously defining the specific big picture security requirements.

InfoSec is a constant exercise in risk assessment.

The business must also define costs not defined elsewhere. These costs range from 'soft-costs' (subjectively defined) to hard costs with firm definitions. Loss of reputation is an example of a soft cost. What is the value of your company's reputation? How much value will be lost in the event of a public InfoSec breach? Hard costs include the cost of paying a ransom to restore your data, and costs for things like credit monitoring for customers whose personal data was accessed during a breach.

The definition of these costs, combined with your Big P, will allow you to assess the Cyber Liability insurance requirements of your organization. You know what you must protect, and the cost of failing to do that. This will allow you to weigh the options of Cyber Liability insurance components, and their costs, against your businesses needs and risks. You'll also have an understanding of the limits you need, whether mandated by a law or aspect of your business or based on your cost exercises above.

Cyber Liability insurance can be broken down into five major categories: Cyber Extortion, Social Engineering, Public Relations, Data Recovery and Forensics, and Customer Requirements:

Cyber Extortion: Covers incidents where IT assets are held for ransom by attackers. The most common occurrence of this is ransomware attacks that encrypt your data, making it inaccessible until you pay a ransom.

Social Engineering: Covers events where an individual, typically an employee, is coerced into enabling an attack. Two common examples are phishing emails manipulating a user to click a link that compromises their system, and spoofed emails from company executives requesting bank transfers which secretly lead to attacker's accounts.

Public Relations: Covers costs that arise from loss of reputation or restoring that reputation. These costs are both subjective and varying based on organization and industry. For example, the reputation of a leading InfoSec technology vendor is more at risk than a small chain of restaurants whose customers' come for the food and atmosphere.

Data Recovery and Forensics: Covers costs that arise from discovering what was breached, and how. It also covers the costs of recovering your data, which may include ransomware costs up to a limit.

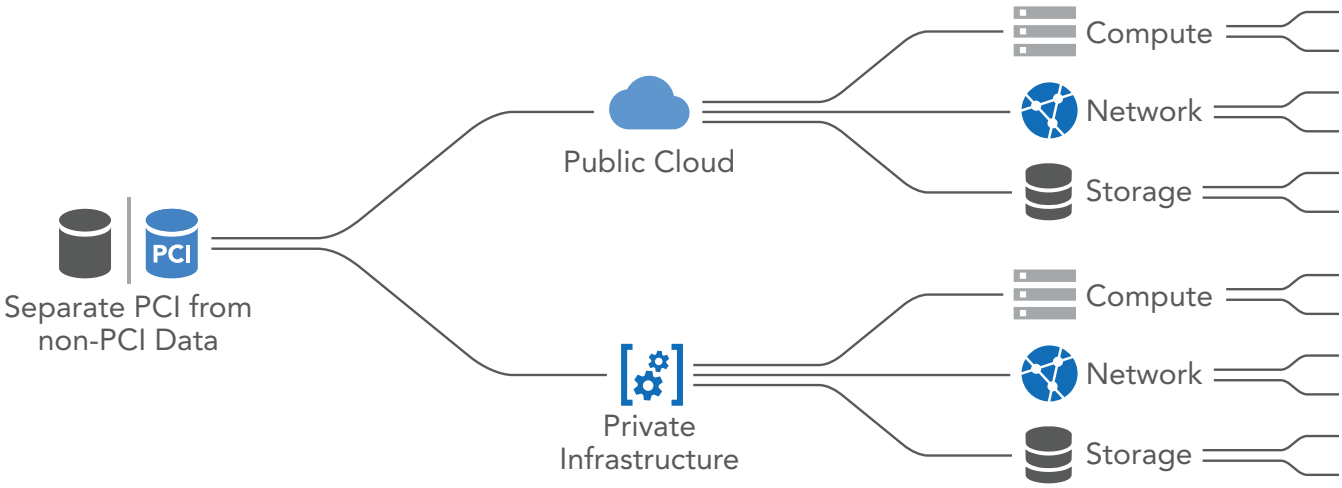
Customer Requirements: Covers costs of your legal requirements to your customers based on state and federal law (often, both your company's state and the customer's state laws apply.) An example of this would be customer notification and credit monitoring services.

DESIGNING FOR Cyber Liability

The insurance provider you select will have unique options for each of these categories. They will often also dictate specific security requirements which may add to your Big P or define specifics for the technology implementation. For example, they may require you to add Cybersecurity Training to your Big P, while mandating that you implement Multi-Factor Authentication (MFA), or backups which are implementation details for the technology stack (these may also be referenced in Big P).

With legal and insurance requirements defined you now have a complete Big P, and often some definition of technical requirements, known as 'Little P', or simply policy. Policy is the translation point from legal and business requirements to implementation specifics.

In our Big P example above we stated, 'Separate PCI regulated data from non-regulated data'. This is a broad stroke statement which applies to a variety of disparate technology domains. Those domains include, but aren't limited to, server & workload, storage, network, and application. That Big P requirement will need to be translated into policy for each domain. Below is a high-level flow showing how this might look.



The example above illustrates just how important it is to have a well-defined Big P that meets the requirements of your business, and insurer, before designing for policy at the InfoSec layer. The implementation of InfoSec policy covers a wide array of technology solutions, each with unique security features and configurations. Without Big P as a 'North Star' to navigate with, policy requirements will be missed along the journey.

A well Defined 'Big P' is Critical to InfoSec Policy Success.

Designing for Cyber Liability doesn't have to be difficult. With a well-defined plan you can move from the broadest requirements to the most granular in incremental fashion. Working top down from legal, to insurance, and ending with the technology will provide InfoSec teams with clear declaration of intent. That intent can then be translated to the policy required at any level of specificity.

Have a specific question or project you'd like to discuss with an expert?
Send a note to info@cassevern.com or just give us a call at 800.252.4715.

IBM Cloud Object Storage

Protect Your Data Against Deletion or Modification

Immutable object storage from IBM Cloud® is designed to help clients preserve records and maintain data integrity in a Write-Once-Read-Many (WORM), non-erasable and non-rewritable manner to protect against deletion or modification until the end of retention periods and the removal of any legal holds.

How is Immutable Object Storage from IBM Cloud® Used?

By creating and enforcing retention policies. Preserve data for a specific retention period using IBM Cloud Object Storage UI or API. Specify a default, minimum or maximum retention period.

1. Create a storage bucket
   Use IBM Cloud Object Storage to create a storage bucket for your unstructured data.
2. Set a retention policy
   Write an object to a bucket with a specific or inherited retention policy.
3. Apply a legal hold
   Prevent individual objects from being deleted or overwritten.

Immutable Data Highlights

Control
Ability to set retention policy on a bucket and specify retention period

Support
Support for variable user-defined retention periods

Options
Object written to a bucket with a retention policy can inherit the default retention period or have a user-defined retention period

Protection
Individual object within a bucket with a retention policy can have legal hold(s) — preventing object from being deleted or overwritten

Settings
Use of API extensions for setting and viewing retention period at a bucket and object level

UI
Ability to efficiently set and manage retention periods by using enhanced UI

Would you like to know how IBM can help you with you cyber liability needs?

As an Platinum IBM Business Partner,
CAS Severn can help cut your storage costs
and reduce malware, disaster and outage losses.
Send a note to **info@cassevern.com** or give us a call at 800.252.4715.

IBM® Platinum Business Partner™