Building and Personal Property Coverage Form (BPP)

A commercial property coverage form that can be used to cover buildings, "your business personal property," and personal property of others.

Commercial General Liability Coverage Form

A coverage form commonly used for insuring an organization's premises and operations liability loss exposures and products and completed operations liability loss exposures.

Business Income (and Extra Expense) Coverage Form

Form that covers both business income and extra expense losses (even if the extra expenses do not reduce the business income loss).

Businessowners policy (BOP)

A package policy that combines most of the property and liability coverages needed by small and medium-size businesses.

Crime insurance

Insurance that covers (1) money and securities against numerous perils (not limited to crime perils) and (2) property other than money and securities against crime perils, such as employee theft, robbery, theft by outsiders, and extortion.

Cyber Touchpoints in Traditional Policies

Traditional policies that are frequently requested to provide coverage for a cyber loss include these:

- **Building and Personal Property (BPP) Coverage Form**
- **Commercial General Liability (CGL) Coverage Form**
- **Business Income (and Extra Expense) Coverage Form**
- **Businessowners policy (BOP)**
- **Crime insurance**
- Directors and officers (D&O) liability insurance

These traditional policies provide commercial liability coverage, property coverage, or both coverages together as a package. Liability coverage protects an organization from third-party losses, and property coverage protects an organization from first-party losses. Traditional policies generally do not provide substantial protection from a cyber loss for one or more of these reasons:

- The cyber loss is not a **triggering event** under a policy's **insuring agreement**.
- The cyber loss is not included within the definition of a relevant policy term—for example, property damage is a term defined in a CGL policy as physical injury to tangible property. The definition further states that, for the purposes of this insurance, electronic data is not considered tangible property.
- The cyber loss is specifically excluded.
- The cyber loss is capped at a low limit.

Essentially, most traditional policies are not designed to cover first- or third-party cyber losses. Organizations instead rely on specialized cyber insurance products to cover cyber exposures.

Coverages Needed

Most organizations that choose to manage cyber threats by risk transfer need coverage for both first-party property and third-party liability cyber exposures. Businesses in the same industry tend to share many of the same risks. For example, retailers are often most concerned about a breach of their database exposing customers' private information. In contrast, a power utility company is likely more concerned about attacks on its network. In addition to the cyber exposures that are common to each industry, each organization has its own, unique cyber exposures. See the exhibit "Cyber Exposures: First Party or Third Party?"

Cyber Exposures: First Party or Third Party?

In the market for cyber risk coverages, there is not a consistent standard for determining whether certain loss exposures are first party or third party. For the purposes of this course material, reputation mitigation and response to regulatory action are regarded as first-party loss exposures, even though some policies label them as third-party loss exposures.

[DA11368]

Triggering event

An event that sets in motion, or initiates, other events.

Insuring agreement

A statement in an insurance policy that the insurer will, under described circumstances, make a loss payment or provide a service.

While not all cyber coverages are required by every organization, third-party coverages that are often needed include these:

- Defense and payment of liability claims asserted by third parties for allowing a breach to occur
- Protection from allegations of intellectual property infringement in an insured's online publications and other forms of media liability
- Breach of privacy liability if employees' or customers' private information is released to an unauthorized party

First-party coverages that are often needed include these:

- Forensic study to determine the scope of the breach
- Business income for loss of income when operations are temporarily shut down
- Reputation mitigation, such as damage control through public relations and education of customers
- Response to regulatory action, such as investigation into whether the organization implemented the minimum required cyber security measures and sent both adequate and timely notification as well as potential fines or penalties assessed
- Restoration of data that was lost as a result of cyber attack[1]

The Need for Specialized Cyber Risk Insurance Products

A mid-size or smaller organization may not have the capital to pay the costs incurred to resolve a cyber loss if its risk management strategy fails to prevent or fully mitigate a cyber breach. Such a cyber loss could bankrupt an organization and therefore emphasizes the need to transfer cyber risks to an insurer that offers specialized cyber risk insurance products.