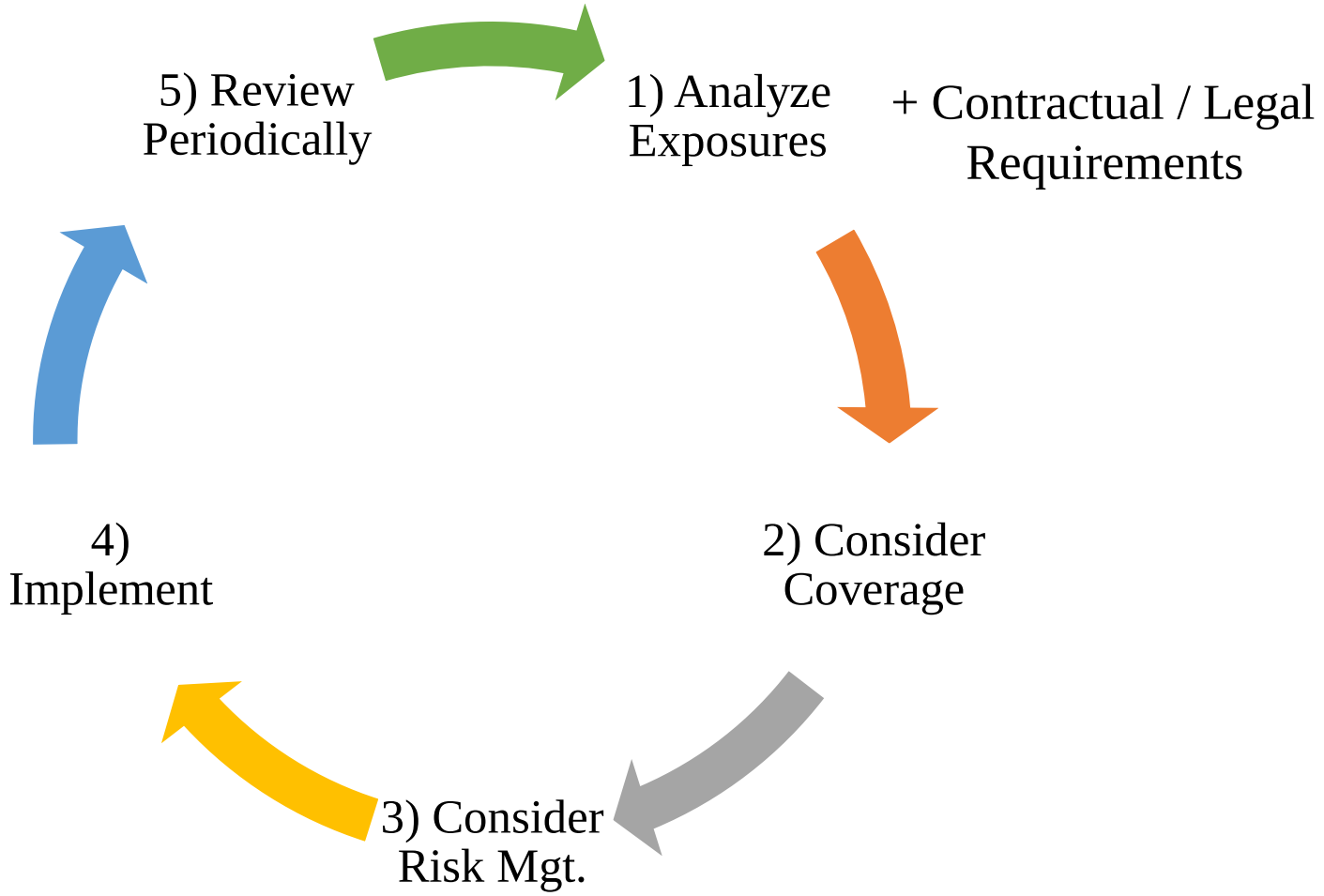
Building a Commercial Insurance Program for Massachusetts Tax School Practitioners



Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

This presentation is designed to offer basic insurance information for an accountant / tax preparing professional and to specifically raise awareness for Cyber exposures and Risk Management methods.

This presentation is not:

- Legal advice. An Attorney is required.
- Security or IT Advice. A Security and IT profession is required.
- Specific coverage advice. A review with an insurance broker much be done to provide accurate recommendations.

Insurance Provides:

Insurance can provide:

- Ability to Satisfy Contractual and Legal Requirements
- Defense Expenses
- Coverage for Judgements / Settlements
- Risk Management Tools
- Legal Hot Lines

TRADING A KNOWN LOSS (PREMIUM) for an UNKOWN LOSS

GOAL = Financial Survival

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Know The Rules of the Road

ROR

Rule 1: Insurance carriers are in business to make money, not pay claims.

Rule 2: After a loss, insurance carriers will always do the right thing…for themselves….make money.

Rule 3: To have coverage, the peril / coverage must be listed and show a premium charged for the coverage.

Rule 4: Other than the law or lender requirements for insurance, there is no right or wrong. It is a matter of risk tolerance.

Rule 5: Insurance is name and location specific. (VERY)

Rule 6: We are not in control, a jury is.

Rule 7: Pay attention to the correspondence and fine print.

Rule 8: An insurance program is only as good as the time & effort put into it…*Otherwise it is a guess*

Cost of Risk = Insurance Premiums, Risk Management Expenses AND Uncovered Losses

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Exposures (vs Policies)

- Employee Liability
- Auto Risk and Liability
- Cyber Risk and Liability
- Property Loss Risk
- Business Income Risk
- Bodily Injury and Property Liability
- Personal and Advertising Liability
- Errors or Omissions / Professional Liability
- Wrongful Management Liability
- Environmental Risk and Liability
- Contractual Requirements (Leases, Loans)

Often Losses Involve Multiple Loss Types

Example: Auto Accident

- Employee Injury
- Auto Physical Damage
- 3rd Party Bodily Injury
- 3rd Party Property Damage

Step 1

Often a Policy Covers Multiple Loss Types

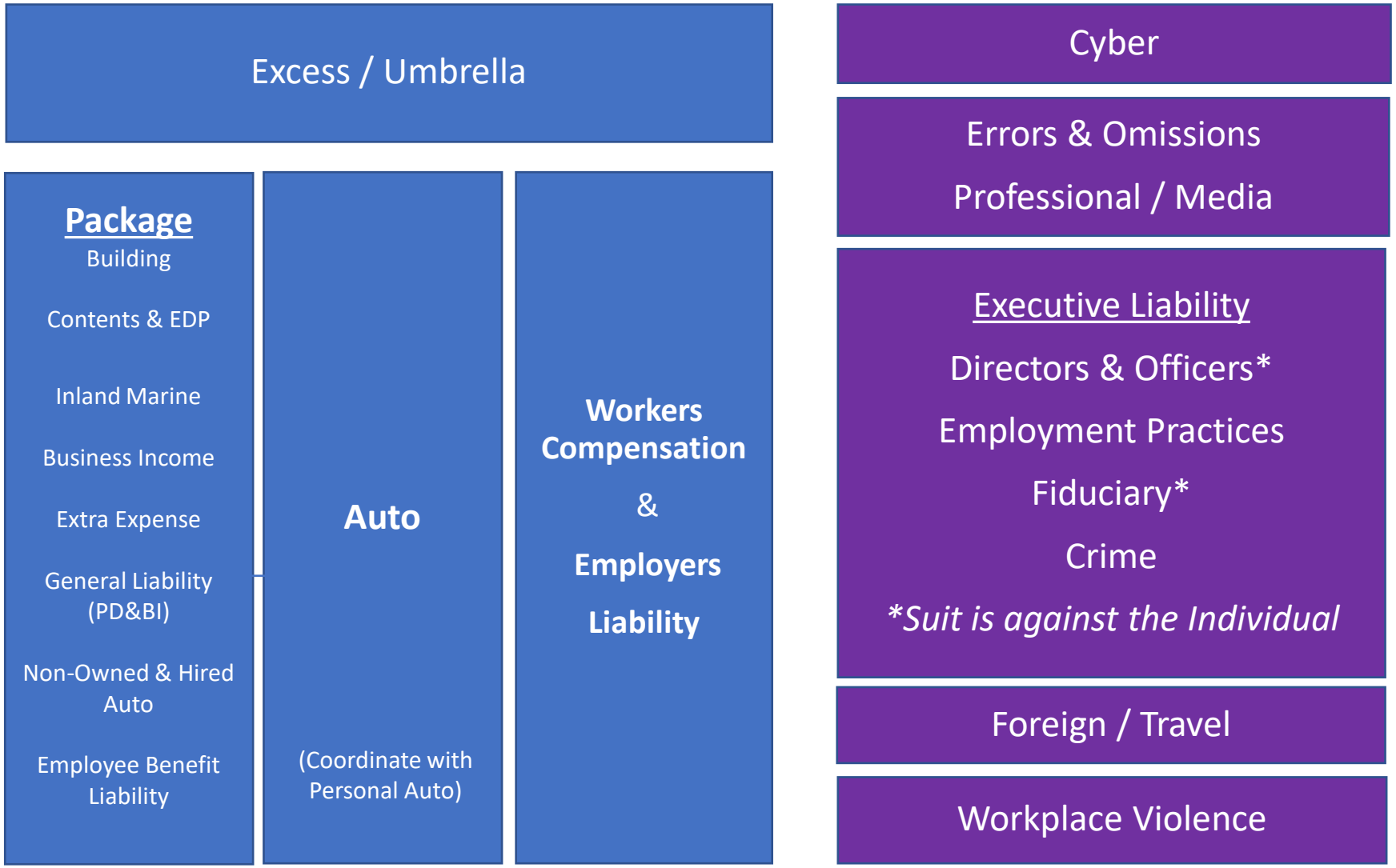
Example: Auto Policy

- Your Auto Physical Damage
- 3rd Party Bodily Injury Liability
- 3rd Party Property Damage Liability

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

Coverage Selection- Mature Company



Step 2

Group

Health

Dental

Life

Disability

Individual Life & Disability

Key Person

Succession

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

Coverage Selection- Today's Subject Matter

Step 2

Cyber

Occurrence

Outside<<<<<<<**Defense**>>>>>>>>Inside

Claims Made

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

Who is behind Cyber Issues?

- Hackers
- Angry Employees
- Angry Ex-Employees
- Criminals
- Activists
- Terrorist
- Governments

For this presentation all will be referred to as criminals.

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

What is Cyber?

Cyber, in short, is the mismanagement of data and personal information (PII) (Your and Others)) that leads to the loss of the data and PII which leads to damage to your firm's and your clients' financial well being.

It has many forms such as:

- **Data Breech**
- **Ransomware**
- **Denial of Service Attacks**
- **Fraudulent Funds Transfers**
- **Social Engineering or Cyber Deception**
- **Business Email Compromise Attacks**

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

Data Breech

Data Breech of information of others you store is stolen, and your firm is then asked to pay ransom to recapture information.

Data Breeches tend to make the news and often lead to class action litigation

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

Ransomware

Ransomware is “malware” that infects your computer and demands ransom of your firm to restore your systems and information.

Once a firm is subject of ransomware, they are often hit again.

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

Denial of Service Attacks

Denial of Service Attacks consists of your website being overrun with inquiries to the point it fails.

Once again, ransom demands are made.

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

Fraudulent Funds Transfers (FFT)

FFT is a criminal working through your system to move money from your account/s or redirect incoming or outgoing funds.

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

Social Engineering or Cyber Deception

Social Engineering or Cyber Deception

is a criminal tricking you into the sending funds to the wrong address / account.

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

Business Email Compromise Attacks

BEC Attacks consist of a criminal gaining control of your email and corresponding on your behalf without your knowledge. Through BEC, a criminal can trick another into acting based on your instructions.

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

What Is Cyber?

Step 2

SUMMARY

Through the myriad of methods, cyber criminals utilize your computing systems to

> Gain your personal information

> Gain Personal Information of Others

➢ Gain access to your funds as well as your clients

to monetize for their benefit resulting in financial harm to you and your clients.

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

Cyber Responsibility

Step 2

THE IRS is well aware of this and expects the following:

Safeguarding IRS e-file Safeguarding of IRS e-file from fraud and abuse **is the shared responsibility** of the IRS and **Authorized IRS e-file Providers.** Providers must be diligent in recognizing and preventing fraud and abuse in IRS e-file. Neither the IRS nor Providers benefit when fraud or allegations of abuse tarnish the integrity and reputation of IRS e-file. Providers must report fraud and abuse to the IRS as indicated in the "Where To Get Additional Information" section. Providers must also cooperate with IRS investigations by making available to the IRS, upon request, information and documents related to returns with potential fraud or abuse. Safeguarding taxpayer data is a top priority for the IRS. **It is the legal responsibility of government, businesses, organizations, and individuals that receive, maintain, share, transmit or store taxpayers' personal information.** Taxpayer data is defined as any information that is obtained or used in the preparation of a tax return (e.g., income statements, notes taken in a meeting, or recorded conversations). Putting safeguards in place to protect taxpayer information helps prevent fraud and identity theft and enhances customer confidence and trust. **Protecting taxpayer data is required by law.**

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-MFA

Step 3

Use of Multi Factor Authentication

Use of Verbal Verification Systems

Off Site Back Up Systems and On Site Back Up Systems

Use of Password Managers

Constant Software Updates and Patching

WISP (Required by law in all states)

RECOVERY PLAN

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Preventing Cyber Loss-Methods

Step 3

Use of Multi Factor Authentication

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-Verbal Verification

Step 3

Use of Verbal Verification Systems

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-Back Up

Step 3

Off Site Back Up Systems and On Site Back Up Systems

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Preventing Cyber Loss-Password Managers

Step 3

Use of Password Managers

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-Updates / Patching

Step 3

Constant Software Updates and Patching

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-WISP

Step 3

WISP

An Information Security Plan (the "Plan") is intended to create effective administrative, technical and physical safeguards for the protection of personal information of employees who are residents of the Commonwealth of Massachusetts. The Plan sets forth the Organization's procedure for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting personal information of residents of the Commonwealth of Massachusetts.

- Assign Data Security Coordinator
- Identify Internal Risks to Personal Information and how information is protected
- Identify External Risks to Personal Information and how information is protected
- Explain what will be done if a breech occurs

GET PROFESSIONAL HELP

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Preventing Cyber Loss-RECOVERY PLAN

Step 3

A Disaster Recovery plan is a critical document for the survival of an organization once it has been attacked. It should contain:

- List of all hardware and software and structure of your IT systems
- Recovery time deadlines
- Copies of agreements with all service providers-who is responsible for what?
- Establish a disaster recovery site
- Establish Personnel Roles
- Provide a Communication plan
- List step by step instructions for the recovery

GET PROFESSIONAL HELP

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-Cyber Insurance

Step 3

- Liability associated with loss of others personal information (3rd Party)
  - Defense
  - Settlements
  - Legal Costs (Working with the Local, State and Federal governments)
  - Travel
- Costs associated with (1st Party)
  - Legal Costs
  - Forensic Work
  - Extortion
  - Business Income Loss
  - PCI DSS Assessments (Credit Card Penalties)
  - Restoration Costs
- Media Liability (Slander/Libel, Copyright, Trademark, False Light, Failure to maintain confidentiality)
- Fraud via:
  - Phishing, Funds Transfer, BEC Attacks Cyber Deception / Social Engineering
- Good To Know
  - All Cyber policies are different.

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-Suggestion

Step 3

- Practice using the recovery plan and audit to keep up to date.

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-Suggestion

Step 3

- Remove your Cyber Insurance Policy, WISP and Recovery plan from your computers. These three documents give criminal your plan book.

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Preventing Cyber Loss-Suggestion

Step 3

- Along with a Cyber insurance policy, also maintain a Crime policy to cover loss from employees stealing for you and your clients via forgery and alteration.

Goals of Risk Management

1) Reduce odds of a loss occurring.
2) Reduce size of a loss once it occurs.

Results: Lower premiums over the long run.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Christopher F. Hawthorne, CPCU, CIC / chawthorne@Clearyinsurance.com / 617-305-0303

Implement

Step 4

- Gather Information / Complete Applications
- Evaluate Quotations
- Answer Final Questions
- Bind Coverage
- Set Follow Up dates
- Take advantage of carrier services
  - Training
  - Risk Management Tools

TERMS TO KNOW

Liability Defense: Inside or Out?

TTK 1

- INSIDE-Every dollar spent defending erodes the limit of liability coverage left to settle. Example: $1,000,000 limit - $400,000 spent defending = $600,000 left to settle.

- OUTSIDE-Defense costs are unlimited and in addition to the limit of liability. Example: $1,000,000 limit - $400,000 spent defending = $1,400,000 spent by carrier.

Therefore a $1,000,000 limit of liability can be quite different in protection.

Example of Possible Outside Defense Policies: Professional, Employment Practices, Directors & Officers, Cyber.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

TERMS TO KNOW

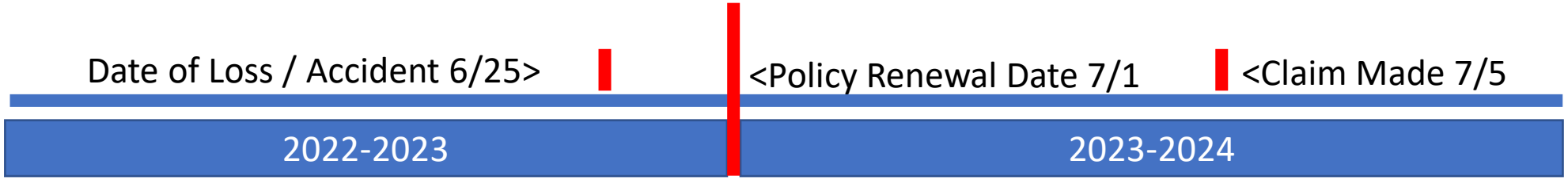
TTK 2

Occurrence Form vs Claims Made (Retro Dates)

Occurrence Form – Policy in force when loss occurs, pays claim.

Example: Employee injured on June 25. WC Policy Renewal Date is July 1. Claim made on July 5. Policy in force on June 25 pays the claim.

Examples of Occurrence Form Policies: General Liability, Auto, WC, Crime



2023 – 2024 Policy will cover the loss / accident occurring in prior policy period.

TERMS TO KNOW

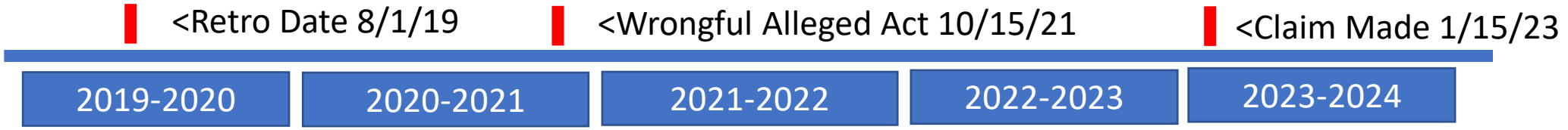
Occurrence Form vs Claims Made (Retro Dates)

TTK 2

Claims Made – Policy in force when the claim is made pays the loss as long as the alleged wrongful act occurred after the Retro Date.

Examples of Claims Made policies: Professional, Employment Practices, Directors & Officers, Cyber.

RETRO DATE EXAMPLE



2023 – 2024 Policy will cover the alleged wrongful act committed in 2021

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

TERMS TO KNOW

TTK 3

Minimum Earned Premium

Minimum earned premium represents the amount a carrier will keep if the policy is cancelled before policy renewal date.

Example: MEP 25% om a $10,000 Premium. If policy canceled on day 2, carrier will return $7,500.

Wrongful Act Definition/s

Policies define what carrier considers a wrongful act therefore a covered act. Policies with multiple coverages may have multiple wrongful act definitions.

Example: A Non-Profit D&O Liability policy and Outside Directorship. Some carriers will cover, some won't.

Who is an Insured Definition/s

Policies state who is an insured for wrongful acts on behalf of the organization.

Example: Sub-Contractors, Temporary Staff, Day Labor may be an insured or may not be an insured.

Extended Reporting Period (aka Tail Coverage)

When an organization terminates a Claims Made policy, a claim may come in after the cancellation. ERPs can be purchased to handle these claims.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303

TERMS TO KNOW

TTK 4

Risk Transfer

Organizations can reduce the size of a loss when working with another organization such as a contractor by implementing Risk Transfer Techniques. The following are examples of risk transfer.

- Required Insurance Limits- Organization tells other party what limits of coverage are required.
- Hold Harmless- Other Party agrees holds Organization harmless for a loss when Other Party has caused part or all of a loss.
- Indemnify - Other Party agrees to reimburse Organization for damages (settlements and judgments).
- Defend - Other Party agrees to pay the cost to defend Organization after a loss if Organization is named in a claim or suit.
- Additional Insured Status - Other Party provides coverage for Organization under Other Party General Liability. Additional Insured status can be provided for Other Party's Operations or for Operations and Completed Operations as well.
- Primary Coverage - Other Party states that its coverage is primary should Organization be brought into the suit.
- Non-Contributory - Other Party states its policy disallows Organization's policy from sharing in the loss.
- Waiver of Subrogation - Other Party disallows its insurance company from pursuing Organizations insurance carrier for any amount due to Organization negligence that may have contributed to the loss.
- Per Project Aggregate - Other Party liability insurance provides a new set of limits for each project in which Other Party is involved. This allows Organization to rely on a full set of limits for their project.

When implementing risk transfer agreement, an attorney should be involved.

Christopher F. Hawthorne, CPCU / chawthorne@Clearyinsurance.com / 617-305-0303