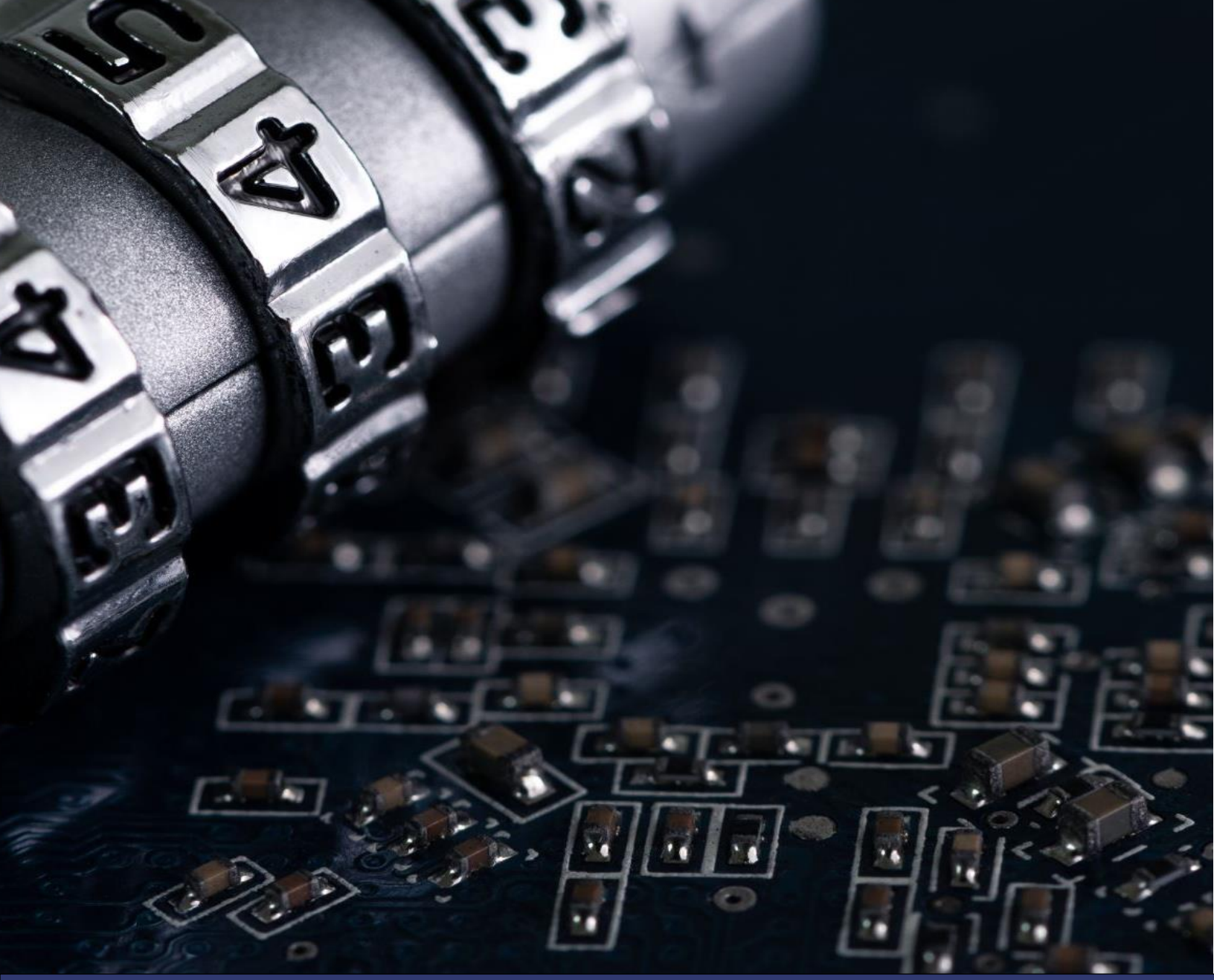


AN AGENT'S GUIDE TO UNDERSTANDING & MITIGATING CYBER EXPOSURES

Special Topic CPIA Seminar

CPIA Designation Program
PO Box 35718
Richmond, VA 23235
877-674-CPIA (2742)
www.cpia.com

NOTICE

These materials are provided solely for educational purposes. Actual policy wording, as well as applicable laws, regulations, forms, and manuals control specific practices in each jurisdiction.

TABLE OF CONTENTS

SECTION 1: INTRODUCTION TO CYBER TERMS AND CLAIMS EXAMPLES

During this section we will:

- Introduce common cyber risk exposures faced by organizations
- Identify terms used in cyber insurance
- Examine a phishing attack event

INTRODUCTION

Keys to Consider

- **Exposure defined:** A situation, practice or condition that may lead to an adverse financial consequence or loss; an activity or resource; people or assets
- **All commercial insurance clients** who use the internet have Cyber Risk Exposures and need insurance professionals to help them manage their risks
- **Definitions** used by insurance companies and loss control cyber service providers may be used to identify cyber threats to the organization
- **Types of cyber-attacks** come both externally and internally to the organization

HOW MANY EMAILS DO YOU RECEIVE EACH DAY?

HOW DO YOU VERIFY THE SENDER?

TERMS YOU SHOULD KNOW

Phishing	Malicious user poses as a trustworthy source (e.g. your bank) and sends you an email that creates a false emergency and requests that you click a link. The link takes you to a website where you are prompted to enter sensitive information
Vishing	A phishing attack conducted by telephone. These attacks may use a fake Caller ID profile to impersonate a legitimate business, government agency or charitable organization. The purpose of the call is to steal personal information, such as a bank account or credit card numbers
Spear phishing (whaling)	A phishing attempt that targets a specific group or individuals. Victims may be targeted because they are more vulnerable or high-profile, such as a CEO or CFO
Baiting	The attacker leaves a malware-infested physical device, such as a USB flash drive, in a place where it is sure to be found
Pretesting	One party lies to another to gain access to privileged information (e.g. attacker pretends to need personal information or financial data to confirm the identity of the recipient)
Scareware	Tricking the victim into thinking his/her computer is infested with malware or has inadvertently downloaded illegal content. The attacker then offers a solution to repair and then the victim is tricked into downloading the attacker's malware
Drive-By Download	Websites are able to upload malicious software to computers without anyone clicking on anything. Simply visiting the website initiates the attack. Drive-by downloads are often combined with phishing emails

MORE TERMS YOU SHOULD KNOW

Malware	Broad term to describe malicious software that can damage the computer and gain access to sensitive data which would include: **Adware:** a form of malware that is bundled with free or pirated versions of software and is designed to launch advertisements or pop-ups when the computer is using a web browser **Spyware:** designed to spy on the user's activities and monitor things such as keystrokes and websites visited in order to steal passwords and can also change the computer's security settings **Trojan horses:** appear as normal files but once downloaded, they give a malicious user access to the computer and information
Point-Of-Sale Hacking	Involves a hacker remotely scraping the credit card information stored on a point-of-sale device
Crypto jacking	A kind of cyber-attack that issues a target's computing power to conduct unauthorized transactions involving cryptocurrencies
Bricking	Refers to hacking that essentially paralyzes a device and renders it inert and unusable, like a brick
Virus	A man-made program or piece of code that causes an unexpected, usually negative event. Viruses are often disguised as games or images with clever marketing titles, such as "Me, nude"
Keylogger	Hardware or software that captures individual keystrokes on a keyboard. Criminals uses keylogging to collect usernames and passwords
Botnet	An interconnected network of computers infected with malware without the user's knowledge and controlled by cyber criminals. They are typically used to send spam emails, transmit viruses and engage in other cybercrime. Aka "a zombie army", botnets are considered one of the biggest online threats

KNOWLEDGE CHECK:
List two sources of cyber- attacks on an organization:

1. _____

2. _____

IMPORTANT!

Employee Training, Cyber Security Policies, and Active Loss Control

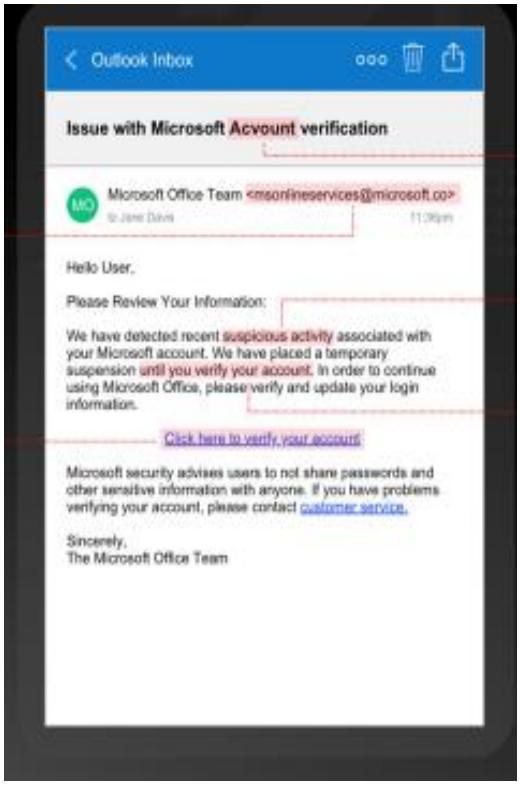
Employees are the first line of defense

Policies and Procedures augment technology solutions

Build Awareness of Red Flags

SAMPLE PHISHING ATTEMPT

- Things to notice:
  - Spelling and grammar mistakes
  - Incorrect / suspicious looking From: Email Address
  - Links appear normal but hovering over reveals suspicious web address



KNOWLEDGE CHECK:

Why is employee training necessary for every employee?

CYBER TERMS QUIZ

Circle the correct response to each question.

1. **Phishing attacks are uncommon and are not considered a real threat.**

   True False

2. **Threats to an organization come from both inside and outside the organization.**

   True False

3. **Bricking enables the computer to process information faster.**

   True False

4. **Keyloggers installed on network computers allow the hacker to collect username and passwords.**

   True False

5. **A Cyber Security Policy is not important to an organization.**

   True False

6. **All cyber terms are defined in Cyber Insurance policies**.

   True False

7. **Cyber insurance is only needed by companies that provide IT services.**

   True False

8. **An understanding of cyber terminology will assist the insurance professional matching coverage with cyber risks faced by an organization.**

   True False

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

-Bruce Schneier, American cryptographer, computer security professional, privacy specialist, and writer

SECTION SUMMARY

In this section you reviewed cyber terms used by insurance carriers and loss control service providers. You identified external and internal sources of cyber-attacks. Finally, you reviewed a sample phishing attempt to build awareness of potentially suspicious email components.

SECTION 2: THE INTERNET OF THINGS (IOT) AND INSURTECH

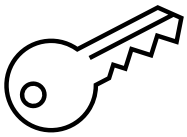
During this section you will:

- Gain understanding of the Internet of Things (IoT)
- Address security issues and causes of concern arising from IoT devices
- Understand the term Insurtech and uses in insurance sales, underwriting, and claims processing

THE INTERNET OF THINGS

IoT Defined:

The ever-growing network of physical objects that feature an IP address for internet connectivity.



Key Concepts Insurance Professionals must understand:

- "Smart Devices"
- Network connectivity
- Privacy issues
- Criminal activity

KNOWLEDGE CHECK:
List two IoT devices used by organizations today that could lead to a security breach:

1. _____
2. _____

INSURTECH

Insurtech Defined:

Insurtech refers to the use of technology innovations designed to find cost savings and efficiency from the current insurance industry model. Insurtech is a combination of the word's "insurance" and "technology".

Understanding the language of Insurtech:

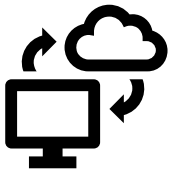
AMS	Agency Management System used to organize the agency's book of business
API	Application Programming Interface. APIs allow software to talk to each other
Back-End	The part of a software solution that users cannot see or interact with
Cloud Computing	Uses online servers to access data
CRM	Customer Relationship Management software that organizes a company's client interactions
Cyber Security	Refers to the steps an organization takes to keep company and client data safe
Front End	The part of the software users interacts with
SaaS	Software as a Service. A method of licensing software instead of purchasing the software, a software license is purchased and then accessed via the internet.
SOC 2	This is the gold standard for Cyber Security. A third-party evaluation is conducted of an organization to ensure that the company adheres to the highest security standards

INSURTECH & INSURANCE SALES

Consider various insurance AGENCY technology tools used in insurance sales and service:

- Agency Management Systems

- Upload/download with insurers



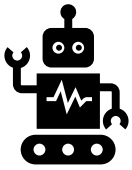
- Quoting for new and renewal policies
- Marketing to new prospects

- Other tools

KNOWLEDGE CHECK:
How has your AMS allowed you to be more productive? List three examples:

1. _____
2. _____
3. _____

INSURTECH: UNDERWRITING & CLAIMS PROCESSING




Consider various artificial intelligence / Insurtech solutions used by insurance COMPANIES for Underwriting:

- Customer identity verification
- Fraud detection
- Payment processing
- Telematics
- Drones

Consider various artificial intelligence / Insurtech solutions used by insurance COMPANIES for Claims Processing:

- Data Storage
- Blockchain
- Settlement

Other Insurtech trends in underwriting and claims processing?

THE IOT AND INSURTECH QUIZ

1. **The Internet of Things (IoT) requires humans to type on the computer in order to connect to another smart device.**

   True False

2. **IoT Security issues and causes of concern for cyber threats include both privacy issues and criminal activities associated with use.**

   True False

3. **In censorship and unfair competition cases, plaintiffs brought claims against internet companies arising out of their search results. The plaintiffs won their case.**

   True False

4. **Back-End is the part of the software that users cannot see or interact with.**

   True False

5. **Cyber Security refers to the steps the cyber criminals use to access computer networks.**

   True False

6. **Insurance companies use AI and IT devices to detect underwriting fraud.**

   True False

7. **List two other uses of AI and IT by insurance companies for underwriting:**

   1. _____ 2. _____

8. **Use of Insurtech has allowed companies to process claims faster.**

   True False

> ***If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you.***
>
> -Stephane Nappo, 2018 Global CISO of the Year

SECTION SUMMARY

In this section you reviewed how the Internet of Things (IoT) and use of smart devices in business today are cause for concern of a security breach. You reviewed several claims examples and related litigation. Finally, you reviewed the concept of Insurtech, the language of Insurtech, and Insurtech uses in insurance sales, underwriting and claims processing.

SECTION 3: IDENTIFICATION TECHNIQUES FOR CYBER LOSS EXPOSURES

During this section you will:

- Use the following to identify cyber exposures of an organization:
  - Checklists
  - Websites
  - Data security compliance review
  - Current insurance policy review
  - Contract review

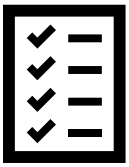
- Review Risk Management Services offered by insurers including:
  - Active Avoidance
  - Pre-breach planning
  - Help line
  - Information portal
  - Others

IDENTIFYING CYBER EXPOSURES

Using Checklists

Use checklists to identify and analyze cyber risk to the organization:

- Available from the insurance company/MGA
- Purchased from vendors
- Created in-house



PROS and CONS of USING CHECKLISTS

BENEFITS	LIMITATIONS
○ Standardized and relevant for most organizations ○ Focus on cyber exposures and hazards ○ Anyone in the organization with access to the information can complete the checklist ○ Useful in gaining management's "buy-in" for the need of cyber insurance and loss control	○ Need to update regularly ○ May miss exposures and hazards if not on the list ○ May have limited benefit in the analysis of the exposures ○ Time consuming

RESOURCES FOR CLAIMS EXAMPLES:

www.renolon.com/data-loss-statistics

www.idtheftcenter.org

www.cyberscout.com

www.netdiligence.com

IDENTIFYING CYBER EXPOSURES

Data Security Compliance Review

Insurance Professionals must be aware of and understand:

- Regulatory requirements for data security in laws of countries and states
- All 50 states, DC, USVI, and Guam have mandatory requirement for breach notification
- Many states / jurisdictions include data disposal laws
- NAIC Data Security Model Act #668
- Federal and international statutes, including:

HIPAA – *Health Insurance Portability and Accountability Act*	Provides protection for health-related information against hacking or accidental release to unauthorized persons. HIPAA regulations protect all health-related information about a person from past, present and future medical conditions, payment information, medications, procedures, etc. Significant fines can be levied against healthcare organizations violating the HIPAA regulations.
HITECH – *Health Insurance Technology for Economic and Clinical Health*	Expanded the use of electronic health records (EHRs) in the U.S. The law expands HIPAA requirements to business associates of healthcare providers (i.e. billing, scheduling, marketing and IT services). HITECH strengthened HIPAA's regulations by expanding the number of companies it covers and punishing violations more severely.
GLBA – *Gramm-Leach-Bliley Act*	Requires financial institutions to explain their information sharing practices and how they safeguard sensitive information.
FERPA – *Family Educational Rights and Privacy Act*	Provides protection for student education records. FERPA gives parents certain rights prior to the student reaching 18 years of age. The student obtains additional rights once they turn 18 years old.
GDPR – *General Data Protection Regulation*	A European Union (EU) regulation providing data protections for citizens of EU countries. Included are US companies that do business in the EU. The regulations are strict and give the individual citizen control over data collection, use and disposal.

ESSENTIAL ELEMENTS OF A DATA SECURITY POLICY

1. Data privacy
2. Password management
3. Internet usage
4. Email usage
5. Company owned devices
6. Employee-owned mobile devices
7. Social media
8. Software copyright and licensing
9. Security incident reporting

RESOURCES:

Most cyber liability insurance companies offer pre-breach plans and sample data security policies as part of their risk management services. Be sure to ASK!

POLICY & CONTRACT REVIEW

- Conduct a Review of current insurance policies to find gaps filled by cyber insurance. Specific considerations include:
  - ➢ Definition of covered property in property insurance
  - ➢ Definition of property damage in liability coverage
  - ➢ Specific exclusions for cyber-related claims
    - Exclusions found in policy forms
    - Endorsements adding exclusions/limitations

- Conduct a Contract Review to determine contractual obligations, include:
  - ➢ Payment Card Industry (PCI) compliance
  - ➢ Service contracts
  - ➢ Others

PROS and CONS of conducting a Policy and Contract Review

BENEFITS	LIMITATIONS
○ Helps identify gaps in coverage ○ May identify external sources of risk funding	○ Limited ability to change the contract ○ Legal experts may be necessary

KEYS TO REMEMBER:

- Before we **insure** your data, it is important to **secure** your data
- Insurers, Insureds, Agents, Brokers, and Risk Managers need to work together to address the exposures faced by an organization
- Understand the firm's reliance on technology
- Identify the technology risks of the firm

IDENTIFICATION TECHNIQUES FOR CYBER LOSS EXPOSURES

KNOWLEDGE CHECK:
List three methods insurance professionals can use to identify an organization's cyber exposures and hazards:

1. _____
2. _____
3. _____

UNDERWRITING STARTS WITH THE APPLICATION PROCESS

It's important to understand that cyber policies are typically not standardized across insurers. Use Risk Management Services offered by insurers.

Examples:

- Active Avoidance
- Pre-breach planning
- Help line
- Information portal
- Other Services

UNDERSTANDING CYBER POLICY BASICS

Cyber insurance coverage is not standardized, and the terms used have different definitions. It's important to read and review every policy!

- Claims made policy forms
- Components of a Typical Cyber Policy
    - Declarations page
        - Coverages
        - Limits
        - Sub limits
        - Aggregates
        - Deductibles/Retentions
    - Common exclusions applicable to all coverages
        - War
        - Interruptions
        - Pollution
        - Securities / Management Liability
        - Claims by Government Agency
        - ERISA and similar acts
        - Bodily Injury and Property Damage Liability
        - Contractual Liability
        - Advertising Liability
        - Dishonest, fraudulent, criminal or malicious act, error or omission, or any intentional or knowing violation of the law by an insured
        - Unprotected portable computers and media
        - Costs associated with upgrading or improving the insured's computer system
        - RICO
        - Malfunction or failure of any satellite
        - Inadequate software
        - Oral or written material if known to be false by an insured
        - Failure to follow minimum required practices

IDENTIFICATION TECHNIQUES FOR CYBER LOSS EXPOSURES QUIZ

1. **Checklists are rarely used to identify cyber exposures; they have no value.**

   True False

2. **Many websites are available for claims examples.**

   True False

3. **All 50 states, DC, USVI and Guam have mandatory requirement for data breach notification.**

   True False

4. **Federal and international statutes do not apply in most states.**

   True False

5. **It is not important to secure data prior to purchasing cyber insurance.**

   True False

6. **Pre-breach planning or an operational assessment may be offered by the insurance company as part of the underwriting process.**

   True False

7. **Most cyber polies are on a claim's made basis.**

   True False

8. **All cyber policies have the same exclusions and limits.**

   True False

A data breach is about both privacy and security. And security becomes very, very important because you can't have privacy unless you have good security. And if someone tries to say otherwise, they are crazy people!

- Dr. Larry Ponemon, Founder and Chairman of the Ponemon Institute

SECTION SUMMARY

In this section you reviewed identification techniques using cyber checklists, websites for claims examples, data security compliance reviews, and current insurance policy and contract reviews.

This section concluded with information regarding risk management services that many insurers provide as bundled services to their customers as well as part of the initial underwriting process.

SECTION 4: INSURANCE COVERAGE, LIMITS, AND EXCLUSIONS FOR FIRST PARTY/POST BREACH RESPONSE

During this section you will:

Review the concepts of First Party Coverage and Post Breach Response

- Analyze coverage, limits, and exclusions for Privacy Notification Cost/Expense
- Analyze coverage, limits, and exclusions for Crisis Management Expense Coverage
- Analyze coverage, limits, and exclusions for Forensic Expense Coverage
- Review typical cyber expenses

PRIVACY NOTIFICATION
COST / EXPENSE COVERAGE

CONSIDERATIONS:

- Coverage trigger – Computer breach
- Coverage for:
  - Costs of external IT to verify breach
  - Costs of legal firm to determine actions necessary to comply with privacy regulations
  - Notification costs and related expenses
- May have sublimit and deductible
- Exclusions
  - Nuclear
  - War and terrorism – *Sample on the next page*
  - Failure of the insured to maintain security standards
  - Contractual
  - Dishonest, fraudulent, criminal, or malicious act, error or omission, or any intentional or knowing violation of the law by an insured

SAMPLE POLICY LANGUAGE:

c. Notification costs and related expenses to notify
   i. Individuals who are required to be notified in compliance with **Privacy Regulations** mandating notifications; or
   ii. Any individual affected by the actual or suspected cyber event or to send email notices or issue substitute notices;
   iii. Costs of setting up a telephone call center in order to support notified individuals and to provide credit file monitoring services and/or identity theft assistance.

EXCLUSION CAUTION!

Read "war" exclusions carefully!

" A. EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS This Policy does not cover Loss, Breach Consultation, Breach Response, Public Relations Costs, Data Forensics, PCI Expenses, Network Extortion Expenses, Social Engineering Fraud Loss, Telecommunications Fraud Loss, Funds Transfer Fraud Loss, Digital Assets Restoration Costs, Business Interruption Costs, or Cyber Expenses: 3. alleging, arising out of, or based upon war, invasion, acts of foreign enemies, nations, groups or natural persons, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power; provided, however, that this Exclusion shall not apply to Cyberterrorism."

"In consideration of the premium charged for the Policy, it is hereby understood and agreed that EXCLUSIONS is amended to include: War and Civil War For, resulting from, directly or indirectly occasioned by, happening through or in consequence of: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority; provided, that this exclusion will not apply to Cyber Terrorism. For purposes of this exclusion, "Cyber Terrorism" means the premeditated use of disruptive activities, or threat to use disruptive activities, against a computer system or network with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives."

KNOWLEDGE CHECK:
List three costs that Post Breach Response Coverage may pay:

1. _____
2. _____
3. _____

CRISIS MANAGEMENT EXPENSE COVERAGE

Triggers for Coverage

Unauthorized access

Introduction of a malicious code

Accidental or unauthorized release of private information

Denial of service attack(s)

Types of Expenses Paid

Investigative/forensic expenses

Mitigation expenses

Cost of advertisements

Notification expenses

Credit monitoring services

Cost of public relations consultant

SAMPLE POLICY LANGUAGE:

Public relations expenses means:

a. Fees and costs of a public relations firm; and
b. Any other reasonable expenses incurred by you with our written consent, to protect or restore your reputation solely in response to “negative publicity”.

CAUTIONS:

“with our written consent”
May be subject to a maximum time limit
May have a sublimit or deductible / retention

KNOWLEDGE CHECK:
Why is Crisis Management coverage important to your clients?

FORENSIC EXPENSE COVERAGE

aka Emergency Response Fund

Sample policy language:

Emergency Response Fund
for the **Insured Entity's** reasonable and actual expenses resulting from an **Exploit**, **an Electronic Theft** or a **Network Extortion** that occurs during the **Policy Period** in engaging a suitably qualified third-party security expert to:
1. assist the Insured in investigating, stopping, or minimizing damage due to such **Exploit**, **Electronic Theft** or **Network Extortion** while such **Exploi**t, **Electronic Theft** or **Network Extortion** is ongoing, or:
2. collecting and analyzing and preserving forensic evidence of such **Exploit**, **Electronic Theft** or **Network Extortion** for use in identifying the perpetrator and in supporting legal action against the perpetrator.

Things to Know:

- May be included in other first party coverage expenses
- Triggers of coverage are similar to other coverage triggers
- Coverage pays reasonable expenses with company pre-approval

Typical Cyber Expenses

- Cyber-crime attorney: $700/hour
- Investigation/Computer Forensics Fees: $300-$700 per hour
- Notification cost: mail notice letter to customers as much as $14/customer
- Credit monitoring $10-$12/year per person
- Public Relations Firm: $10,000/month or $400/hour

Source: Mark Greisinger, President of NetDiligence, a leading Cybersecurity assurance company www.NetDiligence.com

CYBER INSURANCE FOR FIRST PARTY/POST BREACH RESPONSE QUIZ

1. **First party breach is not necessary because cyber insurance includes all first party expenses in the cyber privacy liability coverage.**

   True False

2. **War exclusions are not important in cyber first party coverage.**

   True False

3. **The coverage trigger for Privacy Notification Cost/Expense Coverage is a computer breach.**

   True False

4. **Crisis Management Expense Coverage usually pays for credit mitigation expenses and the cost of a cyber public relations consultant.**

   True False

5. **Crisis Management Expense Coverage is not subject to a time limit.**

   True False

6. **Forensic Expense Coverage may be available for expenses relating to other first party coverages (i.e. electronic theft or network extortion).**

   True False

7. **Cyber-crime attorney's average cost is $700 per hour.**

   True False

8. **Public Relations firms can cost $10,000 per month or more.**

   True False

SAMPLE CLAIM – IS THERE COVERAGE?

ABC, Inc. has a Cyber Insurance Policy with the following:

Policy Aggregate	$1,000,000 Policy Limit
Privacy Notification Cost	$ 300,000
Retention	$ 2,500
Crises Management	$ 300,000
Retention	$ 2,500
Maximum days 20	

During the policy period, the insured called to report the following:

"Our network has been hacked and all of our 1,000 client records have been compromised. Does our Cyber Policy cover this and what should we do next?"

How do you respond?

Security in IT is like locking your house or car – it doesn't stop the bad guys, but if it's good enough they may move on to an easier target.

-Paul Herbka, CISSP, cybersecurity executive

SECTION SUMMARY

In this section you reviewed coverage for first party post breach response that may be available on cyber insurance policies. You looked at examples for Privacy Notification Cost/Expense coverage, Crisis Management Expense coverage, and Forensic Expense coverage. You reviewed typical cyber expenses (costs) associated with a cyber event. Finally, you reviewed a sample claim involving a cyber breach that required notification of those potentially compromised.

SECTION 5: INSURANCE COVERAGE, LIMITS, DEFENSE, AND EXCLUSIONS FOR THIRD PARTY LIABILITY

During this section you will:

- Evaluate coverage for Information (Network) Security and Privacy Liability
- Evaluate coverage for Payment Card Industry Fines and Assessments
- Evaluate coverage for Website Media Content Liability (aka Website Publishing Liability)
- Evaluate coverage for Contingent Bodily Injury and Property Damage Liability
- Evaluate coverages to include coverage triggers, aggregate and sub limits, defense provisions, and exclusions

INFORMATION (NETWORK) SECURITY AND PRIVACY LIABILITY

Sample Policy Language:

Network Security Liability

The **insurer** will pay **Damages** and **Claims Expenses** by reason of a **Claim** first made against the **Insured** during the **Policy Period** and reported to the **Insurer** pursuant to Section VIII. Notice, for any **Wrongful Acts** taking place after the **Retroactive Date** and prior to the end of the **Policy Period**.

Network Security and Privacy Liability

Damages and **Defense Expenses** which the **Insured** is legally obligated to pay as a result of a **Claim** arising from a **Security Breach** or **Privacy Breach**.

Coverage triggers

- Unauthorized access or use
- Computer virus
- Denial of service attack
- Denial of access
- Mistake in administration of network

Coverage for legal liability for loss of data

- Contingent on a written demand for monetary damages or injunctive relief, a regulatory action, written request to participate in an alternative dispute resolution proceeding, or a criminal proceeding

INFORMATION (NETWORK) SECURITY AND PRIVACY LIABILITY

(continued)

Defense provisions

Limit – Annual Aggregate

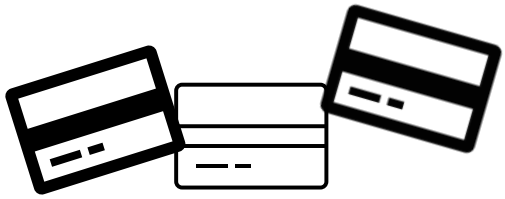
Exclusions

- Intentional Acts
- Utility or infrastructure failure
- Unencrypted information
- Wrongful collection
- War

KNOWLEDGE CHECK:

How are defense costs for Privacy Liability Coverage provided?

PAYMENT CARD INDUSTRY FINES AND ASSESSMENTS



Sample policy language:

> **PCI DSS Assessment Expenses**
>
> **PCI DSS Assessment Expenses** and **Defense Expenses** which the **Insured** is legally obligated to pay as a result of a **Claim** arising from **Security Breach** or **Privacy Breach**.

THINGS TO KNOW:

Coverage trigger – data breach, security breach

Coverage for contractual liability – written agreement required

Usually has a sublimit – especially if insured cannot prove compliance

Deductible/Retention applies

Exclusions

- Increased transactions costs
- Interchange fees
- Chargebacks
- Subsequent assessments, fines and penalties imposed due to continued PCI non-compliance
- Any portion of such amount reimbursed by a third party (i.e. financial institution)

Defense - Is defense provided?

WEBSITE MEDIA CONTENT LIABILITY

(aka Website Publishing Liability)

SAMPLE POLICY LANGUAGE:

Content Injury means:
A. publication or an utterance in violation of an individual's right of publicity, including commercial appropriation of name, persona or likeness;
B. any form of defamation or other tort related to an utterance or publication which disparages or harms the character, reputation or feelings of any person or organization, including libel, slander, product disparagement, trade libel, negligent or intentional infliction of emotional distress, outrage or outrageous conduct;
C. infringement of copyright, title, slogan, logo, trademark, trade dress, service mark, or service name; or
D. unfair competition or unfair trade practices based solely upon the same facts as, and alleged in conjunction with, subparagraph C. above, including but not limited to dilution, confusion, deceptive or unfair trade practices, civil actions for consumer fraud, false, disruptive or misleading **advertising** or misrepresentation in **advertising**.

THINGS TO CONSIDER:

- Must content be electronic?
- What is the Defense provision?
- Sublimit and Deductible / Retention

BE AWARE OF ENDORSEMENTS:

Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability Exclusion CG 21 06 – mandatory endorsement (ISO)

- Excludes loss from access or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information;
- Excludes loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate

Amendment Of Personal And Advertising Injury Liability CG 24 13

- Oral or written publication, in any manner, of material that violates a person's right of privacy is removed as a covered offense.

WEBSITE MEDIA CONTENT LIABILITY

(continued)

POTENTIAL EXCLUSIONS:

- Chat Rooms
- Blogs
- SPAM
- Unlawful collection of data
- Discrimination
- Patent infringement
- False Advertising
- Insider ownership disputes
- Licensing fees

KNOWLEDGE CHECK:

Which clients need coverage for Payment Card Industry Fines and Assessments?

Why is Information (Network) Security and Privacy Liability coverage needed?

CONTINGENT BODILY INJURY AND PROPERTY DAMAGE LIABILITY

Things to Know:

- Coverage trigger – security failure from external data breach
- Defense included in the limit
- Sublimit and Deductible/Retention

SAMPLE CLAIM – IS THERE COVERAGE?

ABC, Inc. has a Cyber Insurance Policy with the following:

Policy Aggregate	$1,000,000 Policy Limit
Privacy Liability	$ 300,000
Retention	$ 1,000
PCI Fines and Assessments	$ 300,000
Retention	$ 2,500

During the policy period, the insured called to report the following:

"Our network was hacked and now we have been receiving calls from our customers that their credit cards have been fraudulently used at several locations. We called the credit card company, and they won't help us! We received an email from the credit card company that says we aren't compliant, and they are terminating our contract. The credit card company will not reinstate our contract until we can prove compliance and sent us a bill fining us $5,000. We just received a letter from one of our clients demanding that we pay the amount of $5,000 that was charged to their card, two years of Identity Theft protection through Life Lock, and attorney fees of $500. We think that 200 of our clients may have been affected. Does our Cyber Policy cover this?"

How do you respond?

THIRD PARTY CYBER LIABILITY QUIZ

1. **Information (Network) Security and Privacy Liability Coverage is for users of the internet and may cover liability from a virus that was transmitted via email.**

   True False

2. **Legal liability is required for Cyber third-party coverages.**

   True False

3. **All Cyber third-party liability coverage includes defense outside the limit of liability.**

   True False

4. **Some Website Media Content cyber coverage list specific perils.**

   True False

5. **An insured who knowingly posted false information on a website is covered because they qualify as an insured.**

   True False

6. **SPAM is covered by Website Media Content Liability.**

   True False

7. **Chargebacks are covered by Payment Card Fines and Assessments.**

   True False

8. **Contingent Bodily Injury and Property Damage Liability coverage is available in most cyber policies.**

   True False

It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public.

-Clay Shirky, American writer, consultant, and teacher on the social and economic effects of IT and journalism

SECTION SUMMARY

In this section you reviewed insurance policy provisions regarding coverage, limits, defense, and exclusions for Information (Network) Security and Privacy Liability, Payment Card Industry Fines and Assessments, Website Media Content Liability, and Contingent Bodily Injury and Property Damage Liability. Sample policy language was reviewed for each. The chapter ended with a claim scenario.

SECTION 6: INSURANCE COVERAGE, LIMITS, WAITING PERIOD, AND PERIOD OF INDEMNITY FOR FIRST PARTY TIME ELEMENT

During this section you will:

- Evaluate Cyber Business Income and Extra Expense Coverage
- Evaluate Contingent Cyber Business Income and Extra Expense
- Evaluate coverage including coverage triggers, aggregate and sub limits, waiting period, period of indemnity, and exclusions in each

BUSINESS INTERRUPTION

Coverage Triggers – cyber incidents

Coverage for costs of expenses to determine cause of interruption (forensics)

Sample Policy Language:

Business Interruption Loss means the total of :

1. **Income Loss** and **Extra Expense** during the **Period of Restoration**; and
2. **Extended Income Loss** if the **Income Loss** during the **Period of Restoration** is in excess of the applicable Retention.

Provided that **Business Interruption Loss** shall not mean and Insuring Agreement I.H. shall not cover any of the following: **Loss** arising out of any liability to a third party for whatever reason; legal costs or legal expenses of any type; **Loss** incurred as a result of unfavorable business conditions, loss of any market or any other consequential loss; or costs or expenses the **Insured Organization** incurs to identify and remove software program errors or vulnerabilities.

Business Income defined:

- Direct loss – loss of sales
- Indirect loss – lose ability to manage inventory

Sample Policy Definition:

"Business Income" means the:
a. Net income (net profit or loss before income taxes) that would have been earned or incurred; and
b. Continuing normal operating expenses incurred, including payroll.

Time Deductible / Waiting Period

- Time deductible stated in hours
- Limit usually a sublimit and may be stated as a percentage of the aggregate limit
- Subject to a specified number of days

BUSINESS INTERRUPTION

(Continued)

Exclusions

- System upgrade
- Utility failures
- Contractual penalties
- Legal costs or expenses
- Losses arising out of liability to a third party
- Other consequential loss or damage

Extra Expense Coverage

- Coverage triggers – cyber incidents
- No waiting period
- Extra expense defined

  Sample Policy Definition:

  Extra Expenses
  Reasonable and necessary costs incurred by the Insured to temporarily continue as nearly normal as practicable in the conduct of the **Insured's** business during the **Interruption Period**, less any value remaining at the end of the **Interruption Period** for property or services obtained in connection of those costs; "Normal" shall mean a condition that would have existed had no **Privacy Breach**, **Security Breach**, **Administrative Error** or **Power Failure** occurred.

  NOTE: Company may require notification of certain expenses for approval

- Exclusions
  - System upgrade
  - Utility failures

KNOWLEDGE CHECK:

What is a typical definition of Business Income found in a cyber policy? _____

_____

_____

_____

Who is required to prove the amount? _____

_____

CONTINGENT BUSINESS INCOME

Coverage Trigger – cyber incident of a shared resource (cloud service provider or processing utility) that is incurred by the insured

Sample Policy Language:

> Business Income Loss and Extra Expenses incurred during the **Interruption Period** directly as a result of the total, partial or intermittent interruption or degradation in service of the **Computer System** of an **Outsourced Service Provider** caused directly by a **Privacy Breach**, **Security Breach**, or **Administrative Error** at the **Outsourced Service Provider**.

Time Deductible / Waiting Period

- Time deductible stated in hours
- Limit usually a sublimit and may be stated as a percentage of the aggregate
- Coverage for a stated maximum number of days

Exclusions

- Specific vendors must be scheduled in some policies
- Infrastructure – basic services like an Internet Service Provider or the electrical grid

Contingent Extra Expense Considerations:

- Coverage Triggers – security failure
- No waiting period
- Extra expense defined
- Company may require notification of certain expenses for approval
- Exclusions

SAMPLE CLAIM – IS THERE COVERAGE?

ABC, Inc. has a Cyber Insurance Policy with the following:

Policy Aggregate	$1,000,000 Policy Limit
Business Income and Extra Expense 24-hour time deductible	$ 100,000

During the policy period, the insured called to report the following:

"We are not able to operate our restaurant business and had to close this morning because when we tried to log on to our network system, it was not available. We called our network service provider and were told that their network had been hacked and it will take them ten days to repair. Tomorrow is Valentine's Day, one of our busiest! We have sold out all our dinner reservations and 80% of our lunch operations. Because Valentine's Day is on a Friday this year, we also sold over 60% of our reservations for Saturday and are expecting one of the busiest weekends of the year. We estimate this will result in a loss of income in the amount of $25,000 and will have to pay our staff so that they won't quit and go to work for one of our competitors. The payroll will be $ 12,000 for the next ten days. Does our Cyber Policy cover this?"

How do you respond?

FIRST PARTY CYBER TIME ELEMENT QUIZ

1. **Because computers are necessary for many clients to operate their business, if the network is down, they may experience a loss of income and incur extra expenses.**

   True False

2. **Many clients feel that they are able to continue normal operations without using computers.**

   True False

3. **Business Interruption coverage on a cyber policy covers costs to upgrade the system caused by virus attack from a cyber-criminal.**

   True False

4. **DoS (Denial of Service) attack by a cyber-criminal that cripples the insured's network may be covered for Business Income and Extra Expenses under a cyber policy.**

   True False

5. **Business Income losses caused by loss of revenues during a cyber-attack are not subject to a waiting period.**

   True False

6. **Business Income coverage in a cyber policy is subject to a time limit.**

   True False

7. **Extra Expense coverage in a cyber policy is subject to a waiting period.**

   True False

8. **Businesses that use outsourced service providers have an exposure for Contingent Business Interruption and Extra Expense Coverage under a cyber policy**.

   True False

One of the tests of leadership is the ability to recognize a problem before it becomes an emergency.

-Arnold H. Glasow, American author

SECTION SUMMARY

In this section you reviewed insurance coverage, limits, waiting period and period of indemnity for cyber policies that cover Business Interruption and Extra Expense and Contingent Business Income and Extra Expense. A sample claim scenario involving Contingent Business Income was reviewed.

SECTION 7: INSURANCE COVERAGE, LIMITS, RETENTION AND EXCLUSIONS FOR FIRST PARTY THEFT OF PROPERTY

During this section you will:

- Review cyber insurance coverage, limits, retention, and exclusions for Data Restoration
- Review cyber insurance coverage, limits, retention, and exclusions for Cyber Extortion
- Review cyber insurance and crime coverage that may cover Computer Fraud
- Review cyber insurance and crime coverage that may cover Funds Transfer Fraud
- Review cyber insurance and endorsements that may cover Social Engineering/Cyber Crime coverage
- Discuss the importance of coordination among insuring agreements

DATA ASSETS RESTORATION COVERAGE

Coverage triggers:

- Unauthorized access
- Introduction of malicious code
- Accidental or unauthorized release of private information
- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack

Sample Policy Language:

Loss of or Damage to Insured's Network

For the **Insured Entity's** reasonable and necessary expenses resulting from an **Exploit** that occurs during the **Policy Period**, that are required to restore the **Insured Entity's Network** or information residing on the **Insured Entity's Network** to substantially the form in which it existed immediately prior to such **Exploit**.

Usually a sublimit and deductible / retention

Exclusions

- Costs of research to create data lost
- Upgrade to systems
- Failure for insured to keep software updated

CYBER EXTORTION

Usually triggered by a threat, introduction of malicious code

Read the policy language very carefully – look for:

- Investigation costs
- Retention of a negotiator
- "Ransom" payment
- Reward to an informant

KNOWLEDGE CHECK:
Do insurers writing Cyber Extortion Coverage use experts in cyber-crime to investigate?

CYBER EXTORTION

(Continued)

Sample Policy Language:

Network Extortion Expense means all reasonable and necessary expenses incurred by the **Insured Entity**
A. in order to protect **Insured Entity's Money** or **Securities** or **Intangible Property** from loss, including payment of monies demanded by an extortionist,
B. in order to avoid loss of or damage to **Insured Entity's Network** in response to a **Network Extortion** including payment of monies demanded by an extortionist.
Provided, however that **Network Extortion Expense** shall not include any **Loss** based upon, directly or indirectly arising out of, or in any way involving any demands by an extortionist other than demands for money in exchange for:
1. the restoration or return **of Insured Entity's Money**, **Securities, Goods**, **Services**, or **Intangible Property**; or
2. the restoration of **Insured Entity's Network**; or
3. the restoration of any defaced portions of the **Insured Entity'**s web site; or
4. not carrying out illegal threats made directly or indirectly, to impair or destroy **Insured Entity's Network** by an **Exploi**t perpetrated by means of **Electronic Transfer** or;
5. not publicizing that **Insured Entity's Network** will be or has been impaired or destroyed by an **Exploit** perpetrated by means of an **Electronic Transfer**; or
6. not disclosing the **Insured Entity's** confidential information to unauthorized recipients.

Network Impairment means disruption or damage to the **Insured's Network** causing that network to be impaired to such an extent that the **Insured** is substantially unable to conduct one or more activities defined as **Network Activity**.

Usually has a sublimit

- Some Kidnap & Ransom policies may provide coverage
- Many companies work closely with insured
- May require an agreement with the insured before paying ransom

Exclusions:

- Acts by an insured (crimes)
- Amounts paid prior to notifying the insurer
- Amount needed to improve systems following an attack

UNDERSTANDING COMPUTER FRAUD

Computer Fraud - What is it?

Coverage Triggers:

"Business Email Compromise" (BEC)

Invoice Manipulation: Hacker(s) impersonate the insured, tricking their client's customers or vendors into payments of fraudulent accounts.

"Email Account Compromise" (EAC)

May include Crypto jacking – "Malicious Crypto mining"

Crypto jacking: Is an online threat that hides on a computer or mobile device and uses the machine's resources to "mine" forms of cryptocurrency. Malicious crypto miners often come through web browser downloads or rouge mobile apps.

May be covered by a Crime Policy:

Sample Crime Policy language

We will pay for loss of or damage to "money", "securities" and "other property" resulting directly from the use of any computer to fraudulently cause a transfer of the property from inside the "premises" or "banking premises"

Other Keys to Consider:

- Sublimit – extremely hard to find and usually by endorsement
- Deductible / Retention applies
- Conditions apply:
  - Multi-Factor Authentication (MFA)
  - Mandatory employee training
  - Updated cyber security software
- Exclusions
  - Indirect or consequential loss
  - Deliberate acts of an insured
  - Claims by Government Agency
  - Securities/Management Liability

FUNDS TRANSFER FRAUD

(aka Financial Fraud)

Funds Transfer Fraud Insurance

Funds Transfer Fraud Insurance covers the loss of money resulting from a financial institution transferring funds based on fraudulent instructions received from someone pretending to be an authorized user.

Coverage Triggers:

- Intentional unauthorized transfer request to a financial institution
- Theft of money or securities by electronic means
- Fraudulent written, electronic or telephone instruction

NOTE: May be covered by a Crime Policy, BOP, or Management Liability Policy

KNOWLEDGE CHECK:
Cyber policies can be used to provide coverage for Computer Fraud. Is another policy able to provide any coverage?

POLICY NUMBER:

CRIME AND FIDELITY
CR 04 17 11 15

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

FRAUDULENT IMPERSONATION

This endorsement modifies insurance provided under the following:

COMMERCIAL CRIME COVERAGE FORM
COMMERCIAL CRIME POLICY
GOVERNMENT CRIME COVERAGE FORM
GOVERNMENT CRIME POLICY

SCHEDULE

Check the appropriate box(es):

I. Fraudulent Impersonation Of "Employees" Included: Yes ☐ No ☐

- ☐ **A.** Verification Is Required For All "Transfer Instructions"
- ☐ **B.** Verification Is Required For All "Transfer Instructions" In Excess Of **$**
- ☐ **C.** Verification Of "Transfer Instructions" Is Not Required

II. Fraudulent Impersonation Of "Customers" And "Vendors" Included: Yes ☐ No ☐

- ☐ **A.** Verification Is Required For All "Transfer Instructions"
- ☐ **B.** Verification Is Required For All "Transfer Instructions" In Excess Of **$**
- ☐ **C.** Verification Of "Transfer Instructions" Is Not Required

Information required to complete this Schedule, if not shown above, will be shown in the Declarations.

With regard to this Fraudulent Impersonation endorsement, the provisions of the Coverage Form or Policy to which this endorsement is attached apply, unless modified by this endorsement.

A. The following Insuring Agreement is added to Section **A. Insuring Agreements:**

Fraudulent Impersonation

1. "Employees" (if indicated in Section I. of the Schedule)

We will pay for loss resulting directly from your having, in good faith, transferred "money", "securities" or "other property" in reliance upon a "transfer instruction" purportedly issued by:

a. An "employee", or any of your partners, "members", "managers", officers, directors or trustees, or you (if you are a sole proprietorship) if coverage is written under the Commercial Crime Coverage Form or Commercial Crime Policy; or

FRAUDULENT IMPERSONATION ENDORSEMENT

Things to Know:

- Endorsement may be subject to sublimit
- Verification is usually required for “Transfer Instructions”
- Fraudulent Impersonation of who?
    - Employees
    - Customers
    - Vendors
- Sublimit applies on Cyber Policy
- Deductible / Retention
- Exclusions
    - Verification not followed
    - Social Engineering

SOCIAL ENGINEERING / FRAUDULENT INSTRUCTION / CYBER CRIME ENDORSEMENTS

NOTE:
This coverage is usually found as an endorsement and goes by many names. Many carriers do not offer coverage and those that do have strict underwriting criteria.

Sample Endorsement Language:

The insurer will pay the **Insured Entity** for **Social Engineering Fraud Loss** resulting directly from a **Social Engineering Fraud Event** in excess of the applicable retention and within the applicable Limits of Insurance.

It is a condition precedent to coverage under the **Social Engineering Fraud** coverage that the Insured attempted to authenticate the **Fraudulent Instruction** prior to transferring and **Money** or **Securities.**

Sample Policy Forms are on the following pages.

Endorsement No.	Effective Date of Endorsement	Policy Number	~ePremHead
~eNo	12:01 a.m. on ~eEff If the above date is blank, then this endorsement is effective on the effective date of the policy.	~ePol	~ePrem

SOCIAL ENGINEERING FRAUD COVERAGE ENDORSEMENT

SCHEDULE OF SOCIAL ENGINEERING FRAUD LOSS COVERAGE	
Social Engineering Fraud Loss Limit of Insurance	~SocialLimit
Social Engineering Fraud Loss Retention	~SocialRetention

Information in the above schedule also may appear on the Declarations.

It is agreed that:

I. The Declarations are amended by the addition of the above new Limit of Insurance and Retention in the Items entitled **First Party Coverages Limits of Insurance** and **First Party Coverages Retention**, respectively.

II. The section of the Policy entitled **FIRST PARTY COVERAGES** is amended as follows:

A. The following new coverage is added:

Social Engineering Fraud Coverage

The Insurer will pay the **Insured Entity** for **Social Engineering Fraud Loss** resulting directly from a **Social Engineering Fraud Event**, in excess of the applicable retention and within the applicable Limits of Insurance.

It is a condition precedent to coverage under the **Social Engineering Fraud** Coverage that the **Insured** attempted to **Authenticate** the **Fraudulent Instruction** prior to transferring any **Money** or **Securities**.

B. Solely with respect to the coverage provided by this endorsement, the paragraph addressing conditions precedent to coverage under the First Party Coverages is amended as follows:

1. Wherever the words "**Enterprise Security Event** or **Extortion Threat**" appear they are deleted and replaced by "**Enterprise Security Event, Extortion Threat** or **Social Engineering Fraud Event**."

2. Wherever the words "**Related Enterprise Security Event** or **Related Extortion Threat**" appear they are deleted and replaced by "**Related Enterprise Security Event**, **Related Extortion Threat** or **Related Social Engineering Fraud Event**."

III. Solely with respect to the coverage provided by this endorsement, the section of the Policy entitled **LIMITS OF INSURANCE, RETENTION AND REIMBURSEMENT** is amended as follows:

A. The subsection entitled **Multiple Insureds, Claims, Claimants** is deleted and replaced by the following:

ENDORSEMENT #003

This endorsement, effective 12:01 a.m., , forms a part of

Policy No. issued to

by .

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

SOCIAL ENGINEERING FINANCIAL FRAUD ENDORSEMENT

In consideration of the premium charged, it is agreed that:

- Item 4. Coverage Schedule of the Declarations is amended by adding a new Insuring Agreement, Sublimit and Retention as indicated below:

Insuring Agreements	Sublimit	Retention
Social Engineering Financial Fraud	$_____	$_____

- Section **I. B. First Party Coverages** is amended to include the following new coverage:

  Social Engineering Financial Fraud

  The **Insurer** will pay or reimburse the **Insured Company** for **social engineering financial fraud loss** in excess of the applicable retention directly resulting from a **social engineering financial fraud event**.

- Section **D.2. Conditions** is amended to include the following new provision:

  The coverage provided under Section **I.B.** Social Engineering Financial Fraud shall apply only if the **Insured** verifies the instruction to transfer **money** or **securities** by following a pre-arranged callback or other established procedural method to authenticate the validity of the request prior to acting upon any transfer instruction.

- Section **IV. Definitions**, is amended to include the following new defined terms:

  AUTHORIZED EMPLOYEE
  An employee of the **Insured Company** who is authorized by the **Insured Company** to transfer, or to instruct others to transfer, **money** or **securities**.

  MONEY
  The **Insured's**:
  1. Currency, coins and bank notes in current use and having a face value; and
  2. Traveler's checks and money orders held for sale to the public.

SOCIAL ENGINEERING / FRAUDULENT INSTRUCTION / CYBER CRIME ENDORSEMENTS

Things to Know:

- Coverage triggers
- Coverage by endorsement
- Sublimit on endorsement
- Deductible/Retention
- Conditions applicable - also on endorsement

Coordination among Insuring Agreements:

*"Coverage exists only for those Insuring Agreements designated as included in Item 3 of the Declarations and attached to this Policy. Each contains terms which limit coverage to the scope of the coverage grant for that Insuring Agreement. Should two or more Insuring Agreements apply to the same **Claim** the Insurer will not pay more than the actual loss or the highest available remaining limit of insurance under any one Liability Coverage, whichever is less. Should two or more First Party Insuring Agreements apply to the same **occurrence**; the Insurer will not pay more that the lowest applicable limit of insurance. In no instance, shall the insurer be required to pay more than the Policy Aggregate identified in the Declarations."*

Other Insurance:

*"The coverage provided by this Policy is excess over and above any other valid insurance, (including any retention or deductible portion) or agreement available to **you**."*

*"The insurance under this Policy shall apply in excess over any other valid and collectible insurance available to any **Insured**, including any self-insured retention or deductible portion thereof unless such other insurance is written only as specific excess insurance over the **Policy Aggregate Limit of Liability** or other applicable Limit of Liability of this Policy."*

"When this Policy is excess, we shall have no duty under Insuring Agreement 6. Security Breach Liability to defend the "insured" against any "suit". If no other insurer defends, we will undertake to do so, but we will be entitled to the "insured's" rights against other insurers."

SAMPLE CLAIM – IS THERE COVERAGE?

ABC, Inc. has an endorsement to their Cyber Insurance Policy for Social Engineering Fraud with the following:

Policy Aggregate	$1,000,000 Policy Limit

Endorsement	**Sublimit**	**Retention**
Social Engineering Financial Fraud	$ 50,000	$ 1,000

During the policy period, the insured called to report the following:

> "Our bookkeeper was balancing our last bank statement and found a $10,000 transfer from our checking account was done without her knowledge. When she called the bank to report it, they said the VP of Operations approved the transfer. We talked to him, and he said yes, he had approved the transfer because he had received an email from the President of our company instructing him to do so and he immediately did as requested. Our president has told us that he did not send the email and had never authorized the transfer. He then said to turn in a claim for Financial Fraud on our policy, so that's why I am calling today."

How do you respond?

CYBER FIRST PARTY THEFT OF PROPERTY QUIZ

1. **Many businesses think that they have coverage under their property insurance for damage to data.**

   True False

2. **Property insurance forms cover data and all expenses to recreate it if it is damaged by an insured peril.**

   True False

3. **Coverage triggers causing theft of data include unauthorized access and introduction of malicious code.**

   True False

4. **Data restoration coverage in cyber policies cover the cost of research necessary to create the data lost.**

   True False

5. **Cyber Extortion coverage will pay for amounts paid prior to notifying the insurer.**

   True False

6. **Media rarely spotlights cyber extortion because it is done by cyber criminals.**

   True False

7. **Social Engineering claims are rare and only affect large high-profile companies.**

   True False

8. **It is important to coordinate coverage among insurance policies in force for the insured.**

   True False

Social engineering is using deception, manipulation, and influence to convince a human who has access to a computer system to do something, like click on an attachment in an e-mail.

-Kevin Mitnick, American computer security consultant, author, and convicted hacker

SECTION SUMMARY

In this section you reviewed Data Assets Restoration cyber coverage, limits, retention, and exclusions. You reviewed Cyber Extortion coverage, limits, retention, and exclusions. You then looked at cyber policy coverage and crime policy coverage that may be available for Computer Fraud and Funds Transfer Fraud.

Next was a review of cyber insurance that may be available as an endorsement for Social Engineering and the sublimit, retention, and conditions that apply.

You reviewed the importance of coordination amount, insuring agreements, and other insurance clauses. A sample claim involving social engineering ended this section.

SECTION 8: COMBINING LOSS CONTROL WITH CYBER INSURANCE COVERAGE

During this section you will:

- Identify a warranted application used by many cyber insurance companies
- Differentiate warranty statements vs representations on cyber insurance applications
- Review Best Practices for Cyber Loss Control
- Review resources that may be provided by cyber insurers
- Review the need for mandatory employee training for cyber threats

WARRANTIES AND REPRESENTATIONS

The cyber application may be "warranted" if a policy is issued.

Sample Policy Language:

> The Underwriters agree with the **Named Insured**, set forth in Item 1. Of the Declarations made a part hereof, in consideration of the payment of the premium and reliance upon statements in the **Application** to this Insurance Policy (hereinafter referred to as the "policy" or "Insurance") and subject to all the provisions, terms and conditions of this Policy:

What is a "warranty application"?

Sample Policy Language:

> I declare that (a) this application form has been completed after reasonable inquiry, including but not limited to all necessary inquiries of my fellow principals, partners, officers, directors and employees, to enable me to answer the questions accurately and (b) its contents are true and accurate and not misleading. I undertake to inform you before the inception of any policy pursuant to this application of any material change to the information already provided or any new fact or matter that may be material to the consideration of this application for insurance. I agree that this application form and all other information which is provided are incorporated into and form the basis of any contract of insurance.

> **THE APPLICANT WARRANTS THAT THE STATEMENTS AND RESPONSES TO THE QUESTIONS ON THIS APPLICATION ARE TRUE AND COMPLETE.** THIS APPLICATION DOES NOT BIND THE APPLICANT OR THE COMPANY, NOT DOES IT OBLIGATE THE COMPANY TO ISSUE COVERAGE. SUCH POLICY MAY BE CANCELLED BY THE COMPANY FROM INCEPTION UPON DISCOVERY THAT THE POLICY WAS OBTAINED THROUGH A FRAUDULENT STATEMENT, OMISSION, OR CONCEALMENT OF THE FACTS MATERIAL TO THE ACCEPTANCE OF THE RISK OR HAZARD ASSUMED.

What are "representations"?

> The **Company** shall have the right to make any investigation they deem necessary with respect to coverage including the **Application**.

KNOWLEDGE CHECK:
What is a warranty on the application for cyber coverage?

BEST PRACTICES FOR CYBER LOSS CONTROL

Multifactor authentication (MFA)	Requiring at least two pieces of evidence to validate a user's identity
Endpoint detention and response (EDR)	The continuous monitoring and analysis of endpoints
Backups	Secured, encrypted and tested backups
Privileged access management (PAM)	Designed to ensure that employees have only necessary level of access – not additional – to perform their jobs
Email filtering and web security	Identifies and blocks malicious emails and attachments; web filtering blocks inappropriate sites
Written Policies and Procedures	Data Security Policy Pre-breach Preparedness Plan Data Breach Response Plan

:

RESOURCES AVAILABLE FROM CYBER INSURANCE COMPANIES

Things to Know and Be Aware of:

- Bundled (included) or additional cost to insured?
- Active Avoidance – Risk Audits and Vulnerability Assessments
- Pre-breach Preparedness Assistance
- Helpline
- Information portal
- Additional/Other services provided
    - Access to specialists including law firms at reduced fees
    - Discounted rates on other services and software
    - Newsletters
    - Training and compliance
    - Post-Breach Notification Services

KNOWLEDGE CHECK:
Name three loss control services that are usually bundled by cyber insurers:

1. _____
2. _____
3. _____

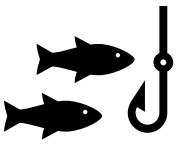
MANDATORY TRAINING OF ALL EMPLOYEES

and those with access to the network

Written contract with vendors, independent contractors

Training & compliance offered as additional policyholder services

Third-party providers for an additional fee



Phishing is the top technique used for initial access of cyber incidents

Adopt a zero-trust approach to security and data management

Types of employee training:

1. Phishing and Spam training
2. Create an acceptable use policy to teach employees which websites are allowed
3. Strong password training
4. Teach employees how to report problems
5. Teach employees to take proper care of their devices both physically and digitally
6. Teach the importance of updates on all devices
7. Set up training on the use of a Virtual Private Network (VPN) for all remote workers

Let us not look back in anger or forward in fear, but around in awareness.

-James Thurber, American cartoonist, writer, humorist, journalist, and playwright

SECTION SUMMARY

In this section you reviewed the difference between an application that may be "warranted" and compared it to representations made on applications that are not "warranted".

You then reviewed suggested Best Practices for Cyber Loss Control and the resources that may be available from cyber insurers.

You reviewed the need for all employees of an organization to have mandatory training on a regular basis. This section ended with an overview of some of the important information that was presented today.

FINAL THOUGHTS ON MITIGATING CYBER EXPOSURE

- **Cyber threats are changing by the minute**
  Cyber-crime is a business that is ever changing. Because we use the internet in our businesses daily, combined with the portability and use of smart devices, we all need to be aware of the threats that exist as well as emerging exposures

- **Continue Educating**
  Cyber insurance coverage is constantly changing. It has evolved from the first policies that were originally written to protect the technology industry for professional liability (Technology Errors and Omissions) to policies designed for users of technology in business operations. The policies are constantly changing, and insurance professionals need to update their knowledge about coverages, limits, exclusions and conditions on a timely basis.

- **Offer Cyber Coverage to all of your commercial clients**
  In order to offer better insurance protection and avoid insurance errors and omission claims against us, we must offer cyber protection to all of our commercial clients and document our offerings

- **Stress the need to incorporate Loss Control with Cyber Insurance**
  Today's cyber insurance market is ever-changing, and most insurers offer bundled loss control services along with their insurance protection. Many have conditions in the cyber policy that require various loss controls are in place before they will offer insurance protection and also state continuous mandatory uses when a claim is submitted in order for coverage to apply.

CPIA Designation

GENERAL INFORMATION

CPIA PROGRAM OFFICE:
PO Box 35718
Richmond, VA 23235
877-674-CPIA (2742)
www.cpia.com

THE CERTIFIED PROFESSIONAL INSURANCE AGENT (CPIA) DESIGNATION

The Certified Professional Insurance Agent (CPIA) Designation is first-of-its-kind, hands-on, how-to training. To earn the CPIA designation, candidates are required to participate in a series of three, one-day Seminars. These Seminars are designed to enhance the ability of producers, sales support staff, and company personnel to efficiently create and distribute effective insurance programs. Participants leave with ideas that will produce sales results immediately.

The *three* core CPIA Seminars are entitled:
Position for Success (CPIA 1)
Implement for Success (CPIA 2)
Sustain Success (CPIA 3)

Concentrated, single-topic seminars are also available. A sampling of topics include:
Disaster and Continuity Planning for Businesses and Families
An Agent's Guide to Understanding and Mitigating Cyber Exposures
An E & O Loss Control Program for All Agencies

Seminars are offered in-person and online in both English and Spanish. Seminars qualify for CE credit in most states. For more details and the complete schedule of course offerings, visit www.cpia.com.

NOTIFICATION OF COMPLETION OF THE DESIGNATION REQUIREMENTS

Upon completion of the three core CPIA Seminars, the CPIA Program Administrator will notify new designees. Designees will receive confirmation of completion along with guidance for using the CPIA logo, a sample press release, a diploma order form, and more. Diplomas are prepared and shipped to new designees on a quarterly basis.

CPIA DESIGNATION UPDATE REQUIREMENT

The Certified Professional Insurance Agent (CPIA) designation stands for professionalism, commitment to professional training and results, and technical knowledge. To maintain the right to use the CPIA designation, designees must update on an annual basis. Reminders are emailed by the CPIA Program Administrator.

The CPIA update requirement can be satisfied by:

- participating in any one of the three core CPIA Seminars,
- participating in any one of the special topic (Advanced) CPIA Seminars, or
- maintaining a CPIA Program Membership annually at the Ruby, Sapphire, or Diamond level.

PIA AND THE CPIA PROGRAM

In late 2022, the National Association of Professional Insurance Agents (PIA) and the American Insurance Marketing and Sales Society (AIMS Society, original creators of the CPIA designation program) decided to consolidate to better serve the educational needs of independent agents and the entire insurance industry. The coming together of these two powerhouse organizations, each with a long history of providing excellent education programming, will benefit both independent agents and the insurance industry as a whole. Through a Professional Development Advisory Council, PIA will build upon the CPIA designation program framework and continue to champion and accelerate marketing and sales development for insurance professionals. Visit www.cpia.com for more details and a complete schedule of upcoming classes.

CPIA PROGRAM MEMBERSHIP

Accelerate Professionalism and Sales Excellence

For insurance professionals who seek to keep marketing and sales skill building top of mind, the CPIA Program Membership offers innovative, practical, actionable solutions. Unlike insurance coverage education providers, we're solely focused on growing revenue and customer relationships.

CPIA Program Membership is structured to build strong marketing and sales skills among insurance agency producers, support staff, and insurance company personnel. CPIA Program membership also means access to a nationwide network of professionals who are focused on increasing personal and agency production.

A variety of member benefits packages are available to best suit your / your organization's needs:

RUBY MEMBERSHIP - $199 per person, annually - Insurance professionals who join the CPIA Program as at the "***Ruby***" level will receive the following:

- Satisfies CPIA Designation Annual Update - This level of membership satisfies the annual update requirement for keeping your CPIA designation.
- Online Membership Networking Directory - Access to member-only resources, including a directory of other members searchable by a variety of criteria.
- Online Member Community - Engage with other members and share best practices, industry news, advocacy efforts, and professional resources.
- Professional Development Insights - Email communiques with sales tips, management advice, and marketing resources. Publications include: *Quik Sales Tips* (12/year) *Marketing Muscle* (6/year); and *Bright Ideas* (6/year).
- Education Program Discounts - Enjoy discounts on select CPIA seminars.

SAPPHIRE MEMBERSHIP - $499 per person annually - The CPIA Program "***Sapphire"*** level provides all the benefits of ***RUBY MEMBERSHIP***, plus:

- RoughNotes-Pro – Enjoy access for ***one producer*** to: PF&M; Coverages Applicable; PL & CL Risk Evaluation Systems, which include comprehensive coverage checklists and questionnaires; Insurance Marketplace; and *InAction* newsletter and *Rough Notes* Magazine.

DIAMOND MEMBERSHIP - $750+* annually - The CPIA Program "***Diamond"*** *level* provides all the benefits of ***RUBY MEMBERSHIP***, plus:

- RoughNotes Advantage-Plus - Enjoy ***group*** access to: PF&M; Coverages Applicable; PL & CL Risk Evaluation Systems; *How to Insure* training classes; *Insurance Words and their Meaning*; Business Building Letters; Blog Content and Digital Media Content; Insurance Marketplace; and *InAction* newsletter and *Rough Notes* Magazine.

**Diamond Membership pricing is based on number of employees*

ROUGHNOTES-PRO

INCLUDES

Policy Forms & Manual Analysis (PF&M)
An essential go-to guide to strengthen your property & casualty expertise on commercial, personal and specialty lines coverages and concepts. Demonstrate your insight to enhance your competency. Use real court case decisions when presenting coverage concerns to new prospects and current clients.

Coverages Applicable
Learn appropriate coverages quickly and gain traction to remain competitive.

Personal Lines Risk Evaluation System
A comprehensive checklist of personal lines risk exposures.

Commercial Lines Risk Evaluation System
A comprehensive checklist for more than 723 classes of business.

In Action
A monthly newsletter that will show you ways to turn coverage knowledge into powerful sales opportunities.

Rough Notes magazine
The industry's leading insurance agent publication.

The Insurance Marketplace
Agency professional's number one source to find hard-to-find coverages.

Property and Casualty Insurance By Philip Gordis
An easy -to-use, quick – reference guide to property and casualty insurance coverages. The indexing and examples put the answers to your basic coverage questions at your fingertips.

ROUGHNOTES ADVANTAGE-PLUS

A $900 retail value, RoughNotes Advantage-Plus is included in CPIA Program Diamond Membership. For details visit www.cpia.com or call 877-674-CPIA (2742).

INCLUDES:

Policy Forms & Manual Analysis (PF&M)

An essential go-to guide to strengthening your property & casualty expertise on commercial, personal, and specialty lines coverages and concepts. Demonstrate your insight to enhance your competency. Use real court case decisions when presenting coverage concerns to new prospects and current clients.

Coverages Applicable

Learn appropriate coverages quickly and gain traction to remain competitive. Explore the insurance needs of more than 700 different kinds of risks with SIC and NAICS codes.

Personal Lines/Commercial Lines Risk Evaluation Systems

A comprehensive checklist of personal lines risk exposures and checklists for more than 723 classes of business.

How to Insure Training Courses

Educational tutorials that close the “insurance knowledge gap.”

Insurance Words and Their Meanings

A guide to insurance terminology for you, your staff, and your clients.

Business Building Letters

Hundreds of business support templates used for sales, and renewals and to run an efficient business.

Blogs

Over 300 short articles that agencies can use to blog, email, or display on their websites to enhance sales pipelines.

Digital Media

Animated videos used to book new clients and increase client retention.

In Action

A monthly newsletter of how you can turn coverage knowledge into powerful sales opportunities.

Rough Notes magazine

The industry’s leading insurance agent publication.

The Insurance Marketplace

Agency professional’s number one source to find hard-to-find coverages.

CPIA PROGRAM MEMBERSHIP APPLICATION

Accelerate Professionalism and Sales Excellence

JOIN TODAY!

To join online, visit www.cpia.com and select "Join Now." Alternatively, complete the following and return it to the CPIA Program Office, c/o AIMS Society, PO Box 35718, Richmond, VA 23235 with your membership dues.

Name (First, MI, Last) _____ Designations _____

Company Name _____

Mailing Address _____ City/State/Zip _____

( ) _____

Business Phone # _____

Email Address _____ Website _____

MEMBERSHIP SELECTIONS:

		TOTAL
❑ Ruby membership……	$199	$
❑ Sapphire membership……	$499	$
Diamond membership		
❑ 1-4 producers……	$750	$
❑ 5+ producers……	Call for pricing	$
Select additional CPIA Designee logo items:		
❑ CPIA Wall Plaque……...	$60 + shipping	$
❑ CPIA logo pin (Gold color with CPIA logo)……	$25 + shipping	$
	TOTAL AMOUNT DUE	$

PAYMENT INFORMATION:

❑ Enclosed please find my check made payable to the "AIMS Society."

❑ Please charge my credit card: ❑ Master Card ❑ VISA ❑ AMEX

Name as it appears on card: _____

Credit Card #: | | | | | | | | | | | | | | | | |

Expiration Date: | | | / | | | | | Security Code: | | | | |

Cardholder's Signature: _____ Date: _____

CPIA SEMINAR ENROLLMENT / CHANGE OF INFORMATION FORM

(Please Print)

Check the appropriate boxes: (*select one*)

- ❑ I am a new student and I plan to pursue the CPIA designation
- ❑ I have attended a CPIA Seminar previously – no changes to report
- ❑ I have attended a CPIA Seminar previously but need to update my information *(complete the information to be updated in the appropriate sections below)*
- ❑ I am attending to satisfy the annual update requirement to maintain my CPIA designation

FULL NAME (First, MI, Last)

INDUSTRY DESIGNATIONS

AGENCY/COMPANY NAME

BUSINESS PHONE EMAIL

BUSINESS MAILING ADDRESS

CITY STATE ZIP

HOME ADDRESS

CITY STATE ZIP

AGENCY PRINCIPAL/MANAGER

AGENCY PRINCIPAL/MANAGER EMAIL

AGENCY/COMPANY FACEBOOK PAGE

AGENCY/COMPANY LINKEDIN PAGE

AGENCY/COMPANY TWITTER HANDLE

SIGNATURE

Insurance Success Seminars

CONTINUING EDUCATION REQUEST FORM

"An Agent's Guide to Understanding & Mitigating Cyber Exposures" is approved for continuing education credit in some states which have a Continuing Education Requirement. Listed below are the states where approval has been granted to-date and the corresponding number of credit hours granted. To receive Continuing Education Credit for this class, complete this form and submit fees as indicated. Return this form to the program coordinator **before the end of the class**. One-hundred percent attendance is required for receipt of continuing education credit.

PLEASE CHECK THE STATE where you hold a resident agent license and for which you would like to receive CE credit. Write in your license number and/or NPN as indicated below. ***PLEASE NOTE**: **A $25 fee (payable to the AIMS Society), the state filing fee (if applicable) and your state filing penalty (if applicable) will be charged for CE requests that are not submitted on the day of the class or if the information required on this form is not complete.***

IF YOU DO NOT REQUIRE CE FOR THIS CLASS, CHECK THIS BOX, SIGN AND RETURN THIS FORM ❑ I DO NOT REQUIRE CE

- ❑ Alabama (attach $8 filing fee)..... 8 hrs.
- ❑ Arkansas (attach $8 filing fee) (3 ethics 5 general) ..... 8 hrs.
- ❑ Florida..... 8 hrs.
- ❑ Indiana (attach $4 filing fee)..... 8 hrs.
- ❑ Kansas (attach $8 filing fee)..... 8 hrs.
- ❑ Maryland (attach $9.15 filing fee) ..... 8 hrs.
- ❑ Massachusetts (attach $9 filing fee)..... 6 hrs.
- ❑ Michigan (attach $8 filing fee) (5 PC 3 ethics)..... 8 hrs.
- ❑ New York ..... 8 hrs.
- ❑ North Dakota (attach $8 filing fee) ..... 8 hrs.
- ❑ Pennsylvania (attach $5 filing fee) (General)..... 8 hrs.
- ❑ Virginia (attach $20.80 filing fee) (8 general)..... 8 hrs.
- ❑ West Virginia (attach $12.00 filing fee) (General) ..... 8 hrs.

Course Date _____ Course Location _____

Full name as it appears on your license _____ License Number and / or NPN Number _____

Business Mailing Address _____ City/State/Zip _____

Home Mailing Address _____ City/State/Zip _____

( ) _____

Business Telephone # Email Address

CPIA Program Office
P.O. Box 35718
Richmond, VA 23235
(804) 674-6466

I hereby attest to the fact that I have attended the above program in its entirety and signed the attendance verification forms which were circulated during the program.

Signature _____