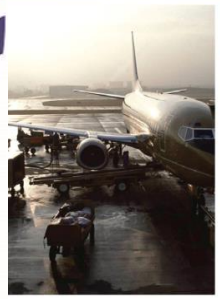
IFFCBANO
INTERNATIONAL TRADE
SYMPOSIUM
2017




Cyber Insurance
Coverage and Real World Claims

Presented by: Grant E. Goldsmith

Division Vice President, Avalon Risk Management

Agenda

- Where can you find “Crime” Coverage in your policies
- How Do Insurance Companies Cover “Crime” in various policies
- Why is Cyber Crime and Cyber Liability Important
- Examples of Real World Situations that we have seen

Policies with “Crime” Insurance Coverage

- Property Policy (Limited)
  - For Theft of goods or money on your premises or away from your premises or in a vehicle or at a Trade Show
- “Crime” Policy (Broad and Typically Inexpensive)
  - For theft of goods/money by Employees or Third Parties. Can cover your business for your Employees on other’s premises that steal while on site.
- Cyber Policy (Newer, Inexpensive in most cases)
  - For thefts related to your use of an electronic system. Can cover your loss, misuse or damage to other’s systems.
- Management Liability Package Policy
  - Includes D&O, Crime, EPLI, K&R, Cyber, Miscellaneous E&O

“Crime” or “Theft” Coverages Change per Policy – Read the Fine Print!

- Property Policy
  - Will typically pay for a “loss” due to “theft” committed by others of “covered property” on a premises or in a vehicle but will not cover “thefts” committed by employees
- Crime Policy
  - Will pay for coverage in several areas from outside thieves or inside (employee) thieves – see next slide
- Cyber Liability Policy
  - Will cover some theft but also covers your risks or doing damage to third parties through loss of private data or damage to others networks

TYPICAL CRIME COVERAGE AREAS

Coverage A: Fidelity		
(1) Employee Theft	$ 2,000,000	$ 25,000
(2) ERISA (Limit Applies Per Plan)	$ 1,000,000	N/A
(3) Clients' Property	$ 2,000,000	$ 25,000
(4) Vendor Theft	$ 2,000,000	$ 25,000
Coverage B: Forgery or Alteration		
(1) Checks	$ 2,000,000	$ 25,000
(2) Credit, Debit or Charge Cards	$ 2,000,000	$ 25,000
(3) Personal Accounts	Not Covered	N/A
Coverage C: Inside and Outside the Premises		
(1) Inside the Premises	$ 2,000,000	$ 25,000
(2) Outside the Premises	$ 2,000,000	$ 25,000
Coverage D: Computer and Funds Transfer Fraud		
(1) Computer Fraud	$ 2,000,000	$ 25,000
(2) Funds Transfer Fraud	$ 2,000,000	$ 25,000
Coverage E: Money Orders and Counterfeit Money	$ 2,000,000	$ 25,000
Coverage F: Telephone Toll Fraud	Not Covered	N/A
Coverage G: Identity Fraud Expense	Not Covered	N/A
Coverage H: Virus and Licensing Violations		
(1) Virus Restoration	Not Covered	N/A
(2) Licensing Violation Fines and Penalties	Not Covered	N/A
Coverage I: Expense	$ 100,000	N/A

CYBER CRIME STATISTICS

Crime – Cyber Deception Endorsement

When it's a trick and not a hack, how is your client protected?

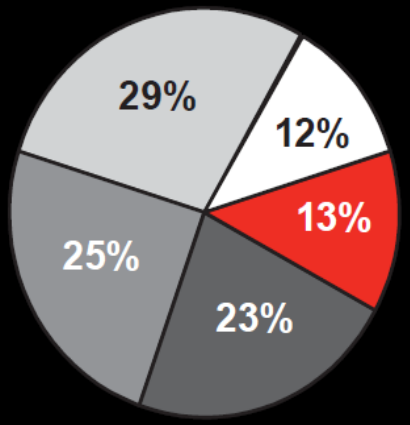
Cyber Deception occurs when a criminal disguises themselves as a vendor, client or employee and tricks the insured's employee into transferring funds to an account under their control. With Hiscox's new Cyber Deception endorsement, your client is protected from such an attack.

13%

OF ATTACKS TIED TO TRICKS NOT HACKING[1]

- Web-based attacks
- Phishing and social engineering
- Denial of service
- Malicious code
- Others

Most costly kinds of attacks



Two Cyber Liability Options

C N A Insurance Company

- Options for limits at $1M and $3M limits
- Premium ranging from $4,300 – 5,834
- Deductibles of $25K and $50K
- Retroactive Date is policy inception date
- Coverage - $1M in limits for:
  - Network Security Liability
  - Privacy Liability
  - Privacy Event Expense
  - Privacy Regulatory Proceeding
  - Network Extortion Expense

Lloyd's of London Syndicate

- $1M in limits
- Premium $12,116
- Deductible of $10K
- No Retroactive Date (will pick up past incidents not known to you now)
- Coverage - $1M in limits for:
  - Multimedia Liability
  - Security and Privacy Liability
  - Breach Event Costs
  - Privacy Regulatory Defense and Penalties
  - Cyber Extortion
  - Voluntary Notification Expense
  - BrandGuard (Lost revenue due to Cyber Breach)
  - Network Asset Protection (System Failure & negligence)
- $100,000 for Cyber Crime (financial fraud, Telecommunications Fraud, Phishing Attack)

Our Experience

- We see both Crime losses and Cyber losses across all levels of our clients – Small, Medium and Large
- Cyber Criminals prefer Smaller to Medium sized businesses – these companies typically have lower security measures and they are heavily impacted by any crime loss or system hijacking or ransomware
- If you do nothing else after this panel please ask your broker to source both a Crime Insurance Quote and Cyber Insurance Quote – these coverages are cheaper than you think and really essential for our kind of business

Scenario 1 – The Confidential Transfer

- Our Insured was researching a purchase of a small company. The only people who knew about this confidential purchase was the owner, CEO and CFO.
- The Owner was going back and forth to the state where the target company was located.
- "Owner" send an email late on Friday asking the CFO to send $20,000 as earnest money for the purchase of the target company.
- On Monday when the owner got back home and the CFO asked how the purchase went things erupted.

Scenario 2 – Website Hijacking

- Our insured does a lot of business via their website and web portal. They interact with clients and service providers and provide tracking/tracing for shipments, etc.
- Hackers get control of the website with ransomware. They crash the site and demand a ransom of $15,000 to release it back.
- Our insured cannot afford the loss of the site or the potential embarrassment of the security breach so they pay the ransom.

Scenario 3 – Email Hacking

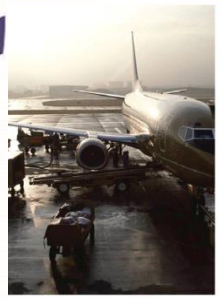
- Hacker gets into our insured's email server and reads emails for months, taking notes, recognizing patterns
- Hacker clones the email of the CFO – email looks exactly like the CFO's email but with a different back end IP address in Nigeria
- Hacker sends email from the CFO's email account to the payables clerk asking for immediate payment of an overseas bill and payables clerk complies – loss is almost $200,000

Risk Management

- Third Party Network Intrusion Testing and Periodic Inspections of your network for malware, etc.
- “Old School” two party payment confirmations for amounts over $$ - don’t use emails as the confirmations between these two parties as emails can be hacked
- Do not let traveling or trade show attending employees accept thumb drives or anything that hooks up to a work computer
- Don’t use free Wi-Fi without using a VPN or other network security features
- Change your passwords regularly

IFFCBANO
INTERNATIONAL TRADE
SYMPOSIUM
2017




Thank you for the opportunity to talk to you today