

# CYBERSECURITY AND CRIME INSURANCE IN THE ALTERNATIVES INDUSTRY:

## *BEST PRACTICES & MISTAKES TO AVOID*

# PRESENTERS



## MICHAEL BRICE

FOUNDER of BW Cyber Services

28 years experience providing technology, security, and related cybersecurity consulting solutions for multiple industries, including deep experience in the financial services industry as well as extensive experience supporting classified government operations. Received specialized training by the National Security Agency in Signals Intelligence. Former Marine Officer – served in the 1<sup>st</sup> Gulf War.



## PATRICK RILEY

SENIOR VICE PRESIDENT of Towne Insurance

Pat has over 30 years in the insurance industry serving in a variety of customer service, mid-level and upper management roles with both insurance companies and brokers. He currently works as a consultant and broker for a wide range of clients, with areas of focus in professional and management liability, cyber coverage, and crime insurance.

# CYBER INSURANCE – FOCUS FOR THIS WEBINAR

- Relationship between cybersecurity & insurance
- Discuss two critical cyber risks (Use Cases)
  - 3<sup>rd</sup> / 9<sup>th</sup> party data compromise
  - 3<sup>rd</sup> party wire fraud
- Provide guidance on key items of coverage
- Provide insight on industry standards per cost

# CURRENT SITUATION FOR “THE NEW NORMAL”

Rush to Remote Ops



IT Departments are told to do “whatever it takes” to get people connected from home

Chaos, Distraction, and Conflicting Business Processes



Kids, investors, markets, capital calls, margin calls, redemptions and wires, wires, wires

Then Comes “The Incident”



Ransomware, E-mail Hack, Network Breach Fraudulent Wire, 3<sup>rd</sup> Party Data Breach, 9<sup>th</sup> Party Data Breach

# A LOOK AT THE “STATE OF THE INDUSTRY” COVERAGE IN ASSET MANAGEMENT INDUSTRY

Registrants & Family Offices Ranging Between \$150m - \$5B AUM:

Crime policies  
(FI Bonds) are  
prevalent

Cybersecurity –  
50/50

Check the box

Not risk aligned

IT & cyber skills  
outsourced

# SO WHY AREN'T BROKERS DOING MORE?

- Trust relationship
- Cyber is relatively new
- Cyber/crime relationship is complicated
- There are complicated financial relationships:
  - Banks, GPs, LPs, Fund Admins, Investors, etc.
  - Outbound wires, Inbound wires
  - 3<sup>rd</sup> party wires (e.g., Fund Admin)
  - Internal data compromise (Sub docs are pure gold)
  - External (3<sup>rd</sup> & 9<sup>th</sup> party) data compromise

# SO WHY AREN'T FUND MANAGERS DOING MORE?

The impact of cyber breach, wire fraud, or 3<sup>rd</sup> / 9<sup>th</sup> party compromise is often not fully 'appreciated'



- ✓ Financial loss – covered
- ✓ Investigation
- X Financial loss – not covered
- X Reputation
- X Regulation
- X Legal reporting, reporting, reporting
- X Litigation
- X Executive distraction
- X ODD 'red flag'

# TWO PROMINENT INDUSTRY EXAMPLES

## Tillage Commodities

\$5.9m wire fraud loss

## Fund Administration

9th party data loss  
affecting a large group of  
asset managers



# FUND ADMIN WIRE FRAUD

- Typo Squat e-mail (“Tilllage” vs. Tillage) fraud against the Fund Admin
- Paperwork (e-mail) appeared correct...
- No voice confirm or double check on wire instructions
- \$5.9m gone...
- Compensation contractually limited to a portion of one year’s fees (standard language)
- Insult to injury – CFTC “Failure to Supervise” fine of \$150k
- Years of litigation

# “9<sup>TH</sup> PARTY” DATA COMPROMISE

3<sup>rd</sup> party of the  
Fund Admin  
(not the fund  
admins fault)

Data related to  
investors –  
reputational event

Months of  
investigation  
(cyber forensics)

Notifications

Attorneys

Reputation

# SO WHAT SHOULD YOU HAVE?

## CYBER INSURANCE SIMPLIFIED

- Cyber insurance modules (the basics)
  - Network privacy & security liability
  - First party cost including forensics, notification, fines, extortion costs, etc.
  - Business interruption, systems failure, and data recovery
  - Limited cyber crime including social engineering and funds transfer fraud
- What you MUST ask for
  - Maximum limit for social engineering \$250k-\$500k – some reluctance for financial institutions
  - Invoice manipulation
  - Specified service providers such as Forensics (e.g., BW Cyber Services)
  - Coordinate with crime
- Understand the claims process – don't wait for an event!

# BUT WAIT – THERE’S MORE...

## CRIME POLICIES SIMPLIFIED

- Financial Institution Bonds
  - Funds transfer
  - Social engineering
  - Other computer and electronic fraud
  - Be aware of authorization requirements
- What you MUST ask for from a cyber perspective
  - Maximum amount of social engineering \$250K - \$1M
  - Include losses from transfer instructions purportedly from you to another “financial institution”
  - Make sure fund administrator is included in definition of financial institution
  - Coordinate with cyber policy

# SO WHAT TO DO?

- Find a broker who knows cyber & asset management
- Perform an enterprise cybersecurity assessment to understand your specific risk profile
- Cyber policies (\$150m-\$5B AUM range)
  - \$1-\$3m
  - \$250k-\$1m sublimit on fund transfer & social engineering
  - \$5k-\$10k retention
  - ~\$3k-\$20k premium range
- Crime policy (same demographic)
  - \$1m-\$5m limits
  - \$10k + deductible
  - Funds transfer & social engineering \$250k - \$1m sublimit
  - ~\$4k-\$25k premium range



# THE BOTTOM LINE

- Executives need to understand the key business/financial risks associated with cybersecurity
- Not all cybersecurity policies are the same – you MUST know what to ask for
- FI Bonds (crime policies) may not mitigate some wire transfer losses – you MUST know what to ask for
- The market is competitive, you can and should seek competitive retention rates
- Your broker, with good intentions, may not be aware of some of these esoteric “Use Cases” that represent 6 & 7 figure financial risks

**Disclaimer:**

**Pat is a licensed broker and can provide insurance advice.**

**Michael is not licensed however he is providing insights based on BW Cyber Services and his personal forensic experiences where it was determined that cyber security insurance failed to mitigate the issue at hand.**



(646) 779-8976 | [www.bwcyberservices.com](http://www.bwcyberservices.com)

THANK YOU



(646) 779-8976 | [www.bwcyberservices.com](http://www.bwcyberservices.com)