EXECUTIVE RISKS

Crime Insurance Discovery Topics

Help your clients identify exposures and improve their risk profiles

Technology has created new opportunities for criminal activities. In today's world, crime happens faster, hits harder, and takes the form of both traditional and digital threats. Whether it's a cyber criminal or an honest mistake, businesses need protection for when the worst happens.

Crime insurance provides coverage* for financial loss and impacts due to various criminal activities, such as employee theft, funds transfer fraud (FTF), forgery, and fraudulent impersonation.

FTF is among the easiest and most prolific ways to monetize cyber crime, accounting for nearly one-third of all cyber insurance claims.[1] Digital threats often straddle the line between cyber risk and management liability risk. With Crime insurance, businesses can close potential coverage gaps and protect themselves against a variety of modern risks.

How to use this guide

We know that small businesses aren't always aware of the things putting them at risk — and many often think they're too small to need Crime insurance. That's why we're giving you the tools to help clients identify exposures and improve their risk profiles. We recommend using this guide to spark conversations with clients to ensure they're protected in the event of a business-related crime. It can also be a useful resource in preparing clients for questions on insurance applications and tailoring coverage to their specific business needs.

> Funds transfer fraud accounts for nearly **one-third of all cyber insurance claims**.

[1] Coalition, *2023 Cyber Claims Report*.

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **help@coalitioninc.com**

Crime Insurance Focus Areas

Accounting Procedures

Why this matters

Whether it's an employee with administrative authority or a cyber criminal who's found their way inside, access makes financial crimes easier to commit. Instituting a rigid system of checks and balances for accounting procedures can help businesses significantly reduce their risk of crimes like check forgery and employee theft.

Key talking points

- **Positive pay:** Positive pay is an automatic cash-management tool that helps businesses reduce their exposure to check fraud. It's typically provided by banks and will detect suspicious transactions before they are processed.
- **Owner reliance:** If the owner is the only person authorized to perform financial transactions, it can limit a business' exposure to criminal activities. These transactions include signing checks, making deposits and withdrawals, and reconciling statements.
- **Separation of duties:** Establishing a system where no one individual (other than the owner) controls the banking process can reduce the likelihood of a crime. Ideally, the person who handles deposits and withdrawals is someone other than the person who reconciles bank statements.

Claim example

A Missouri agriculture company lost $1.2 million after a secretary forged checks to herself from the business' checking account.*

Criminal Background Checks

Why this matters

Employees are often granted access to sensitive information and in a position to take advantage of a business. Whether theft or forgery, crimes committed by employees can pose a serious threat to businesses. Performing criminal background checks is a valuable and informative step in the vetting process when hiring employees.

Key talking points

- **Background checks for all new hires:** Criminal background checks are often most effective when consistently incorporated into the hiring process, similar to using employment applications or calling references.
- **Lower risk of theft:** If background checks are conducted on employees, there is typically a lower likelihood that an employee will commit a crime.
- **Federal compliance:** If a business wants to order criminal background checks from a third party, it should comply with the Fair Credit Reporting Act.

Proof point

34% of SMBs say they use background check services.[2]

[2] Coalition Executive Risks Survey, Wakefield Research, 2021

Approved Vendor Lists

Why this matters

Businesses should look beyond their walls and continuously monitor their relationships with third-party vendors. Any potential risks that stem from a vendor's operations can create exposures for a business. If a business works with many outside vendors, determine the process for vetting vendors, whether an approved vendor list is maintained, and how frequently the list is updated.

Key talking points

- **Prior to doing business:** Businesses should avoid doing business with a vendor until they have been thoroughly vetted for the following types of risks: cybersecurity, operational, compliance, reputational, financial, and strategic.
- **Background checks for vendors:** As with the process of hiring new employees, background checks are typically most effective at decreasing the risk of a crime when performed consistently and universally.
- **Building a list:** Once a vendor has cleared the vetting process, businesses should create a detailed list of all approved vendors to document the details of the relationship and ongoing activities. Things to track include: nature of relationship, size of contract, location, timeliness of payments, primary contact information, and access requirements.

Claim example

A barge shipping company lost nearly $600,000 after a threat actor posed as a third-party vendor and duped the accounting department into rerouting payments to a fraudulent account.*

Electronic Funds Transfer

Why this matters

Electronic Funds Transfer (EFT) is the leading method for sending and receiving digital payments. Thanks to phishing emails and social engineering tactics, funds transfer fraud (FTF) is also the leading event type for cyber insurance claims.[3] To mitigate the risk of digital fraud, it's important to understand the controls businesses have in place.

Key talking points

- **Cybersecurity training:** Employees are often a weak link in a business' security procedures. Teaching employees to remain vigilant and spot common FTF tactics, such as spoofed contact information and urgent requests, can be a good first line of defense.
- **Turn on multi-factor authentication (MFA):** Because many FTF events start with an attacker gaining email access, businesses are encouraged to turn on MFA for all corporate email accounts. This layered protection can block over 99.9 percent of account compromise attacks.[3]
- **Implement a "dual control" process:** Businesses are encouraged to require employees to call the recipient of the wire transfer to verify details, verify the transaction with an executive at the company verbally or in writing, and set up internal controls with the financial institution.

Proof point

The average loss amount for an FTF claim is $212,000 prior to recovery.[4]

[3] Microsoft, *One simple action you can take to prevent 99.9 percent of attacks on your accounts*

[4] Coalition, *2023 Cyber Claims Report*

Active Insurance for Executive Risks

Active Executive Risks Insurance is designed to help organizations mitigate the financial exposures and risks that can occur in the course of doing business. Every Active Insurance product from Coalition is powered by our proprietary Active Risk Platform.

Active Risk Assessment

We provide detailed insights into your clients' risks and empower you to become a trusted advisor on executive risks.

Active Protection

We scan your clients during the policy period for new and emerging risks and offer a robust suite of policyholder resources for added protection, including our pre-claims hotline.

Active Response

If a claim does occur, your clients receive comprehensive management liability coverage and award-winning claims handling.

Close coverage gaps by pairing Crime and Cyber policies

Businesses can enhance their protection against cyber crimes with both Crime and Cyber policies. Combining these two critical coverages helps policyholders protect against a broader range of risks and get the benefit of higher combined sublimits for certain claim types. Best of all, Crime insurance can be purchased on a standalone basis or packaged with our other Executive Risks products.*

DIRECTORS & OFFICERS LIABILITY (D&O)

Coverage for leadership exposure arising out of business decisions, like financial mismanagement or breach of duty.

EMPLOYMENT PRACTICES LIABILITY (EPL)

Coverage for employment-related risks, like claims of wrongful termination, discrimination, harassment, or retaliation.

FIDUCIARY LIABILITY

Coverage for claims of mismanagement of employee benefit plans, like legal defense costs, settlements, and damages.

Download our comprehensive Executive Risks guide

Support your clients by helping them navigate the ever-changing world of executive risks. Join us in our mission to protect the unprotected with Executive Risks insurance. Log in to our Broker Platform to start quoting or sign up to become an appointed Coalition broker.

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **help@coalitioninc.com**