Broker's guide to cybercrime risk management

Cybercrime is pervasive, persistent, and extremely lucrative. Coalition's claims data consistently shows that Funds Transfer Fraud (FTF) is one of the most frequent claims types. FTF often results from low-tech scams like phishing and is one of the easiest ways for malicious actors to monetize cybercrime. According to the 2023 Coalition Cyber Claims report, the average FTF loss was $212,264 prior to recovering funds. This is a significant loss for any organization and makes having the right protection against cybercrime—including insurance coverage and appropriate controls—a top priority.

How to use this guide

Your clients look to you for guidance on how to protect their business from a wide range of risks and threats, including cybercrime. Coalition developed this two-part guide to put you in the best position to advise your clients on key cybercrime risks they may face.

1. The first section includes a checklist of the core cybercrime coverage every business should consider to protect against the most likely cybercrime threats. This nonexhaustive checklist focuses only on the essential cybercrime coverages to make it broadly applicable to organizations of all shapes and sizes. The last two columns in the checklist are designed to provide suggested Coalition Executive Risks and Cyber Insurance insuring agreements that most closely align with each cybercrime scenario.
2. The second section is a nonexhaustive cybercrime best practices checklist that helps consolidate cybercrime protections, process and response recommendations to help you guide your clients' in cybercrime prevention and recovery.

Cybercrime coverage essentials[1]

				RECOMMENDED CYBERCRIME INSURING AGREEMENTS	
LOSS TYPES	SAMPLE CYBERCRIME SCENARIOS	COVERAGE TRIGGER	ACTOR	EXECUTIVE RISKS	CYBER
Employee theft	Theft of money, securities and property resulting from a theft or forgery committed by an employee.	Theft or forgery	Employee	Employee theft	N/A
Electronic theft of property	Theft of property resulting from use of a computer system.	Fraudulent use of computer	External actor	Computer fraud and Funds transfer fraud	Funds transfer fraud[2]
Electronic theft of money and securities	Fraudulent transfer of money and securities resulting from use of a computer system.	Fraudulent use of somputer	External actor	Computer Fraud and funds transfer fraud	Funds transfer fraud
Wire transfer fraud	Fraudulent wire funds transfers made by a cybercriminal.	Fraudulent instruction	External actor	Computer fraud and funds transfer fraud	Funds transfer fraud
Social engineering fraud	Losses from transfers, payments, and other transactions made by the organization because they were misled by a cybercriminal through misrepresentation of facts and/or social engineering.	Social engineering	Unwitting internal actor	Fraudulent impersonation	Funds transfer fraud
Invoice manipulation	Financial losses suffered by a third party when a cybercriminal gains unauthorized access to an organization's network, intercepts and manipulates invoices. As a result, the third party unknowingly pays the cybercriminal instead of the insured.	Security failure	External actor	N/A	Invoice manipulation
Service and telecom theft	Overage charges resulting from hackers gaining unauthorized access to technologies that are charged based on usage, such as shared computing resources, operational technology, and VoIP systems.	Security failure	External actor	N/A	Service fraud

1 The loss types, scenarios, insuring agreements and other references contained herein represent only a subset of the policy language and coverage options. Please refer to the policy for complete information on the coverages provided.
2 Theft of property resulting from funds transfer fraud is currently only available on the Coalition Insurance Company (CIC) admitted policy.

Best practices for cybercrime protection

Cybercrime defense

- Turn on multi-factor authentication (MFA) for all business applications, especially email.
- Implement advanced email security and threat protection solutions (see Coalition's recommendations in the email security section of the Coalition Control Marketplace).
- Ensure the email administrator for the organization has disabled the ability to auto-forward emails to an external domain.
- Conduct cybersecurity awareness training for all new hires and ongoing training for all current employees.
- Conduct regular phishing awareness simulation training.
- Follow Coalition's recommended cybersecurity best practices.

Cybercrime prevention - Making payments

- New payment requests: Implement a "dual control" process where all new payment requests are verified by calling the last known phone number for the person initiating the request.
- Payment instruction changes: Implement a "dual control" process where payment instruction changes are verified by calling the last known phone number (not supplied in the email) to the individual requesting the change.
- Establish a documented wire transfer process and templates to initiate a transfer internally and make a transfer to the organization's bank.
- Require the organization's bank to verify account ownership before initiating a transfer.
- Use a bank callback process that requires the organization's bank to request final authorization by phone before releasing funds.
- Verify all vendor and supplier bank accounts by a direct call to the receiving bank prior to accounts being established in the organization's accounts payable system.
- Require approval from more than one person to initiate a wire transfer in excess of $5,000.
- Regularly monitor bank activity and wire receipts to identify anomalous or fraudulent transactions.
- Only use financial institutions that require multi-factor authentication to log into any online account.
- Establish wire transfer blocks where possible - international transfers, other accounts, etc.

Cybercrime prevention - Receiving payments

- Remove routing and account numbers from invoices whenever possible.
- Establish a documented, standardized and repeatable process for sending payment instructions.
- Ensure payment transactions are not facilitated via email.
- Clearly communicate the organization's process for changing payment instructions to invoice recipients and request that recipients verify any changes with a method other than email.

Cybercrime response

- Establish process for employees to quickly escalate actual or suspected phishing or email compromise.
- Identify external providers (Legal, Forensics, Cybersecurity, IT, etc.) that will help the organization respond to a cybercrime event and coordinate providers with your cyber insurance and crime providers.
- Establish a process for employees to quickly escalate actual or suspected cybercrimes, fraudulent transactions or anomalous financial activity.
- Document internal communication, incident classification thresholds, and escalation strategies to help accelerate responses.

ABOUT COALITION

Coalition is the world's first Active Insurance provider designed to help prevent digital risk before it strikes. By combining comprehensive insurance coverage and cybersecurity tools, Coalition helps businesses manage and mitigate digital risks. Coalition offers its Active Insurance products in the U.S., U.K., and Canada through relationships with leading global insurers, as well as cyber capacity through its own carrier, Coalition Insurance Company. Coalition's Active Risk Platform provides automated security alerts, threat intelligence, expert guidance, and cybersecurity tools to help businesses worldwide remain resilient against cyber attacks.

Visit us at victorinsurance.com to learn more.

This document is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.

© 2023 Victor Insurance Managers LLC | 123861
Victor Insurance Services LLC in MN | DBA in CA and NY: Victor Insurance Services | CA Ins. Lic. # 0156109