CANNABIS NEWS YOU CAN USE
CANNABIS RISK MANAGER

Do You Need Crime Insurance if You Have Cyber Liability?

Understanding the Difference Between Crime Insurance and Cyber Liability Insurance

When cannabis business owners think about protecting themselves from modern threats, cyber liability insurance often comes to mind first. This makes sense the cannabis industry has embraced technology for seed-to-sale tracking, online ordering, and digital payments, which all open the door to cyber risks.

However, cyber liability insurance is not the same as crime insurance. While there is some overlap in the type of losses these policies can address, each is designed to protect against distinct categories of risk.

- **Cyber liability insurance** covers losses arising from cyber incidents, such as data breaches, ransomware attacks, and unauthorized network access.
- **Crime insurance** covers financial loss from criminal acts like employee theft, fraud, forgery, social engineering scams, and physical theft of cash or securities.

Understanding the difference is critical assuming your cyber policy will protect you from all theft-related losses could leave dangerous gaps in your coverage.

Why Cannabis Businesses Are Especially Vulnerable to Crime-Related Losses

The cannabis industry operates in a unique risk environment. Beyond the typical concerns of theft or fraud, the combination of high cash volume, strict compliance rules, and evolving regulations creates a perfect storm for crime-related losses.

Common crime risks for cannabis businesses include:

- **Internal theft** by employees, such as skimming cash or manipulating sales data.
- **External theft** of products or cash, often targeting dispensaries and distribution hubs.
- **Fraudulent transactions**, including forged checks or altered vendor payments.
- **Social engineering scams**, where criminals trick employees into transferring funds or sharing sensitive credentials.
- **Manipulation of inventory records**, especially in cultivation or distribution operations.

Cyber liability insurance won’t cover most of these scenarios if they don’t involve a cyber attack or a breach of data systems. Crime insurance, however, is designed specifically to respond to these situations.

Where Cyber Liability Ends and Crime Insurance Begins

A common misconception is that cyber liability policies automatically cover all digitally driven thefts. In reality, these policies are focused on protecting against **network and data breaches**, not direct financial theft unless it is clearly tied to a cyber event.

Here’s how the two policies differ in practice:

- **Cyber liability insurance may cover:**
    - Costs to investigate and recover from a data breach.
    - Legal expenses and regulatory fines after a privacy violation.
    - Ransomware payments and restoration costs.
    - Notifying affected customers and providing credit monitoring.

- **Crime insurance may cover:**
    - Stolen funds from fraudulent wire transfers initiated by a phishing email.
    - Losses from counterfeit money accepted at point of sale.
    - Inventory stolen by an employee or an outsider.
    - Forged signatures on business checks.

If a hacker steals your customer database, that’s a **cyber liability** claim. If an employee pockets $20,000 in cash from the register, that’s a **crime insurance** claim.

Overlap Isn’t Enough Why You Still Need Both

While it’s true that some cyber liability policies include limited coverage for certain types of financial theft (such as fraudulent funds transfer), these provisions often have slow sublimits sometimes only $10,000–$25,000 and come with strict requirements for proof.

Crime insurance typically offers broader definitions of covered losses, higher limits, and fewer exclusions for theft that happens outside of strictly digital environments.

For cannabis businesses, having both policies is similar to having both property insurance and general liability they complement each other, cover different scenarios, and close coverage gaps that could otherwise lead to significant losses.

Real World Example: How a Gap in Coverage Could Cost You

Consider a mid-sized cannabis dispensary that processes $300,000 in cash transactions each month.

- **Scenario 1: Cyber Loss**
  A hacker infiltrates the dispensary’s point-of-sale system and steals credit card data. The business faces breach notification costs, legal fees, and possible regulatory fines. Cyber liability insurance steps in to cover these expenses.
- **Scenario 2: Crime Loss**
  An employee manipulates inventory records, removes cannabis flower from stock, and resells it illegally. The loss totals $60,000 worth of product. Cyber liability insurance does not cover the theft because it is not the result of a cyber incident. Crime insurance would cover it.

In the second scenario, relying solely on cyber liability insurance would leave the business absorbing the entire $60,000 loss.

Regulatory Considerations for Cannabis Businesses

In cannabis, losses from theft or fraud are not just financial problems they can also trigger compliance violations. Missing inventory can raise red flags with regulators, potentially leading to audits, fines, or even license suspension.

Crime insurance doesn't just provide reimbursement; it also ensures you have the resources to respond quickly, investigate thoroughly, and demonstrate compliance with state tracking requirements.

Key Features to Look for in Crime Insurance for Cannabis

If you decide to add crime insurance to your risk management strategy, pay attention to the policy's scope and cannabis-specific adaptations. Look for:

1. **Coverage for employee theft** (including both money and product).
2. **Coverage for third-party theft** (robberies, vendor fraud, or burglaries).
3. **Social engineering coverage** for scams involving impersonation or manipulation.
4. **Forgery and alteration coverage** for fraudulent checks or documents.**Computer fraud coverage** to bridge small overlaps with cyber risks.

Some insurers have started tailoring crime insurance specifically to cannabis operations, accounting for high cash turnover, product tracking, and regulatory obligations.

Building a Layered Risk Management Approach

The best protection for a cannabis business comes from layered coverage. Cyber liability and crime insurance should be part of a broader insurance portfolio that may also include:

- **General liability** for bodily injury and property damage claims.
- **Property insurance** for physical assets like equipment and inventory.
- **Product liability** for claims related to the safety of your products.
- **Commercial auto** if your business owns or uses vehicles for deliveries.
- **Workers' compensation** for employee injuries.

Layering these policies helps ensure that no single gap can cause catastrophic financial harm.

Don't Assume Verify Your Coverage

Cyber liability insurance is crucial in today's cannabis industry, but it is not a substitute for crime insurance. The two policies are complementary, not interchangeable.

If you already have cyber liability coverage, review the policy language carefully to see what, if any, theft-related losses are included and whether those limits are realistic for your operation. In most cases, adding a dedicated crime insurance policy is the safest way to protect against the broad range of financial crimes that can impact cannabis businesses.

By understanding where one policy ends and the other begins, cannabis operators can make informed choices that protect their assets, maintain compliance, and safeguard their long term growth.

Email: info@cannabisriskmanager.com | Phone: +415-226-4060