

Digital Assets: Insurance's Critical Role

President Biden's March 2022 executive order establishing the beginnings of a regulatory framework for digital assets is an unmistakable signal that digital assets — in one form or another — are here to stay.

Like those in any industry, digital asset companies — and those in the digital asset ecosystem — face sizable risks. Just like more "traditional" businesses, digital asset companies' risks can be managed via commercial insurance. By transferring risk to an insurer, a company can free up capital and other resources to innovate and push the envelope in ways companies that retain all their risk cannot.

More broadly, the benefits of a well-developed risk management strategy will provide enhanced protections for individuals and businesses that engage with digital asset companies. That, in turn, will lead to additional stability for the digital asset ecosystem as a whole.

To enable the growth and innovation necessary to ensure their longevity, companies engaged in the digital asset ecosystem should consider maintaining seven key types of professional and management liability insurance coverages.

LOCKTON®

1. DIRECTORS AND OFFICERS LIABILITY (D&O) INSURANCE

D&O insurance, which many refer to as "personal asset protection," is often considered the last line of defense before an executive's personal assets are exposed for the payment of defense costs or a settlement or judgment. D&O insurance represents a meaningful tool companies can use to attract and retain highly qualified executives to run a company.

In addition to protecting the individuals running a company, D&O insurance can protect a company's balance sheet. Any major action your company takes — including an IPO, merger, coin offering, or decision to transact or invest in digital assets — can expose your company to litigation risk. At the same time, as the Securities and Exchange Commission and other agencies continue to develop a framework for digital assets, regulatory investigations and actions will remain a concern. Even if without merit, defending any litigation or regulatory action is costly.

2. CRIME/FIDELITY INSURANCE

The loss of assets is a risk for any business. But the potentially high valuation of digital assets is another reason why companies engaged in the digital asset space should consider protecting not only their own assets but those they may be holding for customers. In addition to insuring the theft of the assets themselves, having robust insurance makes it easier to attract customers, who will be more comfortable that they could be made whole should the company holding their assets sustain a loss.

Fidelity/crime insurance can protect against direct financial losses as a result of the theft, disappearance, or destruction of property, including digital assets and private keys. A crime policy can protect assets in a variety of environments, including cold, warm, and hot storage. Accordingly, crime coverage is one of the most often sought coverages in the digital asset space.

3. CUSTODY INSURANCE

Often purchased in conjunction with crime coverage, custody insurance — sometimes called "cold storage coverage" — is equally, if not more often, sought.

Custody insurance, available through the London specie market, provides coverage for the loss of digital assets (private keys) from physical loss and/or damage caused by natural perils, deliberate and dishonest acts, as well as third-party theft, all while stored in secure locations. While historically considered to apply only to those assets stored offline (air gapped), the specie market has broadened its appetite to include coverage for solutions related to Multi-Party Computation (MPC).

Like crime/fidelity coverage, in addition to providing coverage for the loss of assets, custody insurance typically plays a large part in the marketing process of those companies involved in custodying assets for third parties, offering another layer of protection for custodians and their customers alike.

4. CYBER INSURANCE

The uptick of cyber events in recent years — notably, the explosive growth in the frequency and severity of ransomware attacks — has affected all industries. Like more traditional companies, those in the digital asset space often collect and store personally identifiable information about their customers, which could leave them exposed to significant breach notification and business interruption costs in the event of an incident.

Cyber insurance coverage can protect against a variety of technology — and data-related exposures. A well-designed policy can respond to data breaches, ransomware attacks, technology-related business interruption, and other events that generate first- and third-party losses for insured organizations.

For digital asset companies, the failure of critical technologies and/or allegations of copyright or other intellectual property infringement is of concern. Cyber

coverage is often provided alongside technology errors and omissions (E&O) and media liability coverage. These coverages are often required either to fulfill a regulatory licensing requirement or some type of contractual obligation to a third party. Accordingly, in recent years we have seen a dramatic increase in the number of digital asset companies seeking these coverages — a trend we expect to continue.

5. ERRORS AND OMISSIONS (E&O)/PROFESSIONAL INDEMNITY (PI) INSURANCE

The rendering of professional services often gives rise to client claims alleging that incorrect, insufficient, or incomplete services resulted in financial harm. Claims related to technology-related errors and omissions in products and services (see above), in particular, are growing in frequency and severity for digital asset companies.

Professional liability insurance, also known as E&O coverage and/or PI coverage, can respond when clients or customers allege negligence or omissions in the delivery of professional services, giving both providers and customers peace of mind. As noted above with respect to cyber/tech E&O/media liability coverage, broader E&O coverage is not just desirable for professional services companies — it's often required in contracts signed by digital asset companies with clients, vendors and others.

6. KIDNAP AND RANSOM (K&R) INSURANCE

Within the digital asset space, private keys are often controlled by a few individuals, who could become attractive targets for a kidnapping event. The amount of wealth in the space also continues to grow to new heights daily.

K&R insurance is a form of specialty crime coverage that can insure against the threat or actual harm to specific employees and their families. Many K&R policies provide access to invaluable threat response services that are made available in the event of a kidnapping or ransom demand.

7. EMPLOYMENT PRACTICES LIABILITY (EPL) INSURANCE

Any company with employees can be subject to litigation or other claims relating to "wrongful" employment-related acts. While sexual harassment and discrimination claims have been in the spotlight since the #MeToo movement began in 2017, employers must also be mindful of employee claims of other forms of harassment and discrimination, retaliation, wrongful termination, breach of contract, failure to promote and more.

An experienced digital asset insurance broker can help you navigate a dynamic and limited but growing insurance marketplace and help you find partners that both protect your business and develop consumer confidence.

For some in the digital asset space, these risks can be magnified. True startups often do not have human resources departments or well-developed policies and procedures relating to employment matters. More mature digital asset companies, meanwhile, often have employees with relatively large compensation packages; in the event of an employment-related claim, the potential damages at issue could be significant.

For these reasons and others, EPL insurance can prove to be invaluable to companies in the digital asset space.

Choosing the right advisor

It is vital that companies in the digital asset space partner with the right advisors whether purchasing any or all of these important forms of coverage. An experienced and knowledgeable insurance broker can help you analyze and understand your specific risks and become an extension of your risk management team, helping you make important decisions about your insurance program. This includes determining what coverage to purchase based on your organization's risk exposures, how much coverage to purchase, and how to structure individual policies to best protect your organization and senior leaders.

An experienced digital asset insurance broker can help you navigate a dynamic and limited but growing insurance marketplace and help you find partners that both protect your business and develop consumer confidence. Working with a trusted insurance broker with knowledge of the digital asset space is particularly important now, as the demand for insurance is greater than its supply.

Every business' risk profile is unique, and its risk management structure should be as well. The right broker can help you explore the best ways to refine your risk management structure in light of market realities, including examining alternative strategies, including captives and reinsurance opportunities.

For more information, contact Lockton's Emerging Asset Protection (LEAP) team at LEAP@lockton.com.

LOCKTON®

UNCOMMONLY INDEPENDENT

lockton.com | © 2022 Lockton Companies. All rights reserved.