Digital Asset Insurance

Digital asset insurance can cover the costs associated with the theft, hacking or destruction of valuable digital formats. The type of digital asset that is covered and the compensation received when a loss occurs depends on the type of policy.

Digital Assets Defined

These days, almost every business operates online in one form or another. This requires information to be transmitted and stored. This information must come in digital form and can be anything from processing and storing credit card numbers to publishing data on a website.

Because these digital forms of information are often necessary to conduct business, they become assets to the company. Some digital forms are tied to a company's image to the public--such as a logo--while others relate to the business's ability to conduct business.

The online form that collects the customer's address, for example, makes the digital process of that order possible. So does the customer's details, such as their name and what they ordered. Therefore, both the website that collects the information, as well as the customer's details, become digital assets of the company.

The digital assets a company owns can come in many forms. Some other examples are:

- custom photos, videos or graphics
- proprietary software
- internal documents
- articles and white papers
- passwords
- social security and driver's license numbers

- email lists & more

Cyber Attacks on Digital Assets

Unfortunately, as businesses have moved more and more information online, hackers have increasingly taken advantage. Here are some alarming statistics regarding cyber attacks:

- there is a hacker attack every 39 seconds (*Security* magazine)
- hackers steal 75 records every second (Breach Level Index)
- the average cost of a data breach is $3.86 million (IBM.com)
- 300,00 new malware is created each day (hostingtribunal.com)

Sometimes, a digital asset is compromised in-house. In other words, cyber sabotage can come from a disgruntled employee or from a system or network failure.

In extreme cases of sabotage, a cyber criminal may hold the information they steal “hostage” until a ransom is paid. In 2019, for example, the computer files of Lake City, Florida were locked by hackers. The cyber criminals refused to release the data until they received payment of 42 bitcoin--worth roughly $460,000 at the time.

In another incident, Norsk Hydro, a Norwegian aluminum producer, had 22,000 computers taken offline by a cyber attack. The company spent over $62 million restoring their business operations after refusing to pay the ransom demanded by the attackers.

But cyber attacks are not limited to larger entities. Small businesses, who are often ill-equipped to thwart an attack, can become the target of digital assaults. Such events can be costly: A data breach, for example, can cost smaller merchants 40 to 50K in lost revenue and expenses.

Digital Asset Risk Transfer

Insurance protection for digital assets can help mitigate the financial risk of a cyber attack. Digital assets loss insurance, for example, can cover the financial costs associated with restoring or replacing company records or software. Cyber security insurance, on the other hand, can help cover liability expenses should customers' sensitive information be compromised.

In either case, both types of policies are tied to negative digital events such as a malware infection, data breach, phishing scam or other similar incidence.

Finally, it should be noted that in order for an asset to officially be classified as digital, it must be recorded on a distributed ledger called a blockchain.

Blockchain Technology

Blockchain technology is a type of database that uses blocks of information to record virtual transactions. Each transaction creates a new block that is added to the previous transaction, creating a digital chain.

The History of Blockchain Technology

The idea of blockchain technology was first presented in 1991. It was outlined by two researchers named Stuart Haber and W. Scott Stornetta. The pair wanted a system that could timestamp data and not be compromised. At the time, however, blockchain didn't seem to have a commercial purpose and the technology wasn't pursued.

All of that changed with the introduction of cryptocurrency. Today's most popular cryptocurrency, Bitcoin, was introduced in 2009 by an unknown person or group of people. It was introduced as a decentralized currency not controlled by a government or institution.

Because Bitcoin was set up to transact solely online on an open market, a system needed to be implemented that could prevent cyber attacks. Suddenly, blockchain technology had a real-world application.

Since its inception in 2009, Bitcoin has used blockchain technology to record, track and protect all transactions. It is the oldest and most common use of blockchain.

Blockchain Technology Explained

Blockchain is a type of database that uses chunks of information called blocks instead of cells. It's implemented by using numerous protocols.

One of these protocols is using a peer-to-peer network to distribute the information. This network, also known as nodes, grants equal access to all it's users.

When a transaction takes place on a blockchain, it's recorded on many computers all over the world. These computers communicate with one another in order to keep identical records. These records become permanent.

This makes hacking difficult since, should an anomaly occur, the other computers in the network will communicate back the correct details. The infected computer(s) will then self-correct.

In the case of this self-correction, the majority rules. This means that a hacker would have to control over 50% of the entire network in order to alter the ledger. With thousands of computers around the world on the blockchain, this becomes a nearly impossible task.

Another protocol of blockchain is the use of cryptography. Cryptography is a technique that secures the communication between two parties and, therefore, keeps the information private. This is the technology that allows Bitcoin to publish details such as the amount of a transaction while protecting the identities of the parties involved.

Applications of Blockchain Technology

When it comes to Bitcoin, the blockchain technology is differentiated further in that all transactions, since its inception, can be accessed at any time and by anyone in the world. While the parties involved in the transaction remain anonymous, other details such as the date and amount, can be viewed by the public.

When it comes to digital currencies like Bitcoin, blockchain technology also prevents double-spending. Double-spending is the act of copying a digital token and then using the copy while keeping the original.

While blockchain technology came to fruition to support Bitcoin transactions, it has applications beyond cryptocurrency.

Since blockchain allows data to be secured and unchanged, it can be applied to other digital assets and transactions. In the future, blockchain technology may be applied to protect and access medical records, IDs, banking details and more.

The value of its application beyond cryptocurrency has spawned blockchain technology companies that help commercial clients, such as banks, develop blockchain solutions for their businesses. With malware, data breaches and other cyber attacks on the rise, the use of this technology in commercial institutions is expected to grow.

Crypto Insurance

Crypto (or cryptocurrency) insurance policies cover certain losses related to cryptocurrency. These losses must be related to digital malfunctions or breaches, such as cyber attacks or system failures.

Crypto insurance came into existence due to negative incidents with cryptocurrency platforms.

For example, in 2018, $500 million of digital currency was stolen from the cryptocurrency exchange Coincheck. In 2014, former cryptocurrency exchange Mt Gox was hacked and lost $460 million.

These are just two examples of former cyber attacks against cryptocurrency platforms. With the attacks expected to continue, cryptocurrency insurance policies become more instrumental.

Crypto Insurance Coverage

Crypto Insurance can help mitigate risk related to digital currency. While it is most often used by cryptocurrency platforms, a handful of companies now offer insurance to the users of these platforms.

For cryptocurrency companies, a crypto policy typically covers losses sustained by cyber attacks. One example of this is to restore funds to its users when their crypto coins or tokens are stolen.

It can also pay out in the case of ransomware. Ransomware is when an attacker locks virtual data via encryption until a ransom is paid.

When it comes to cryptocurrency, hackers can attack the platform that supports the currency or individual account owners. For example, they can seize a user's account, called a crypto wallet, and encrypt the data. The data isn't released until the demanded ransom is paid.

The frequency and amount of ransomware related to Bitcoin and other cryptocurrencies is increasing. The total paid out in ransomware is well over a billion. Chainalysis, a blockchain analysis company, reported that ransomware attacks were up 311% in 2020 compared to 2019.

While there are many cryptocurrencies now on the market, Bitcoin is the most valuable and well-known. Because of this, 98% of ransomware payments are Bitcoin-related

Decentralized Insurance

A growing number of digital insurance companies are taking a nod from the Bitcoin industry. Like cryptocurrency, these companies are decentralized.

By using the same blockchain technology, they create pools of funds that are shared by all who participate. In order for a claim to be paid, a virtual consensus must be reached.

Digital tokens, or coins, represent value much the same way as physical coins represent a certain amount of currency. For the decentralized insurance industry, crypto insurance tokens, or coins, are used to represent an individual's participation in its policies.

Participants deposit these tokens, or coins, into a virtual wallet or smart contract. The funds contributed by all become the pool of which an approved claim is paid. It is in this sense that crypto insurance coins (or tokens) mimic the traditional insurance premium.

Crypto insurance is also offered by a handful of traditional insurance companies as well. While most traditional companies currently steer clear of these types of policies, that could change in the upcoming years. With the growing use of cryptocurrency and blockchain technology, as well as the rise of ransomware demands, the insurance industry is sure to adapt.