
COVERAGE
MATTERS
WORKING WITH INSURANCE
INSIGHTS SEP 2025

New Frontiers: Insuring the Value of Lost Data

In the digital economy, data is currency. For traditional financial institutions and fintech companies, the value of data—customer credentials, transaction histories, private keys, smart contract code—is not just operational; it is existential. Yet, as the volume and sensitivity of data grow, so too does the risk of loss, theft, or misuse. And while cyber and crime insurance have evolved to address many traditional data breach and theft of assets scenarios for all kinds of businesses, they leave largely untouched the loss of digital assets and, more widely, lost (or stolen) data.

This article highlights some recent UK legal developments in the legal status of data, specifically digital assets as "property", and then looks at challenges and possible solutions involved in insuring it.

First, A Quick Legal Update

The UK's legal framework is beginning to catch up with the new realities:

- Relevant to the cyber market, the Data (Use and Access) Act 2025 introduced updates to the UK GDPR.
- Relevant to the Financial Institutions' ("FI") market, the Financial Services & Markets Act 2000 (Cryptoassets) draft Order 2025 has started the move towards an established regulated framework for crypto assets including stablecoin (ie cryptocurrency pegged to an established currency such as USD).
- We also have the new Property (Digital Assets etc) Bill 2025. It is this which has prompted the discussion in this Newsletter: digital assets will be officially recognised in English law as "property". This marks a significant step in recognising the economic and legal value of certain data. The Bill complements the other regulatory developments mentioned above, which is intended to help create a more coherent and supportive legal framework for digital and decentralised technologies.

The Legal Landscape: Data as Property

The Property (Digital Assets etc) Bill 2025, when it becomes law (see below), will represent a landmark shift in UK law, addressing the growing need to legally recognise and protect digital assets such as cryptocurrencies, NFTs, and other blockchain-based tokens. Traditionally, UK property law has only recognised two categories of "personal property": things in possession (physical items) and things in action (rights enforceable through legal action). However, digital assets do not fit neatly into either category, creating legal uncertainty around ownership, transfer, and enforcement.

This Bill introduces a third category of "personal property", ensuring that digital assets are not excluded from legal protection simply because they are intangible or novel. By doing so, it provides statutory confirmation that digital assets can attract property rights, aligning the law with technological innovation and the realities of modern finance.

Don't be fooled by the term "personal" property: it embraces all business ownership too. For businesses, especially in the fintech and digital asset sectors, the Bill offers clarity. It enables digital assets to be used as collateral, included in estate planning, and, vitally for our purposes, protected by property rights in cases of loss, theft or fraud.

The Bill does not define what a digital asset is – this will be left for courts to decide. I can see this being a fertile area for lawyers!

The Bill is currently in the UK House of Commons, having completed its second reading on 16 July 2025. If it continues to progress smoothly, it is expected to receive Royal Assent later this year or early 2026, officially becoming law in 2026.

Insuring Data as Property

The Bill only applies to digital assets not to data more generally. Once officially established as property, ownership of digital assets can properly be protected in law with rights being fully enforceable in the same way as for tangible property or rights under a contract. This means in theory you can insure it much like any other property – physical or otherwise.

Data is valuable. Where is it covered?

We have cyber policies that cover us for the legal or financial consequences of losing or misusing data, whether through malicious or non-malicious means, such as the costs of recovering it and the legal/regulatory fallout. To the extent the loss of data causes a business interruption this may also be covered. So, the consequences of losing data are fully taken care of. But you won't find any cyber policy covering the value of the lost data itself.

What about crime policies? I wrote about crime insurance in our September 2023 Newsletter *here*. There firstly needs to be a crime of a nature covered under a crime policy. For instance, theft or "social engineering" or documentary fraud are likely to be covered, but in relation to what assets? Typically, they will be money, securities or valuable property whether in physical or electronic format. Data will not be included in that list. If there is no restriction on the type of asset (like, for instance, with internal crime) there is likely to be an exclusion for data, digital assets, and all other valuable assets that exist solely in an intangible form such as intellectual property rights and confidential information. Loss of data via a crime is not intended to be covered. If you look at the valuation clause it will state that damaged or lost data as a result of a covered crime will only be covered to the extent of the costs required to reconstitute it, nothing more.

What about property insurance? Physical loss or damage to computer hardware and storage media will be covered. Similar to cyber, you may find coverage for the financial consequences of losing data too. However, the direct losses from a cyber incident are likely to be excluded (because they are covered under cyber), and, like the other policies mentioned above, nowhere will you find cover for the value of lost data.

There are specialist "cold storage" policies available in the specie market where crypto assets have been placed under the care of a regulated custodian – generally covering the custodian for loss of the crypto assets under its care and control. These policies, which contain very strict requirements on the part of an Insured, are not common and are certainly not available to the "owner" of the crypto asset directly – presumably due to the risks of poor data governance (eg failing to secure the private key properly: there are stories in the press about people losing their private keys all too often).

So, at present, the answer to the question therefore seems to be "none of the above" with historical limitations in insuring clauses and policy exclusions yet to adapt to evolving client exposures and legal developments.

The Data Dilemma in Insurance

What are the challenges facing insurers when looking at insuring data?

Data Generally

We are all personally protected if "our own" data is misused by someone who acquires it (lawfully or unlawfully), via the UK GDPR and its offshoots. These are not "property" rights as such, but rights enshrined in statute and regulations. Their value is indefinable, but a breach of such rights may permit us to seek recourse through the courts and there will doubtless also be regulatory sanction. A cyber policy will typically provide cover to organisations who inadvertently breach privacy law.

Does anyone need to insure against lost data? I am no IT expert, but data is almost always recoverable if you spend enough money with the right people. Unlike some physical assets, it can be replicated multiple times at little cost with no loss of integrity or quality. You might need experts to do this where the data does appear to have genuinely disappeared, but mostly it will be recoverable. So, the existing cyber (malicious and non-malicious loss) and crime policies (where there is a crime) will likely provide all the cover you need here. Cyber will likely also provide you with access to the experts you need.

What about the financial consequences of *leaked* data? In this scenario it is not "lost" – you still have it – but so now does someone else (or multiple parties) so the *value* of that data to you may be fundamentally compromised. It's easy to see that if a company inadvertently shares a trade secret this will cause financial harm, and there may be no recourse against anyone through the courts. This appears to be an area where there is no generally available cover. You might go to an insurer for an IP policy to help protect your IP rights, if you have any, but even this is unlikely to cover anything other than the consequential losses of losing an exclusive right to something. It will not cover the value of your lost rights. The position with *theft* of a trade secret or IP right is slightly different – the organisation will have recourse in the courts against the perpetrator, assuming they can be found, even if there is no insurance cover.

Digital Assets

Some types of data might only be held in a single or unique place, which if lost or stolen, could give rise to a genuine loss because it will be irreplaceable. Digital assets fall into this category. A private key, for instance, is not merely a credential; it is the sole means of accessing and transferring digital assets. If stolen, it cannot be revoked or reset like a password. Similarly, smart contract code governs the execution of financial agreements. A flaw in that code can result in irreversible loss of funds.

The value of such data can potentially be immense. In 2024 alone, some $2.2 billion in digital assets were lost globally due to smart contract exploits, phishing attacks, and wallet breaches[1]. In many cases, the root cause was not a failure of infrastructure but a failure of data governance—poor key management, inadequate access controls, or insecure APIs.

Unlike traditional financial services, where data is often stored centrally and protected by layered security protocols, crypto and Decentralised Finance (DeFi) platforms operate on decentralised infrastructure. This creates a radically different risk profile. In these environments, data is not just a record of transactions—it is the asset itself. Now that the asset will soon be recognised as “property” surely there is an even more compelling need to be able to insure it.

Yet, as mentioned above, despite the potential for lost value, most insurances will not provide coverage for them.

Quantifying the Value of Data

One of the key challenges in insuring data-related losses is valuation. How do you quantify the value of the data asset in the first place? As mentioned above, some values might be colossal. Others might be measured more in terms of the lost opportunity value that results from no longer being able to utilise the data, a hugely problematic scenario to quantify, and might be viewed as being too remote.

———————————

[1] https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/

Some insurers have begun experimenting with parametric models, where payouts are triggered by predefined events (e.g., a smart contract exploit exceeding a certain threshold). Others are exploring data valuation frameworks that consider:

- The market value of assets linked to the data (e.g., crypto holdings).
- The revenue impact of data loss or corruption.
- The reputational harm and customer attrition resulting from a breach.

However, these approaches remain nascent, and there is no industry consensus on how to price or underwrite such risks.

Another objection might be moral hazard (the risk of an insurance scam or other abuse of the policy proceeds) or the failure to take reasonable care of the asset in the first place due to poor data governance. These are legitimate concerns, but the industry has always found ways to mitigate these issues in the past.

Insurance Gaps

In this article we've established the following potential gaps in the insurance armoury as of today:

- Covering lost digital assets as property
- Covering the value of compromised confidential information, IP or trade secrets

We've also established there is potentially plenty of cover "around the edges" of these things and data more generally, such as for costs. Soon there will be stronger recovery rights in law – once the Property (Digital assets etc) Bill 2025 becomes law next year. We are surely edging closer to a day when the value of the assets themselves will be covered.

There are a couple of approaches to products that might help us do this, ensuring that the interests of all parties to the insurance contract are in balance. These could include a combination of the following:

- covers with capped limits or coinsurance percentages per incident;
- data valuation clauses that prescribe cover for lost value pursuant to a calculation;
- conditions which automatically reduce the payout by a specified percentage or impose a lower sub-limit for each precaution not followed; and
- strong subrogation rights or maybe cover only on a "net loss basis" once reasonable efforts have been made to enforce recovery rights.

Contrary to what I sometimes hear, the Insurance Act 2015 did not outlaw warranties nor conditions precedent – so long as they are proportionate in the circumstances. Section 11 provides that where the breach of a warranty or CP could have increased the risk of the loss occurring, the courts will allow the insurer to enforce it. Such clauses could play a central role here to help protect insurers from weak risk management on the part of an Insured, but still allowing coverage for genuinely fortuitous loss.

Despite the challenges, there are signs of innovation. Some London market syndicates are developing bespoke policies for crypto custody providers, DeFi platforms, and fintechs with high-value data assets. These policies may include:

- Digital asset crime cover, including theft of private keys.
- Smart contract failure cover, including coding errors and exploits.
- Data valuation endorsements, allowing for agreed-value settlements.

There is also growing interest in captive insurance and risk pooling among fintech consortia, particularly where commercial insurance is unavailable or unaffordable.

Conclusion: A Call to Action

Finding ways to insure the value of lost data will become a business imperative for both buyers and sellers of insurance.

Closing the coverage gap will require:

- Legal clarity on the status of data as property. 2026 should see that addressed.
- Regulatory clarity on insurability and enforcement risk.
- Underwriting and wording innovation to address valuation and claims complexity.
- Broker advocacy to ensure clients understand their exposures and options.

In a world where data is money, the cost of being uninsured, whether knowingly or unknowingly, is no longer theoretical—it is existential. ■