LOCKTON

Cyber and Technology

SPOILAGE: CYBER PROPERTY DAMAGE



Protecting against spoilage losses resulting from cyber attacks

A successful cyber-attack can carry devastating impacts, including the interruption of business operations, affected balance sheets, damaged reputations, and physical damage to buildings and facilities. But attacks can also lead to damage to raw materials, finished goods, or inventory – a type of loss known as spoilage.

The food and beverage industry is highly exposed to spoilage losses, owing to high levels of exposed stock. However, similar risks apply to any business that sells or transports perishable products, including pharmaceutical and life sciences, manufacturing, healthcare, agricultural and farming, chemical, and hospitality.

As cyber-attacks continue to increase in frequency, protecting against spoilage losses has never been more paramount. However, these losses are often excluded under traditional property and cyber policies, underlying the need for businesses to consider bespoke insurance solutions.

Understanding cyber-related spoilage losses

Common examples of cyber-related spoilage losses include:

Example 1 (direct loss)	A threat actor infiltrates the network of a grocery chain and switches off the refrigeration systems at multiple locations, causing all fresh product to spoil.
Example 2 (direct loss)	A threat actor infiltrates the network of a chemical company and switches the formulas that are used to produce certain products, leading to chemical production going to waste.
Example 3 (indirect loss)	A threat actor infiltrates the network of a supermarket chain and encrypts the whole network, leaving the firm unable access systems including warehouse management, logistics, and point-of-sale. The firm is unable to sell any of the available products, causing the goods to spoil.
Example 4 (indirect loss)	A logistics company experiences a cyber incident that disrupts its ability to locate inventory and fulfil deliveries within required timeframes, resulting in perishable goods expiring before they can be delivered.

Authorised and regulated by the Financial Conduct Authority. A Lloyd's broker.
Registered in England & Wales at The St Botolph Building, 138 Houndsditch, London EC3A 7AG. Company No. OC353198.

Potential costs of spoilage

If a cyber-attack leads to spoilage, businesses may incur direct costs in the form of any interruption to business, as well as the cost of replacing the spoiled goods.

However, spoilage can also lead to expensive additional costs. Notably, businesses may incur substantial costs associated with the disposal of spoiled goods, including the cost of engaging specialised waste management providers to collect and dispose of the materials safely and in compliance with regulations.

Consider example 3 (above). Where a supermarket chain operates 1,000 locations, even a moderate disposal cost incurred at each site can result in a very substantial overall financial impact when aggregated across the business.

Is cyber-related spoilage insurable?

Nearly all property insurance policies typically exclude cover for cyber-related losses, meaning that coverage won't extend to physical damage – including spoilage – or any ensuing business interruption caused by a cyber-attack. Likewise, cyber insurance policies do not typically provide cover for physical damage to property or goods, nor any ensuing business interruption and additional expense.

Despite this, solutions are available for businesses looking to protect thefmselves against cyber-related spoilage. Cover is available via the London cyber insurance market, either on a standalone basis, or by buying back the exclusion within traditional cyber policies.

At Lockton, we have several bespoke cyber property damage solutions that ensure businesses are covered when they suffer physical damage via cyber-attacks. These solutions will reimburse businesses when a cyber-attack either directly or indirectly results in spoilage.

The cyber insurance market is particularly flexible, with the ability to design tailored solutions that reflect your operations, risk profile, and unique business needs. By engaging early, businesses can explore bespoke cyber property damage cover that helps close critical gaps – providing confidence that spoilage losses triggered by cyber incidents are properly protected.

If you believe your firm may have an uninsured exposure, or for more information on the topics discussed above, reach out to a member of our team.

Let's Talk!



Carlo Ramadoro | Head of Cyber and Technology

T: +44 (0)7760 690 637

E: carlo.ramadoro@lockton.com



Jack Matthews | Senior Vice President | Cyber and Technology

T: +44 (0)7876 847 489

E: jack.matthews@lockton.com



Toby Graham | Assistant Vice President | Cyber and Technology

T: +44 (0)7769 424 948

E: toby.graham@lockton.com