

Protect Yourself with Crime Cover



You may think that your employees would never steal from you or that your business would never be the victim of theft, but the harsh reality is that nearly every business is eventually victimised by fraud or theft.

Thieves (including your employees) do not need direct access to cash to steal from you—merchandise, supplies and securities are all vulnerable. Criminals can steal finished products or even raw materials without your knowledge. Make no mistake: Any product can be a target if there is an opportunity to make a profit, which is why you need crime cover.

Internal Crime

There are two main types of crime threatening your organisation: internal and external. Internal crime is perpetrated from within your organisation and is dangerous because it is so insidious—depending on the situation, it may be difficult to detect, especially if your employees are skilled at disguising it. That is why constantly scrutinising your accounting processes is so important. The following are examples of some of the most common strategies for internal crime:

- Keeping two sets of books or removing ledger sheets to cover up shortages
- Stealing cash, merchandise and materials
- Charging inactive accounts
- Paying bonuses to those who should not get them
- Increasing amounts on cheques and invoices after they have been paid

- Paying bills to companies that do not exist and then cashing those cheques
- Padding payroll and cash expenditures
- Not crediting cash payments
- Invoicing materials below sale price and receiving the undercharge from the customer

External Crime

Internal crime is not the only crime exposure your organisation faces—external criminals also pose a serious threat. External criminals can steal from you either in-person or online. As businesses rely increasingly on digital technology, the threat of computer fraud increases. Not all crime policies cover computer crime, but it is a growing trend as the frequency of cyber-crime continues to rise. Some common examples of external crime include:

- Using computers to hack into your system and transfer funds, steal sensitive financial data, etc
- Purchasing goods by way of identity and card fraud
- Scamming your business using counterfeit money
- Stealing company property and money, either online or in person

Insurance Solutions to Combat Crime

Crime cover is becoming increasingly common and necessary. Depending on your organisation, the clients you serve may even require you to possess crime

Provided by Sirelark Risk Services

The content of this Cover Overview is of general interest and is not intended to apply to specific circumstances. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly. © 2008, 2012-2013, 2016 Zywave, Inc. All rights reserved.

Protect Yourself with Crime Cover

cover—especially if you hold their stocks or monies. Crime cover is typically sold as a comprehensive policy, which may or may not include computer and funds transfer fraud and other types of cyber-crime.

Comprehensive Crime: Protects against loss of money and securities by way of external and internal theft, fraud, forgery, dishonesty, disappearance or destruction while the property is on your business and/or banking premises.

- Protects against loss to other property in a safe or vault from an attempted or actual robbery within your premises.
- Outside of your premises, cover protects money, securities and other property in the care of a messenger.

Computer and Funds Transfer Fraud Cover: Protects against loss of money, securities and other property via computer fraud.

- Covers money that is directly related to the use of a computer to fraudulently cause a transfer of property from your premises or banking premises to someone or some entity outside of your premises.
- Pays for the loss of money through fund transfers communicated to a financial institution.

Other Safeguards Against Crime

In addition to obtaining crime cover, try implementing these safeguards to better protect your business:

Internal Crime Safeguards:

- Limit employees' access to storage areas.
- Inspect merchandise and goods thoroughly when they are received as shipments.

- Ensure that there is more than one employee inspecting outgoing and incoming shipments.
- Conduct periodic inventory counts, and compare that information to your records.
- Implement a concrete strategy for handling returned merchandise.
- Establish a line of authority at your organisation, and ensure that everyone is acting responsibly.
- Separate your accounting and operating functions.
- Create a 'paper trail' for each transaction.

External Crime Safeguards:

- Secure raw materials, semi-finished goods and finished goods in walled, fenced or locked areas on your premises.
- Invest in robust premises security to deter potential thieves.
- Rely on free resources from [the Information Commissioner's Office](#) to boost your cyber-security.
- Shred documents with sensitive financial data to prevent thieves from accessing them.
- Undertake periodic crime risk assessments to uncover any vulnerabilities you are not addressing.

Crime can be sneaky and difficult to address, which is why it is imperative that you take the necessary measures to protect your business. Contact Sirelark Risk Services at 01603 343 053 today to learn about how we can fortify your business against crime—no matter where it comes from.