Criminal Financial Loss Claims Examples

EMERGENCE

Cyber insurance helps business recover after a cyber event. Businesses are increasingly reliant on technology, digital products and third party services to conduct their operations. This further emphasises the need for cyber protection as part of their risk mitigation strategy. Increasingly, businesses are suffering from financial loss arising from criminal fraud.

Our Cyber Event Protection insurance provides the ability to provide cover to manage exposures such as:

- Cyber theft
- Socially engineered theft
- Telephone phreaking
- Cryptojacking

Example	Claim Scenario	Cyber Event Protection Solution
Socially Engineered Theft 1st Party Loss	An accountant's employee receives a request from a regular supplier's email address for payment of an outstanding invoice. The employee pays the supplier in good faith and in reliance upon the received invoice. As it turns out, the supplier's invoicing system was hacked and the supplier's bank account details were changed to the hacker's account. The paid amount is unrecoverable as a result.	If the accountant's policy includes Optional Cover for Criminal Financial Loss including Socially Engineered Theft, the direct financial loss to the accountant is covered, including investigation costs.
Socially Engineered Theft 3rd Party Loss	A real estate agent holds third party money in trust. The agent receives instructions from a lookalike email address to transfer money to the third party's bank account. The email is fraudulent. The agent transfers the money and, as a result, the third party funds are lost irrecoverably.	If Criminal Financial Loss coverage including Socially Engineered Theft is applicable, the lost third party funds are covered. Investigation costs are also covered.
Socially Engineered Theft 1st Party Loss	A medical centre received communications from a fraudster impersonating the ATO requiring urgent payment of outstanding taxes. The medical centre paid the 'outstanding' taxes in good faith having believed the demand was genuine.	If Criminal Financial Loss coverage including Socially Engineered Theft is applicable, the lost funds are covered including investigation costs.
Cyber Theft Business e-mail Compromise	The CFO received a fraudulent email from the CEO, whose e-mail account has been compromised due to a Cyber Event, requesting the transfer of a large sum of money. The email convinced the CFO to transfer money to a third party bank account. Later its determined that the email was not authored by the CEO, but it's too late for the bank to stop the transfer.	Cyber Event Protection will cover forensic investigation of the crime as well as response costs to remove the threat and secure the e-mail system. If Cyber Theft coverage is applicable, the direct financial loss the insured suffered will be covered as well.
Telephone Phreaking	A marketing firm's phone system gets hacked. The hacker creates a mailbox to route calls overseas. The unauthorised international calls result in thousands of dollars in call charges.	The policy covers the cost to investigate and remove the threat to firm's telephone system. Our optional Cyber Theft and Telephone Phreaking Cover pays the direct financial loss to the insured.
Cryptojacking	A legal firm noticed their computers are running slower than usual. Upon further investigation, someone has hacked into their IT infrastructure to utilise the processing power to mine cryptocurrency.	Cyber Event Protection will cover response costs to remove the virus. If Criminal Financial Loss coverage is applicable, the increased bandwidth and electricity costs are also covered.

Disclaimer:

These claim examples illustrate the potential scope of coverage provided under Emergence's EME CEP-003.1 Cyber Event Protection policy wording. Each claim is different and outcomes may vary on a case by case basis depending upon the facts and details of the particular situation.