MARSH

Financial and Professional Practice

INTERACTION OF COVERAGE UNDER FINANCIAL LINES POLICIES

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

INTERACTION OF COVERAGE UNDER FINANCIAL LINES POLICIES*

In this document we provide a brief overview of the most common financial and professional insurances that can be purchased by companies. We also highlight the areas where policies can overlap, and the differences in cover.

A good example of how policy responses can differ is when social engineering[1] fraud occurs. This can raise interesting coverage questions relating to the policies that companies purchase, and how and when they respond to loss from a "scam".

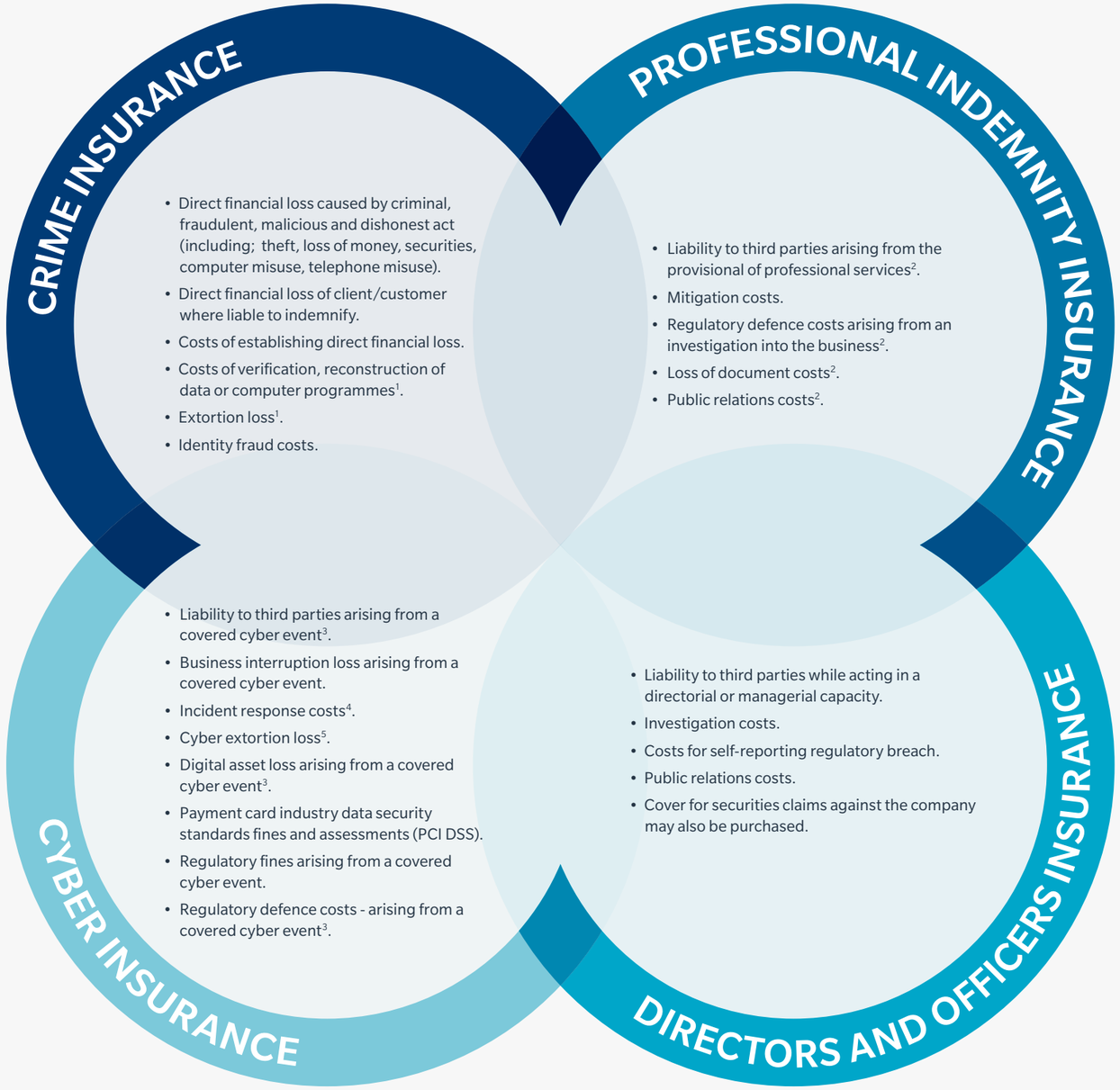
A social engineering fraud can be carried out online, over the telephone, or even in person. Where such a fraud results in the theft or compromise of data, and/or malware being introduced or transmitted to computer systems, the cyber policy may respond to any resultant third party liability, and associated breach response costs. It may also respond to specific first party losses suffered by the insured, including payment card industry (PCI) fines and assessments, costs to restore data, and any business interruption loss suffered due to computer system interruption. However, where the fraud involves theft, or loss of money or securities, this will not ordinarily be covered by the cyber policy. The direct loss to the insured arising from a theft, or loss of money or securities, is more likely to be covered under a crime policy.

The fraud described above may also lead to a risk of litigation against the insured's directors and officers. Although some cyber events will be beyond a company's control, board members may be found to have been remiss in their duty to review the organisation's risk practices. This can include not providing adequately for network breaches, business continuity planning, insurance coverages, and not disclosing material cyber risks or incidents to stakeholders. Such scenarios could leave senior individuals exposed to regulatory investigation, shareholder litigation, and possible reputational damage. Those exposures should be addressed by a directors and officers (D&O) policy, but any direct loss would not be covered and neither would the costs of dealing with the breach.

Finally, there is the situation when the fraud results in a professional negligence claim – for example, if data belonging to a third party or an employee is stolen. Any resulting damages or defence costs incurred would normally be covered under a professional indemnity (PI) policy, and, as set out above, may also be covered under a cyber policy. In regard to a data breach, the cyber policy may also cover the costs of notifying affected parties and/or dealing with the immediate aftermath of the breach, however, the PI policy would not ordinarily cover such costs.

Companies need to be aware of how policies are triggered, and the specific losses each type of cover is designed to address.

1 Social engineering is when fraudsters employ a variety of techniques to elicit information, and trick individuals into voluntarily performing actions that allow access to a company's money, securities, or intellectual property.



WHICH TYPE OF INSURANCE DO YOU NEED?

First and third party insurances both protect an insured from events which can have an impact on their balance sheet. The difference between the insurances lies in how the financial loss to the insured is sustained.

First party insurance is predominantly purchased to protect insureds from loss which they sustain directly – such as, when money is stolen.

Third party insurance is purchased to provide protection for financial or legal claims that an insured may face from a third party. Loss from a third party claim is sustained indirectly, as it is the third party's claim for its own loss which then impacts on the insured. A third party claim usually arises in connection with the actions of the insured – such as, an allegation that the insured did not provide adequate professional services.

Company risk managers and insurance buyers need to be clear on the differences between first party and third party insurance policies, and how these will respond to different types of claims.

Misunderstanding could lead to the wrong insurance being purchased, resulting in lack of cover for a loss. If you are unclear on the best insurance option for your risk, please speak to your Marsh contact.

* DISCLAIMER – This information is intended as general guidance only. Please ensure that you check your specific policy terms and conditions.

1 May be overlap with cyber insurance.

2 May be overlap with cyber insurance.

3 May be overlap with PI/liability insurance.

4 Including: IT forensics, PR costs and privacy breach response - notification, call centre, credit and ID monitoring and legal costs.

5 Ransom payments, and investigation and response costs.

MARSH

For further information, please contact one of our experts below, your local Marsh office or visit our website at marsh.com

CRIME INSURANCE

ELENI PETROS
FINPRO UK
+44 (0)20 7357 1507
eleni.petros@marsh.com

CYBER INSURANCE

DAVID ARNOLD
FINPRO UK
+44 (0)20 7357 1759
david.arnold@marsh.com / cybershield@marsh.com

PROFESSIONAL INDEMNITY INSURANCE

GEORGE GEORGIOU
FINPRO UK
+44 (0)20 7357 3791
george.georgiou@marsh.com

DIRECTORS AND OFFICERS INSURANCE

EMMANUELLE TARDY
FINPRO UK
+44 (0)20 7357 3768
emmanuelle.tardy@marsh.com

GRAPHICS NO. 16-1331