MARSH

CYBER PRACTICE

Drawing the line between traditional Crime and Cyber Crime

Social engineering fraud is widespread, increasing at an alarming rate as fraudsters remain persistent and relentless in the pursuit of their crimes. For organisations that fall victim to an attack, the financial consequences can be devastating.

The Australian Cyber Insurance Market is still in its infancy. As such the purchase of cyber insurance has been slow, although since late 2017 and into 2018 Marsh has seen a notable growth in the take-up of Cyber insurance. Despite this recorded growth in the purchase of cyber insurance, there remains a significant number of organisations that are not insured, via a dedicated stand-alone policy, for their cyber risk exposures. One of these key exposures arises from cyber crime.

The most prevalent cyber crime incidents are emerging from social engineering fraud:

Social engineering is the art of manipulating human behaviour to use the target to unintentionally reveal sensitive information or perform actions that compromise the security of networks, to obtain unauthorised access to a system for financial gain[1].

1 Combating Social Engineering Fraud – A guide for Chubb Insureds

In July 2018, the FBI issued a Public Service Announcement which included statistical data from the Internet Crime Complaint Centre, highlighting that between October 2013 and May 2018 there was USD12.5b lost worldwide in funds being transferred as a result of social engineering fraud[2].

It is evident that there is growing confusion pertaining to the differences between Crime protection insurance in its traditional form and insurance coverage for cyber crime that may be provided under a Cyber insurance policy.

Given the significant financial impact that a social engineering incident can have on an organisation, understanding possible insurance coverage is important for businesses and raises interesting questions on the interaction of various policies and how they may respond to a loss as a result of a 'scam'.

Social engineering fraud typically originates from criminals leveraging duplicitous emails or phone calls to request the transfer of funds from legitimate accounts to their own. One of the most common examples of social engineering is the 'fake president/ CEO' fraud – impersonation of a senior executive or CEO within the organisation that deceptively instructs a member of the finance team to make an urgent payment to a false account.

Where the primary fraud involves theft, or loss, of money or securities, this will ordinarily not be covered by a Cyber policy. The direct financial loss to an insured arising from such events is more likely to be covered under a Crime policy.

Where such a fraud results in the theft or compromise of data, and/or malware being introduced or transmitted to computer systems, a Cyber policy may respond to any resultant third party liability. 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, breach response costs and any business interruption loss suffered due to computer system interruption. In other words, there is scope under some Cyber insurance policies to consider economic loss suffered by an insured; however the initial trigger must ordinarily be a failure of network security or privacy controls and not the fraud incident itself.

CRIME INSURANCE POLICIES – COVERAGE MAY INCLUDE:

- Direct financial loss caused by criminal, fraudulent, malicious and dishonest act (including theft, loss of money, securities, computer misuse, and telephone misuse)
- Direct financial loss of client/customer where liable to indemnify
- Costs of establishing direct financial loss
- Costs of verification, reconstruction of data or computer programmes
- Extortion loss
- Identity fraud costs

CYBER INSURANCE POLICIES – COVERAGE MAY INCLUDE:

- Liability to third parties arising from a covered cyber event
- Business interruption loss arising from a covered cyber event
- Incident response costs
- Cyber extortion loss
- Digital asset loss arising from a covered cyber event
- Payment card industry data security standards fines and assessments (PCI DSS)
- Regulatory fines arising from a covered cyber event
- Regulatory defence costs arising from a covered cyber event

2 https://www.ic3.gov/media/2018/180712.aspx

As incidents of cyber crime remain on the rise; it is important for organisations to understand the scope of coverage afforded under their current insurance policies to ensure they provide adequate levels of protection for both first party and third party losses. Understanding how a financial loss was sustained will be important for an organisation, bearing in mind that:

- 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 to the actions of the insured – such as, an allegation that the insured did not adequately protect the privacy of customer data.

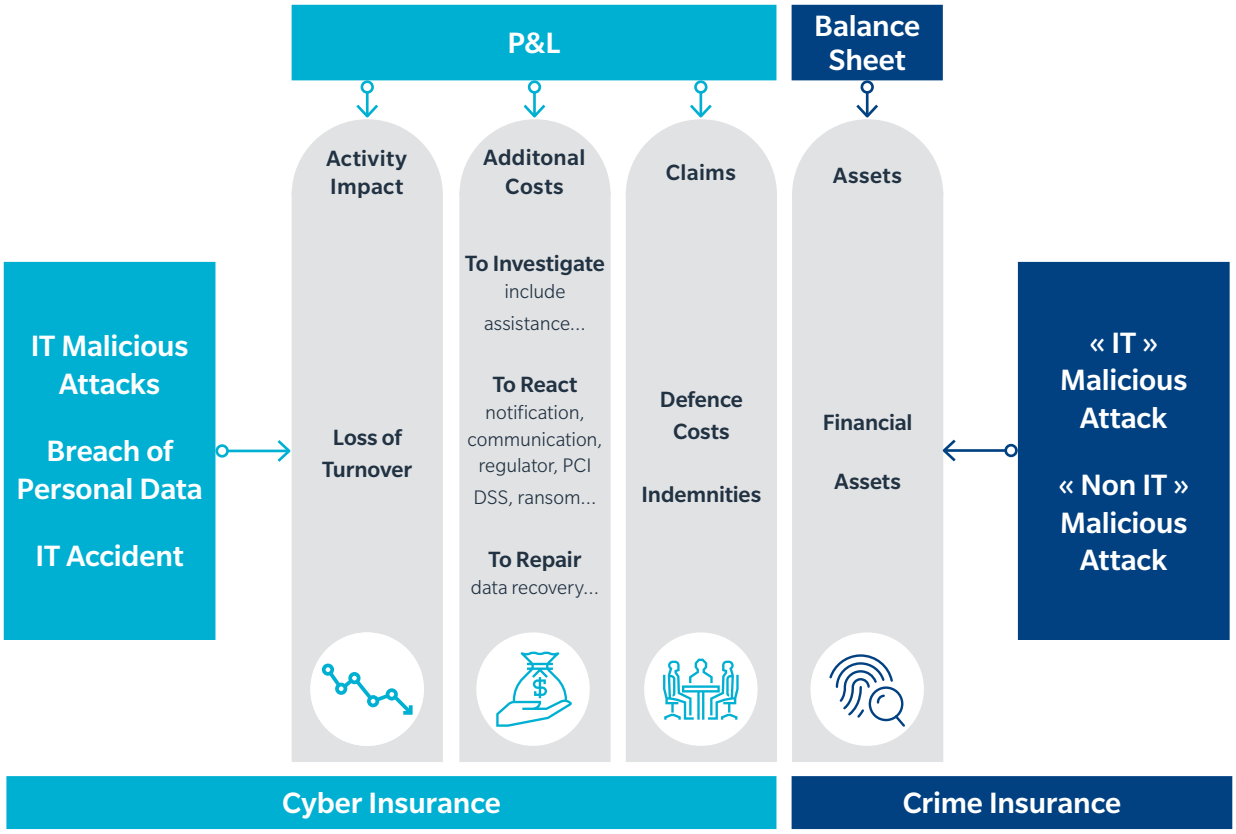
Social engineering relies on human interaction and exploiting people. The nature of attacks is diverse and continues to evolve, creating a significant potential threat to organisations as it takes advantage of the human element of a business. For companies to effectively mitigate this potential threat it is important to invest in staff awareness and education, and ensure information security policies and procedures are in place and regularly audited.

In conjunction with implementing mitigation procedures and awareness training, organisations should work with their insurance advisors to assess the potential exposures to social engineering, and undertake a review of the current insurance policies to ensure the insurance risk transfer solution is fit for purpose based on the organisations needs.

FIGURE 1

What can be covered through cyber insurance?

SOURCE: MARSH CYBER RISK DEFINITION



For more information, contact your Marsh representative or:

KELLY BUTLER
Cyber Leader – Pacific
+61 3 9603 2194
kelly.butler@marsh.com

KRISTINE SALGADO
Managing Principal – Cyber
+61 3 9603 2871
kristine.salgado@marsh.com

NICOLE PALLAVICINI
Principal – Cyber
+61 2 8864 8323
nicole.pallavicini@marsh.com

Marsh's Cyber Insurance Practice by the Numbers

80+ Dedicated Cyber Colleagues among more than 300 FINPRO colleagues

Placing more than USD750 million Premiums Globally

Pioneer of 30 Years-Old Cyber Insurance Market

More than 6,000 Cyber and E&O clients

Disclaimer: Marsh Pty Ltd (ABN 86 004 651 512, AFSL 238983) arrange insurance and are not an insurer. This is brochure contains general information and a general overview of the type of policy terms only. It is not a complete description of any policy's terms, conditions and exclusions which would determine coverage for a claim. This brochure does not take into account your individual objectives, financial situation or needs and may not suit your personal or commercial circumstances. For full details of the terms, conditions and limitations of a cover and before making any decision about whether to acquire an insurance product, refer to the specific applicable policy wordings. The information contained herein is based on sources we believe reliable but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update this brochure and shall have no liability to you or any party arising out of this publication or matter contained herein. Any statements concerning legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as legal advice, for which you should consult your own professional advisors. Marsh cannot provide any assurance that insurance can be obtained for any particular client or for any particular risk.

Copyright © 2018 Marsh Pty Ltd. All rights reserved. LCPA18/0045. M18-1165.