MARSH

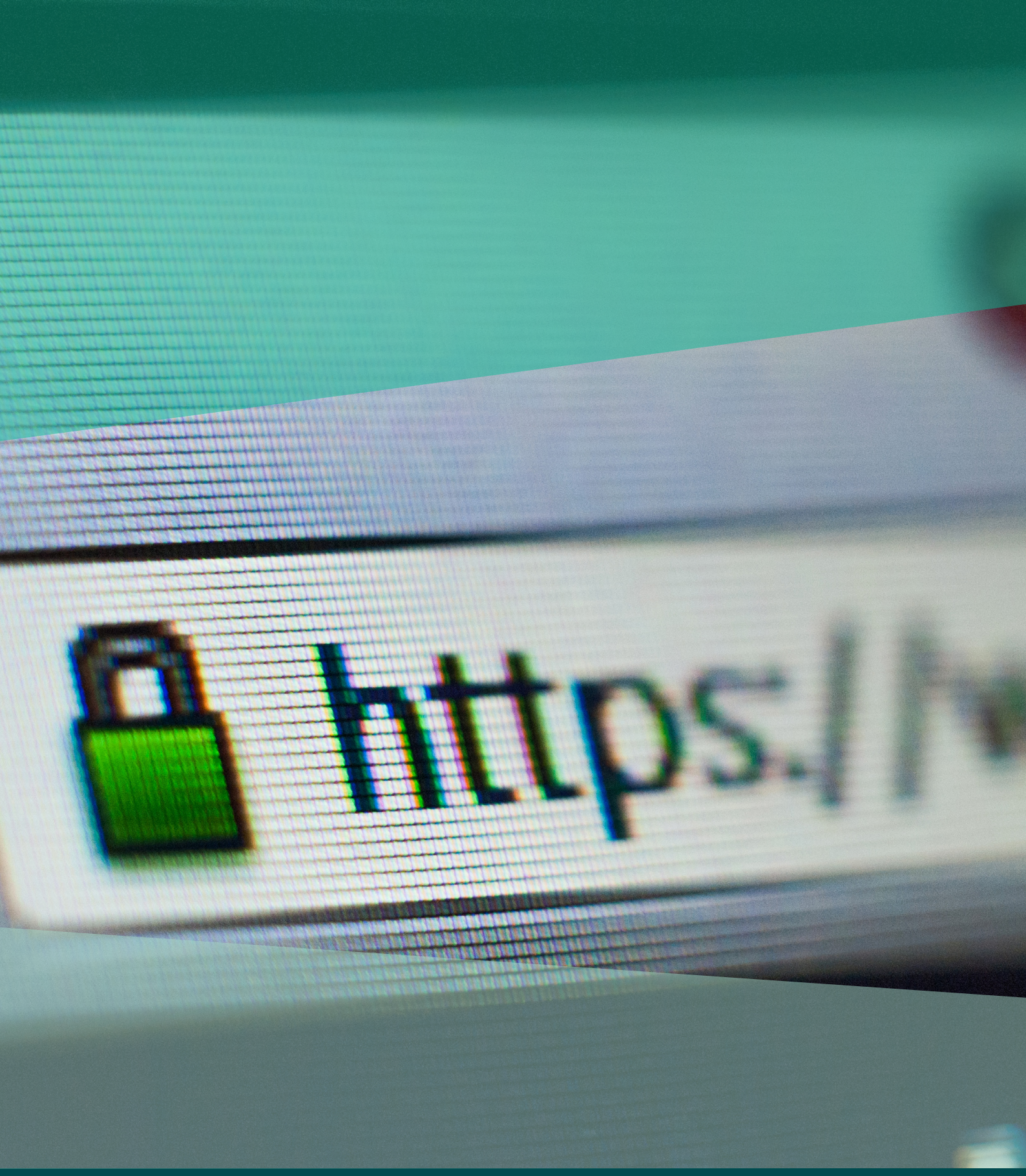
Global Marine Practice

CYBER GAP INSURANCE

CYBER RISK: FILLING THE COVERAGE GAP

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES


https://

CYBER RISK: A GROWING CONCERN

The ability to create and analyze vast quantities of electronic data, and to share it over a network of computers within an organization and potentially with the outside world via the internet, is essential to today's business environment. Rapid advances in information technology over the last quarter century have brought enormous benefits in terms of reduced costs, increased efficiency, and a general streamlining of operations. However, while the benefits are clear and undeniable, the speed of the advances has brought with it a succession of new threats that are not fully understood, and which the cybersecurity industry has struggled to keep pace with.

While there have been relatively few reports of successful cyber-attacks on either shipping or on shore-based facilities, they are not unknown, and comparable industries have suffered attacks that suggest, at the very least, that the maritime sector may be vulnerable.

It has been reported that significant weaknesses have been identified in the cyber security of critical technology used for navigation at sea. Global Positioning Systems (GPS), Automatic Identification Systems (AIS), and Electronic Chart Displays and Information Systems (ECDIS) are all essential aids to navigation, and each has been identified as potentially vulnerable to attack.

The International Maritime Organization (IMO) has required that AIS be fitted on board the majority of ships, since 2004. The IMO regulations require that AIS will be capable of automatically exchanging information regarding a vessel's identity, type, position, course, speed, navigational status, and other safety-related information with other ships, shore-based facilities, and aircraft. AIS has come to be relied upon as a navigational tool on board ship as an alternative to radar, and is also an integral part of vessel traffic separation systems used by organizations with delegated authority for safety at sea.

Vessel navigation and propulsion systems, cargo handling, and container tracking systems at ports and on board ships, and shipyard inventories and automated processes, are all controlled using software that needs to be completely reliable. However, recent events suggest that these systems might be vulnerable.

CASE STUDY 1

Hackers working with a drug smuggling gang infiltrated the computerized cargo tracking system of the Port of Antwerp to identify the shipping containers in which consignments of drugs had been hidden. The gang then drove the containers from the port, retrieved the drugs, and covered their tracks. The criminal activity continued for a two-year period from June 2011, until it was stopped by joint action by Belgium and Dutch police.

CASE STUDY 2

Using equipment that reportedly cost US$700 cyber-security firm Trend Micro, was able to demonstrate how AIS could be compromised by preventing a ship from providing movement information, by making "phantom" vessels or structures appear, by staging fake emergencies, and by making it appear to other AIS users that a ship was in a false location.

EXISTING CYBER RISK INSURANCE

The first cyber risk insurance products were introduced in the mid-1990s, but only became popular when changes in US legislation dictated the inclusion of the unauthorized disclosure of personal information. This resulted in premium volumes increasing from zero to circa US$1 billion[1] in under a decade.

To date, cyber risk insurance has primarily focused on liability exposures for privacy and data breach, but insurers are now offering broader products that cover certain first-party risks. The most significant developments have been in business interruption for which the cyber risk insurance market offers coverage that can be triggered by non-physical business interruption events.

WHAT IS CURRENTLY COVERED BY A CYBER RISK POLICY?

Cyber risk policies tend to include the following policy sections either as standard wording or by specific endorsement. Specifically, the cyber risk policy covers:

Privacy and data breach – the unauthorized disclosure of personally identifiable information. Cover includes:

- Liability claims.
- Defense against regulatory action (and penalty where insurable).
- First-party response costs, including the notification of affected individuals.
- Forensic IT costs involved in investigating a security breach that led to the disclosure.

Business interruption – Coverage can be triggered by certain intangible (non-physical damage) business interruption events, such as hacking of IT systems and the negligent acts of staff causing software/hardware failure.

Hacking damage – The reconstitution of data, and the replacement and/or repair of software following a hack.

Extortion – Covers the cost of the ransom demand arising from a hack and the appointment of an expert negotiator to deal with the extortionist.

Multimedia – Provides protection against claims arising from defamation, intellectual property infringement, and invasion of privacy through content published online (corporate website, corporate pages on social media platforms, etc.).

WHAT IS NOT COVERED?

While cyber risk insurers now provide cover for business interruption arising from an IT system failure, policies generally exclude bodily injury and property damage – even loss of use in some instances.

THE "CYBER RISK GAP"

Due to the presence of certain cyber risk exclusions, commercial policies will not provide cover for bodily injury, property damage, and business interruption arising from a hacking event.

Clause CL380, which has been inserted into the majority of marine policies since 2003, removes cover for the use of IT systems as a means of inflicting harm. This exclusion removes all cover for a cyber-attack leaving a client completely uninsured, including any associated business interruption loss.

In marine insurance, Clause CL380 (and any variants that may be applied by protection & indemnity (P&I) clubs and others) will be widespread, but other clauses may be in place on insurances covering shore-based facilities such as ports, terminals, and shipyards.

These include:
Terrorism Form T3 LMA3030 Exclusion 9 excludes cyber-attacks motivated by terrorism (in a similar fashion to CL380).

Electronic Data Exclusion NMA2914 is typically found in non-marine property and business interruption policies. It does not contain as many exclusions as CL380 but still leaves significant gaps in coverage.

Negotiations with insurers to remove these exclusions have been unsuccessful because the removal of these clauses, which are features of most treaty contracts, could leave them exposed to substantial "net" losses.

Existing cyber risk policies do not respond to the gap in coverage (the "cyber risk gap") created by these exclusions.

1. Cyber/Privacy Insurance Market Survey – 2012, *The Betterley Report*.

CYBER EXCLUSION WORDINGS

Institute Cyber Attack Exclusion Clause CL380:

1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss, damage, liability, or expense directly or indirectly caused by, or contributed to by, or arising from, the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

Terrorism Form T3 LMA3030 Exclusion 9 (Extract)

This Policy does not insure against loss or damage by electronic means including but not limited to computer hacking or the introduction of any form of computer virus or corrupting or unauthorised instructions or code.

Electronic Data Exclusion NMA2914

Notwithstanding any provision to the contrary within the Policy or any endorsement thereto, it is understood and agreed as follows:

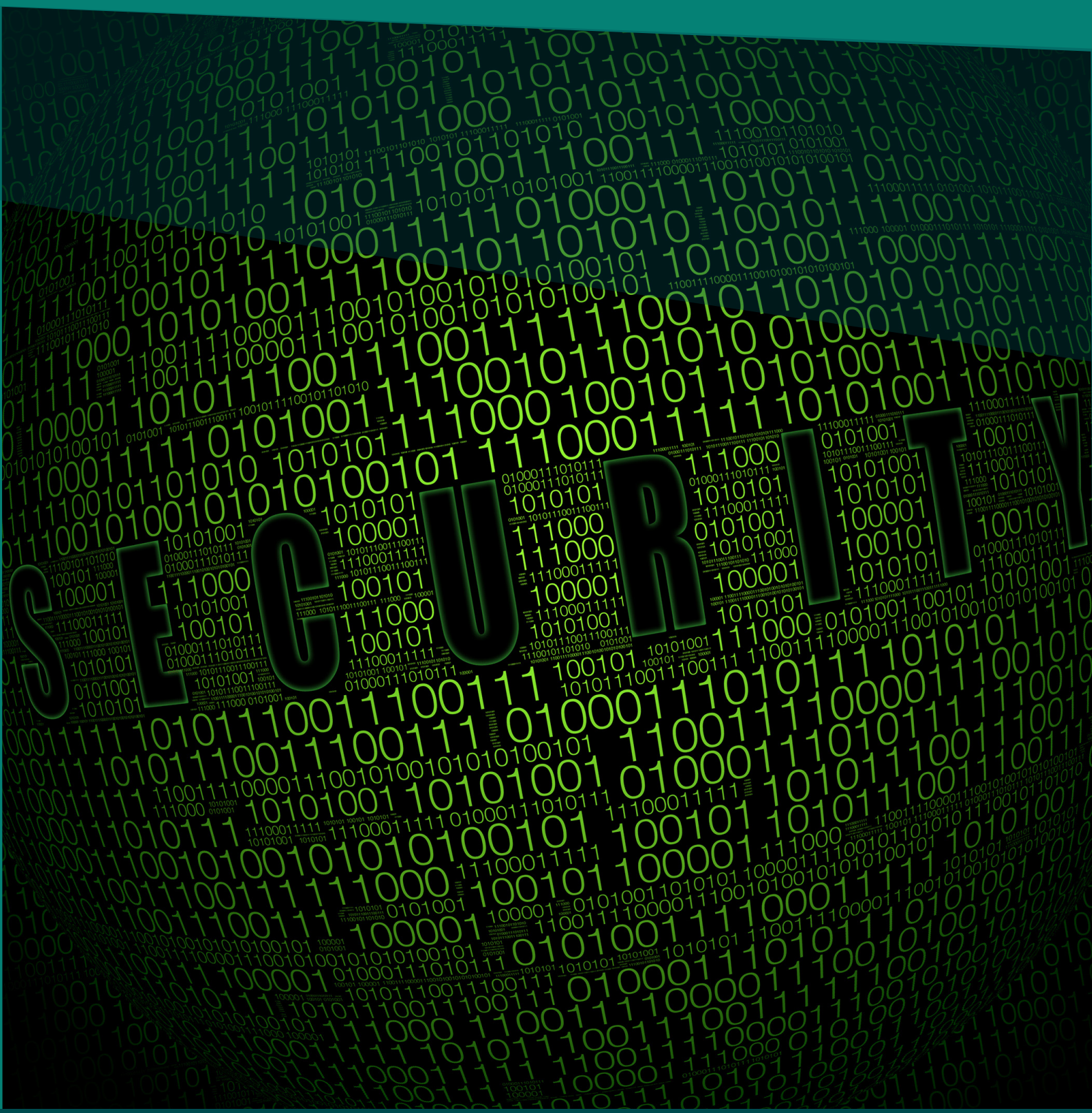
a) This Policy does not insure loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

ELECTRONIC DATA means facts, concepts and information converted to a form useable for communications, interpretation or processing by electronic and electromechanical data processing or electronically controlled equipment and includes programmes, software and other coded instructions for the processing and manipulation of data or the direction and manipulation of such equipment.

COMPUTER VIRUS means a set of corrupting, harmful or otherwise unauthorised instructions or code including a set of maliciously introduced unauthorised instructions or code, programmatic or otherwise, that propagate themselves through a computer system or network of whatsoever nature. COMPUTER VIRUS includes but is not limited to 'Trojan Horses', 'worms' and 'time or logic bombs'.

b) However, in the event that a peril listed below results from any of the matters described in paragraph a) above, this Policy, subject to all its terms, conditions and exclusions, will cover physical damage occurring during the Policy period to property insured by this Policy directly caused by such listed peril. Listed Perils:

- Fire
- Explosion


SECURITY

FILLING THE GAP IN COVERAGE

The coverage gaps in policies created by Exclusion Clause CL380, and by other cyber risk exclusion clauses potentially leave catastrophic events unindemnifiable and the numerous attempts to remove or alter them have, to date, been unsuccessful.

To help our clients overcome the gaps in coverage created by these exclusions, Marsh has developed a new facility, provided by Lloyd's of London insurers, that will indemnify the insured in the event that indemnification under the normal property, business interruption, liability, terrorism, or package policies (the "Controlling (Re)Insurance Policies") is denied solely due to the existence of any of these cyber risk exclusions. In effect, it negates the inclusion of these clauses (and subject to its limits, and terms and conditions it eradicates the cyber gap).

UNDERWRITING

In collaboration with underwriters and specialists in ICS security, Marsh has developed a questionnaire specifically tailored to deliver the information required by insurers to assess the maturity of insured companies' security practices. This dedicated questionnaire is further supported by in-depth assessment capabilities delivered by these security audit specialists and utilized when a more detailed understanding of corporate practices is required. Insurers will also be provided with a copy of the underwriting submission for controlling insurance policies.

BENEFITS

Benefits of Marsh's cyber gap insurance include the:

- Provision of protection against a cyber-attack.
- Closure of the gaps in coverage.
- Facilitation of more complete risk mitigation and risk planning strategies.
- Security of protection provided by insurers with a minimum Standard and Poor's (S&P) rating of A-.

MARSH

For further information, please contact your local Marsh office or visit our website at: marsh.com

ANTWERP
Uitbreidingstraat 180
B 2600 Antwerp
Belgium
+32 3 286 6411

CYPRUS
1 Michael Michaelides Street
Limassol
CY-3030
Cyprus
+357 25 878100

DUBAI
Al Gurg Tower 3
Plot 125-117
Riggat Al Buteen
Baniyas Road, Deira
P.O.Box 14937, Dubai
United Arab Emirates
+971 4 223 7700

HAMBURG
Cremon 3
D-20457 Hamburg
Germany
+49 40 376920

HONG KONG
26th Floor, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
+852 2301 7000

LONDON
Tower Place
London
EC3R 5BU
United Kingdom
+44 20 7357 1000

NEW YORK
1166 Avenue of the Americas
New York
NY 10036-2708
United States
+1 212 345 6000

OSLO
Vika Atrium
Munkedamsveien 45 D
0123 Oslo
Norway
+47 2201 1000

PARIS
Tour Ariane - La Défense 9
Paris La Défense cedex
992088
France
+33 1 4134 5000

ROTTERDAM
Conradstraat 18
3013 AP Rotterdam
The Netherlands
+31 10 40 60 600

SAN FRANCISCO
345 California Street
Suite 1300
San Francisco, CA 94104
United States
+1 415 743 8000

SINGAPORE
8 Marina View #09-02
Asia Square
Tower 1
Singapore 018960
+65 6922 8388