MARSH

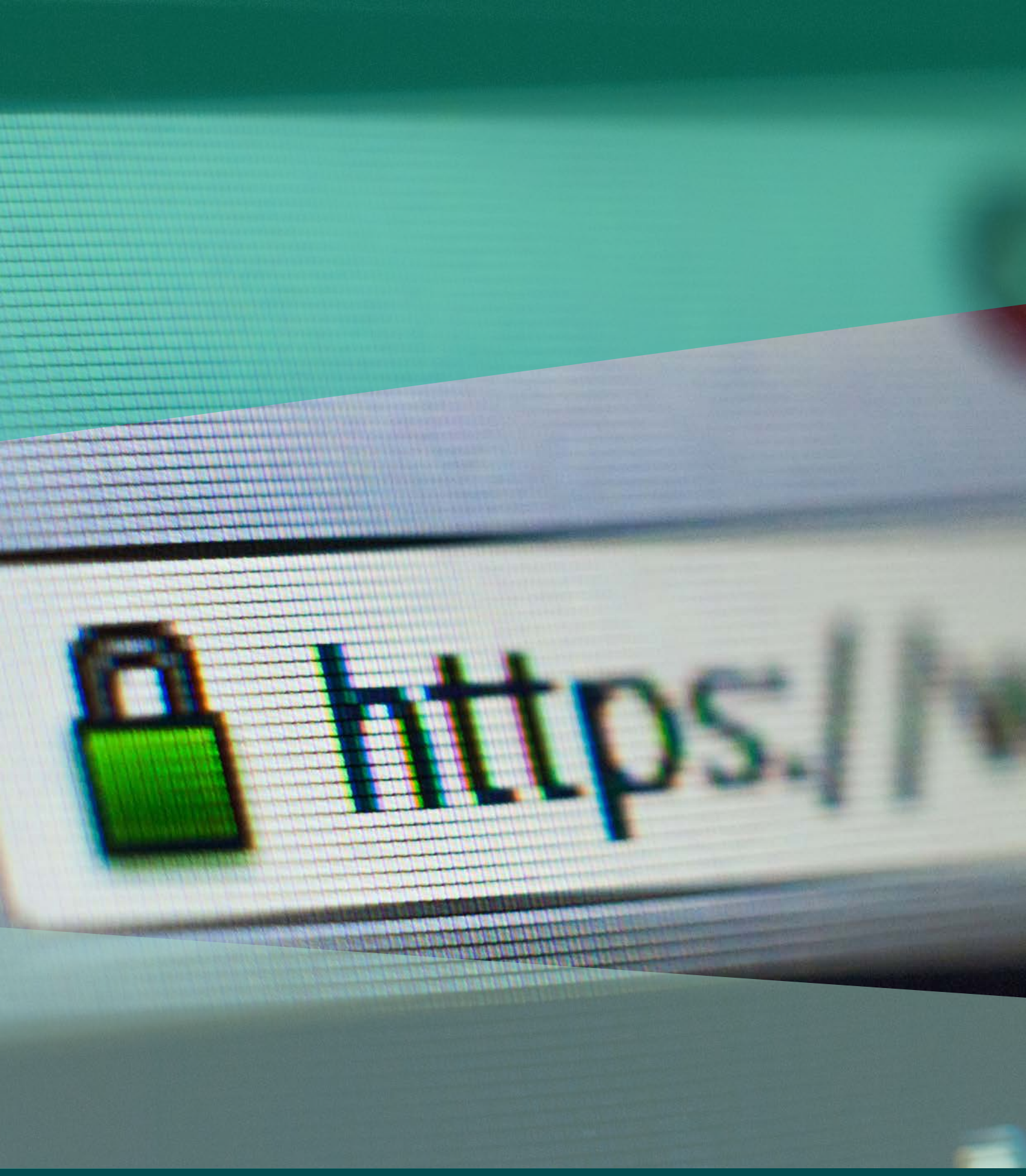
Global Energy Practice

CYBER GAP INSURANCE

CYBER RISK: FILLING THE COVERAGE GAP

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES


https://

CYBER RISK: A GROWING CONCERN

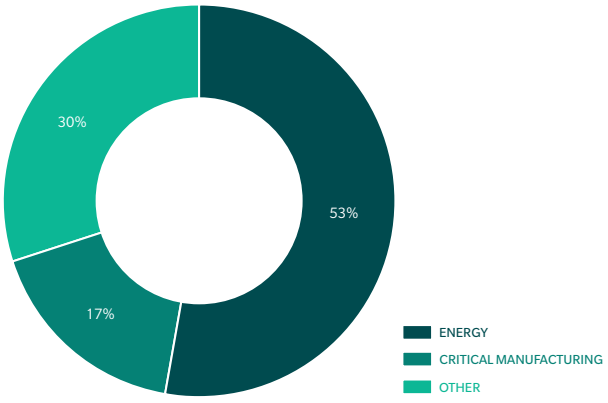
For the last quarter of a century, the global energy sector has relied on the protection offered by standalone and closed industrial control systems (ICS) as the primary barrier to the cybersecurity threat. Today, however, with energy facilities worldwide generally aging, upgrades and expansion projects are ushering in a wave of new ICS and supervisory control and data acquisition (SCADA) systems built on openness and interoperability. While the sector has been quick to take advantage of these new internet-connected systems to reduce cost, improve efficiency, and streamline operations, they have exposed it to a host of cybersecurity risks that are only just beginning to be understood.

To date, cyber-attacks directed towards the global energy sector have largely been untargeted and data-driven[1], as companies and individuals have attempted to gain access to personal or sensitive financial data. The nature of the threat is beginning to change, however, and companies across virtually all industry sectors have begun to witness much more intelligent and complex attacks that seek to take charge of ICS in order to inflict damage to property and operations.

Although the global energy sector has yet to experience catastrophic physical damage to facilities or disruption to supply as a result of a cyber-related event — publicly, at least — the disproportionate rate at which it is targeted in cyber-attacks makes it apparent that it is only a matter of time before this trend is broken. According to the US Department of Homeland Security, 53% of the 200 incidents responded to by its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) between October 2012 and May 2013 were directed toward the energy sector. To put that in perspective, the second highest industry was manufacturing, which sustained 17% of attacks.

ICS-CERT INCIDENT RESPONSES — OCTOBER 2012 TO MAY 2013

Source: US Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), June 2013



1. US Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), June 2013

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[2] 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 property policies (mainly upstream) 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, thereby leaving a client completely uninsured, including any associated business interruption loss.

Terrorism Form T3 LMA3030 Exclusion 9 excludes cyber-attacks motivated by terrorism (in a similar fashion to CL 380).

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. Since these exclusions also apply to package policies, including the general liability and loss of well control risk, the cyber risk gap needs to be addressed across a wide spectrum.

2. 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, the Electronic Data Exclusion NMA2914 or even exclusion 9 of the Terrorism Form T3 LMA3030 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 simple questionnaire specifically tailored to deliver the information required by insurers to assess the maturity of insured companies' security practices. This dedicated, simplistic questionnaire is further supported by in-depth assessment capabilities delivered by these security audit specialists and utilized where 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

BEIJING
Unit 1506, North Tower
Beijing Kerry Centre
1 Guang Hua Road,
Chao Yang District
Beijing, 100020, China
Tel: +86 10 6533 4070
Fax: +8610 8529 8761

CALGARY
222 - 3rd Avenue S.W.
Suite 1100
Calgary Alberta T2P 0B4
Canada
Tel: +1 403 290 7900
Fax: +1 403 261 9882

CAPE TOWN
1 Thibault Square
Long Street
Cape Town, 8001
South Africa
Tel: +27 21 403 1940
Fax: +27 21 419 3867

DUBAI
Level 10, Al Gurg Tower 3,
Riggat Al Buteen
Baniyas Road, Deira
P.O.Box 14937,
Dubai, United Arab Emirates
Tel: +971 4 223 7700
Fax: +971 4 227 2020

HOUSTON
1000 Main Street, Suite 3000
Houston, Texas 77002
United States
Tel: +1 713 276 8000
Fax: +1 713 276 8888

LONDON
Tower Place
London, EC3R 5BU
United Kingdom
Tel: +44 (0) 20 7357 1000
Fax: +44 (0) 20 7929 2705

MADRID
Edificio Puerta Europa,
Paseo de la Castellana, 216
Madrid
E-28046 Spain
Tel: +34 914 569 400
Fax: +34 913 025 500

MOSCOW
Serebryanicheskaya
Emabankment 29
Moscow, 109028
Russian Federation
Tel: +7 495 787 7070
Fax: +7 495 787 7071

MUMBAI
1201-02, Tower 2,
One Indiabulls Centre
Jupiter Mills Compound,
Senapati Bepat Marg
Elphinstone Road (W)
Mumbai, 400013, India
Tel: +91 226 651 2900
Fax: +91 226 651 2901

NEW YORK
1166 Avenue of the Americas
New York
10036-2708
United States
Tel: +1 212 345 6000
Fax: +1 212 345 4853

OSLO
Vika Atrium,
Munkedamsveien 45 D
Oslo
N-0123
Norway
Tel: +47 22 01 10 00
Fax: +47 22 01 10 90

PERTH
Exchange Plaza
2 The Esplanade
Perth
Western Australia
Tel: +61 8 9289 3888
Fax: +61 8 9289 3880

SAN FRANCISCO
345 California Street
Suite 1300
San Francisco, CA
94111-5421
United States
Tel: +1 415 743 8000
Fax: +1 415 743 8080

SINGAPORE
18 Cross Street
#04-03
Marsh & McLennan Centre
Singapore
048423
Tel: +65 6327 3150
Fax: +65 6327 8845