howden Specialty

CYBER: PROPERTY DAMAGE

INTRODUCTION

No business, no matter what industry, is immune from cyber risk.

Energy, logistics, mining, manufacturing, shipping and other heavy industries increasingly utilise both information technology and operational technology in their day-to-day operations, but this reliance on technology can pose significant, unique ris

The World Economic Forum* put cyber-attacks among the top 10 risks for both likelihood and impact in 2020 and with a rapidly changing threat landscape, businesses must constantly adapt in line with the risks that they face. Operational errors, system failure, ransomware attacks or other malware can all result in both intangible (financial) and tangible (physical damage) losses for businesses.

Whilst the legal ramifications and financial losses resulting from data breaches are better known, cyber events resulting in physical damage have been less widely publicised. This is due to the sensitive nature of critical infrastructure and difficulties in attributing causation, however there have been a number of cyber events resulting in physical damage to date and the increasingly complex international stage, only makes the likelihood of malicious cyber activity more significant.

*** Source:** World Economic Forum Global Risks Perception Survey 2019-2020.

Norsk Hydro

Norsk Hydro, a global leader in aluminium production was exposed internationally to an extremely effective cyber-attack with a piece of ransomware called LockerGoga. The ransomware directly impacted digital systems at Norsk Hydro's smelting plants in Norway, Brazil and Qatar. It also affected Norsk's metal extrusion plants which had to be completely shut down. The risk of LockerGoga damaging Norsk's smelting facilities forced the company to go into manual operation which incurred business interruption costs of USD 70,000,000 in the first half of the year.

$70m

Business interruption cost.

NotPetya cyber-attack

In 2017 both Merck & Co. and Mondelez International Inc. were affected by the NotPetya cyber-attack. The level of the collateral damage from the attack was unparalleled. Numerous claims were made as a result of the incident and it is described as the closest the insurance market has come to experiencing a cyber-catastrophe loss. The NotPetya incident caught the attention of the UK's Prudential Regulation Authority (PRA), who emphasised the need for non-life insurers to better manage cyber risk exposures for UK bound business and in 2019 requested insurers to properly and effectively identify, quantify and manage non-affirmative (silent) and affirmative cyber risk exposure.

$10bn+

Total damages brought about by NotPetya.

Sodinokibi

Researchers at Dutch Telecoms company KPN tracking Revil aka Sodinokibi have detected over 150,000 unique infections and extracted ransom demands from 148 samples demanding more than USD 38,000,000 from its victims. This equates to an average extortion demand of over USD 250,000 per company affected.
» Click here for more information

$250k+

An average extortion demand.

Lloyd's Business Blackout report

The potential impact of property damage is huge. Lloyd's Business Blackout report estimated the economic impact from the scenarios it examined would be from $243 billion to $1 trillion, with insured losses estimated between $21.4 billion and $71.1 billion. (The report describes all such theoretical scenarios as realistic, although some parties have queried this.)
» Click here for more information

$21.4bn+

Insured losses estimated between $21.4 billion and $71.1 billion.

Cyber property report

Business leaders who are aware of insurance solutions for cyber tend to overestimate the extent to which they are covered. Surveys show that 52% of CEOs believe that they have cover, whereas in fact less than 10%
» Click here for more information

$250k+

An average extortion demand.

Industrial control system threats

In 2017, a report conducted by the Cybersecurity Research Group found that 67% of companies with critical infrastructure experienced at least one cyber-attack in the last year and 78% expected their ICS and SCADA systems to be exploited in the next two years. Whilst, A 2016 industry report found that attacks targeting ICSs increased over 110% compared to the previous year, and a 2017 SANS study found that 69% of ICS security practitioners believe threats to the ICS systems are high or severe and critical.
» Click here for more information

69%

ICS security practitioners believe threats to the ICS systems.

INDUSTRY VULNERABILITIES FROM A CYBER PROPERTY DAMAGE PERSPECTIVE

As industries have modernised, so has the technology that they rely on. The use of industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems has increased production, performance and profitability of industries that have previously been reliant on manual operations. This can be observed in almost every sector or industry whether it be oil and gas, renewables, manufacturing, utilities, mining, shipping or logistics.

The diversity and range of ICS means there are applications for almost every industry, however there is a level of vulnerability that cannot be ignored. Poor management of ICS protocols, weak segregation from information technology and a lack of security awareness can create exploitable scenarios whereby threat actors can harm an organisation's physical assets.

Cyber attacks such as ransomware, malware and distributed denial of service (DdoS) are also no longer exclusively considered information technology events. Businesses utilising ICS and SCADA systems have not traditionally needed to address these types of IT problems, however, as assests become more interconnected, IT and OT can no longer be considered as two entirely separate domains. IT focussed malware such as WannaCry, EternalBlue and LockerGoga have frequently impacted operational technology networks, which may cease to work all together without digital functionality and are not able to be run as efficiently or as safely under manual operations.

In order to address the perceived cyber risk to ICS and SCADA, a security measure called the 'Air Gap' has been proposed. The purpose of the 'Air Gap' is to create an absence of a direct or indirect connection between a computer and the internet, for security reasons. This means that there is complete segregation between corporate networks and process control networks (PCN). The 'Air Gap' is an effective tool for segregation however, due to necessity for information exchange from business leaders the boundaries between corporate and process control networks can become porous at key points. For example, the Dragonfly malware that was discovered in 2014, targeted the pharmaceutical industry. One way it obtained access to ICS networks was via malicious payloads inserted into legitimate software updates provided on vendor websites.

Specific cyber risks

Malware threats

Portable media carried by employees can often be used to transfer Malware. Malware can be embedded in JPG and PDF files on portable media, which can be used to bypass security systems and attack ICS or SCADA systems.

Insider attack

Intentional or unintentional malpractice can lead to compromise. Attacks can originate from disgruntled employees who are paid to carry out an attack or steal company data. Phishing emails can also lead to unintentional errors leading to attacks via manipulation of communications from unknown sources to be perceived as known or trusted.

Denial of service

ICS communicate via wired and wireless connections. Intentionally fowling these communication routes by overloading servers can have real-time impacts, disrupting operations.

Third-party threats

Outsourcing system support for ICS can result in compromise due to third party vendors not requiring the same level of security clearance for the systems that they are providing services to. For example, Dragonfly Malware gained access to ICS within the Pharmaceutical Sector in 2014 via legitimate software updates provided by third-party vendors.

Technical or physical malfunction

Component level failure such as disconnection, power outages, cable breakage, system crashes or hard disk failure. Stopping the function of a device, controlling switches and moving parts can cause damage and outages to a system.

Threats from terrorists and hackers

Attacks on critical infrastructure from terrorist groups or hackers that wish to cause fear, damage and potential loss of life. Malicious parties, terrorist groups or industry rivals can pay hackers to target companies, which can lead to reputational damage, financial loss and physical damage.

PHYSICAL DAMAGE CYBER EVENTS

Turkish Pipeline

2008

In August 2008, a major explosion and fire took place on the BP majority owned and built Baku–Tbilisi–Ceyhan pipeline, which led to its closure for nearly a month. This was linked to a cyber-attack on the line's control and safety systems, where alarms and communications had been shut down and the crude oil was super-pressurised which led to the explosion.

Iranian Nuclear Plant

2009

This attack caused centrifuge destruction through a virus infiltrating into ICS at an Iranian nuclear power plant in 2010. Stuxnet was used on Iran's Natanz uranium enrichment facility and targeted specific operating systems within the plant, damaging 20% of the nuclear centrifuges and was regarded as one of the most sophisticated pieces of malware at the time. The dangerous aspect of Stuxnet was its ability to install itself undetected and self-replicate through multiple systems.

Industrial Sector

2010

A series of Advanced Persistent Threat (APT) attacks on various industries, primarily focussing on SCADA systems. This was described as a cyber espionage threat primarily targeting SCADA systems within the energy and manufacturing sectors, which allowed constant access with sabotage capabilities. It was noted that Energetic Bear formed part of an exploratory phase where threat actors sought to gain access to the network systems of target organisations and industries.

German Steel Mill

2014

In 2014, the German government released reports detailing a cyber-attack on an unspecified steel mill, where systems were compromised by social engineering tactics and phishing emails. This allowed hackers to gain access to IT networks, which enabled them to gain access to OT systems involved in production on the plant. Once the control systems were breached, the attackers initiated a number of control system failures in order to prevent the correct closure of blast furnace doors, causing large amounts of physical damage to plant, property and equipment. It was noted in a German government report that the threat actors had an in-depth knowledge of ICS and steel plant processes, using traditional methods of attack that were extremely advanced and specifically intended to interrupt operational processes.

Ukrainian Power Grid
2015

A malware attack that affected substations at a Ukrainian utility caused a blackout of electricity supply. In the run up to Christmas in 2015, Ukraine experienced a power outage effecting almost 250,000 people. It transpired that this was a cyber-attack on SCADA systems rendering them inoperable, which resulted in manual restoration of all systems and power. Hackers introduced three variants of malware via phishing emails called Black Energy. Although, it was never confirmed who was behind the attack, many believe the attack was orchestrated by Russia.

Merck & Co. and Mondelez International Inc.
2017

In 2017, the NotPetya cyber-attack utilised a vulnerability in Windows' Server Message Block (SMB) protocol called EternalBlue, which allowed hackers to harvest passwords and run code on other computers. A US government assessment suggested that the total damages brought about by NotPetya exceeded USD 10 billion globally and Merck & Co. and Mondelez International Inc. were two of the worst affected organisations. Mondelez reported that 1,700 of its servers and 24,000 laptops were left permanently dysfunctional as a result of the incident, putting its losses in excess of USD 100,000,000. Merck & Co. also reported to have demobilized 30,000 laptops and desktops while 7,500 servers were affected, resulting in a USD 260,000,000 loss.

LLOYDS SILENT CYBER

Throughout 2017-2020, the Prudential Regulation Authority (PRA) and Lloyd's of London became concerned that 'silent cyber' risks – e.g. cyber-attacks impacting insurance lines that don't contemplate cyber coverage – places insurers at unexpected levels of exposure.

With an increasing trend in claims activity and litigation relating to the NonPetya Ransomware in particular, Lloyd's announced that, from January 2020, all (non-cyber) insurance policies must start providing clarity on cyber, either excluding all cyber risks or providing specific endorsements to address the exposure and underwriting the risk accordingly.

The Lloyd's requirements are being introduced in a phased manner, starting with first-party property damage policies in January 2020, and moving to cover liability and treaty reinsurance throughout 2020 and 2021. This mandates that all policies provide clarity on cyber. Insurers must either specifically exclude or explicitly provide (re)insurance coverage for the exposure.

Phase 1

1st party property damage insurers from **1st January 2020**. This includes:

- Energy Construction
- Energy Offshore Property
- Energy Onshore Property
- Power Generation
- Cargo
- Marine Hull
- Property D&F (US & Non-US open market)
- Engineering

Phase 2

Accident & health, political risks and reinsurance of 1st party property business from **1st July 2020**.

Phase 3

3rd party liability, general liability, financial and professional risks and any remaining reinsurance lines from **1st January 2021**.

There are a number of solutions available in the Lloyd’s market, supported by syndicate capacity or through consortia.

These can be tailored to fit the unique requirements of each insured, affirmatively covering property damage and ensuing business interruption from a cyber event, or as a buy-back of an exclusion with the property placement.

LONDON MARKET CYBER PROPERTY DAMAGE SOLUTIONS

In addition, these policies can be blended with traditional, non-damage cyber coverage where required. Some of the solutions available include:

Consortium led by market leading property and cyber (re)insurer

- Max USD 275M limit offering through one market (backed by a consortium of London market capacity)
- Appetite and policy language tailored for up-stream and mid-stream businesses
- Buy-back and affirmative property damage and ensuing business interruption coverage available
- Trigger is malicious cyber-attack
- Schedule of values (BI & PD) and copy of property policy for a non-binding buy-back indication
- Schedule of values and revenues for a non-binding indication for affirmative coverage
- Conference call and/or application for bind-able terms.

Additional consortium led by market leading property and cyber (re)insurer

- Max USD 150M limit offering through one market (backed by a consortium of 100% Lloyd's capacity)
- Appetite for all risks
- Policy language taken from existing energy, property, cyber and terrorism policies and designed to sync with the new LMA5400 or LMA5426 exclusions
- Modular insurance policy providing affirmative cyber PD coverage or buy-back coverage
- Schedule of values (BI & PD) and copy of property policy for a non-binding buy-back indication
- Schedule of values and revenues for a non-binding indication for affirmative coverage
- Conference call and / or application for bind-able terms.

Lloyd's cyber syndicate (re)insurer solutions

- Open market cyber property damage capacity available: USD 150M-USD 250M total limits from 5-10 different syndicates
- Broad appetite for all 'heavy industry' insureds
- Buy-back coverage for a cyber-exclusion contained within energy package, terrorism or property policies and affirmative solutions for property damage and ensuing business interruption coverage available
- Triggers include malicious cyber-attack and a computer system malfunction resulting from an error in updating and/or programming the computer system
- Schedule of values (BI & PD) and copy of property policy for a non-binding buy-back indication
- Schedule of values and revenues for a non-binding indication for affirmative coverage
- Conference call and / or application for bind-able terms.

Lloyd's cyber syndicate Marine cyber property damage product

- Max USD 50M capacity from a London market, with USD 100M additional open market capacity available from 5-10 different Lloyd's syndicates
- Specifically for marine hull risks, but can also cover ports and terminals
- Buy-back coverage for a cyber-exclusions contained within the hull and marine policies
- Triggers is malicious cyber-attack
- Hull policy and fleet schedule for a non-binding buy-back indication
- Application and / or statement of fact for bind-able terms.

David Rees
Executive Director
+44 (0)75 3578 2203
david.rees@howdengroup.com

Dan Westinghouse
Divisional Director
+44 (0)79 6425 0366
dan.westinghouse@howdengroup.com

James Gordon
Divisional Director
+44 (0)77 0631 3778
james.gordon@howdengroup.com

Chris Cotterell
Divisional Chair - Cyber
+44 (0)75 6679 4516
chris.cotterell@howdengroup.com

James Pope
Associate Director
+44 (0)77 9126 2562
james.pope@howdengroup.com

Kathryn Brown
Associate Director
+44 (0)77 1159 5581
kathryn.brown@howdengroup.com

Raghav Bharathan
Associate Director
+44 (0)77 0635 0811
raghav.bharathan@howdengroup.com

Nicholas Lithgow
Account Handler
+44 (0)79 2323 2624
nick.lithgow@howdengroup.com

Sueli Williams
Associate Director
+44 (0)79 8576 2204
sueli.williams@howdengroup.com

David Armstrong
Intermediary Account Manager
+44 (0)78 7486 2828
david.armstrong@howdengroup.com

Daniel Leahy
Senior Account Executive
+44 (0)79 2324 6517
daniel.leahy@howdengroup.com

Kriss Bond
Senior Account Executive
+44 (0)77 1070 4699
kristina.bond@howdengroup.com

Richard Morrice
Senior Account Executive
+44 7809 337290
richard.morrice@howdengroup.com

Freddy Ruff
Account Executive
+44 (0)78 7486 2836
freddy.ruff1@howdengroup.com

Jessica Roper
Account Executive
+44 (0)20 3808 5663
jessica.roper@howdengroup.com

Sam Blakeley
Account Executive
+44 (0)78 4231 4186
sam.blakeley@howdengroup.com

Charlotte Beaumont
Account Handler
+44 (0)77 0635 5342
charlotte.beaumont@howdengroup.com

One Creechurch Place, London, EC3A 5AF

T +44 (0)20 7623 3806
E enquiry@howdenspecialty.com

www.howdenspecialty.com

howden
Specialty

Howden Specialty is a trading name of Howden Insurance Brokers Limited, part of the Howden Group Holdings. Howden Insurance Brokers Limited is authorised and regulated by the Financial Conduct Authority in respect of general insurance business. Registered in England and Wales under company registration number 725875. Registered Office: One Creechurch Place, London, EC3A 5AF. Calls may be monitored and recorded for quality assurance purposes. 11/21 Ref: 5136