Silent (Non-Affirmative) Cyber Across Traditional Insurance Lines…Not So Silent Anymore

Kara Owens

January 21, 2020

FIRST.org – Cyber Insurance SIG

MARKEL®

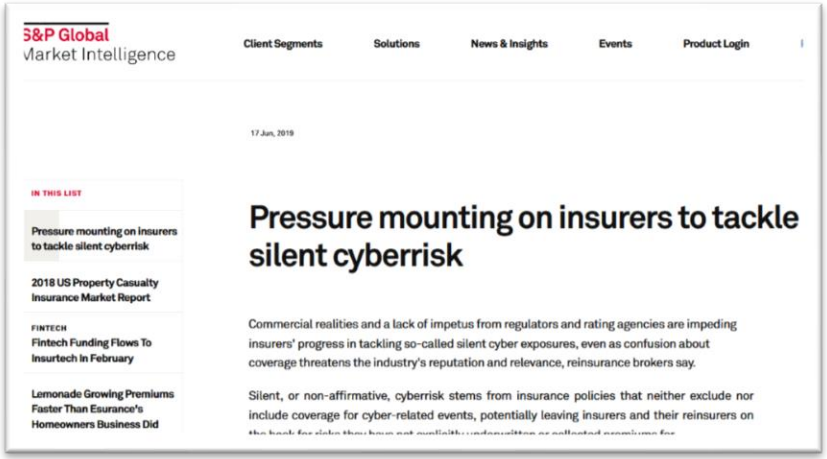
Agenda

- What is Silent Cyber?
- Why is it not so silent anymore?
- Industry response
- Examples across insurance product lines
- Where to go from here?

Silent Cyber

Silent / Non-Affirmative Cyber Definition: Insurance policies that do not explicitly include or exclude coverage for cyber risk or where gaps may exist in current wording creating contract uncertainty

Why Is It Not So Silent Anymore?



S&P Global
Market Intelligence

Client Segments | Solutions | News & Insights | Events | Product Login

17 Jun, 2019

IN THIS LIST

Pressure mounting on insurers to tackle silent cyberrisk

2018 US Property Casualty Insurance Market Report

FINTECH
Fintech Funding Flows To Insurtech In February

Lemonade Growing Premiums Faster Than Esurance's Homeowners Business Did

Pressure mounting on insurers to tackle silent cyberrisk

Commercial realities and a lack of impetus from regulators and rating agencies are impeding insurers' progress in tackling so-called silent cyber exposures, even as confusion about coverage threatens the industry's reputation and relevance, reinsurance brokers say.

Silent, or non-affirmative, cyberrisk stems from insurance policies that neither exclude nor include coverage for cyber-related events, potentially leaving insurers and their reinsurers on

LLOYD'S

Market Bulletin

Ref: Y5258

Title	Providing clarity for Lloyd's customers on coverage for cyber exposures
Purpose	To notify the market of new requirements requiring clarity of coverage for cyber exposures in all policies
Type	Event
From	Caroline Dunn, Head of Class of Business, Performance Management
Date	4 July 2019
Deadline	To be adopted for all first-party property damage business incepting on or after 1 January 2020

FitchRatings

Search

Fitch Rtgs: Silent Cyber Assessment Key to Managing Evolving Insurance Risk

10 DEC 2019 10:45 AM ET

Fitch Ratings-New York-10 December 2019: Property and Casualty (P/C) insurers are gradually gaining sophistication in measuring risk aggregations and modeling potential losses from catastrophic cyber events, but efficacy of this analysis is inhibited by exposure to non-affirmative or "silent" cyber risk, Fitch Ratings says. Many insurers now view cyber insurance as an attractive source of premium growth and profits. However, future segment performance faces considerable uncertainty given the evolving nature of cyber incidents in a constantly changing technological, lega and regulatory environment.

Insurers face silent cyber risk when broad commercial package or other insurance policies do not explicitly address cyber-related coverage terms or specifically exclude cyber risks. This ambiguity in coverage can lead to disputes and litigation following a cyber event when insureds seek funds from available policy limits for protection; it also poses risk of reputational damage to insurers.

Reinsurance News

PRA calls for silent cyber action from Lloyd's, UK insurers

31st January 2019 - Author: Charlie Wood

The Prudential Regulation Authority (PRA) believes Lloyd's and the wider UK insurance industry can do more to ensure the effective management of affirmative and non-affirmative (silent) cyber risk exposures, ordering firms to develop an action plan in the first half of 2019, with clear milestones and dates by which action will be taken.

MARKEL®

Why Is It Not So Silent Anymore?

Lloyd's Bulletin Y5258

To support the market-wide adoption, there will be a phased implementation:

Phase 1**:** From 1 January 2020, all Lloyd's first-party property damage policies incepting on or after this date must have affirmative cover or an exclusion. This includes all open market and delegated risks, whether new or renewed.

Open market risks:

- From 1 January 2020, all Phase 1 risks incepting on or after this date, regardless whether written on an 'All Risks' basis or as 'Named perils', must have affirmative cover or an exclusion. This applies to new and renewal policies and to policies written on both a standalone basis and where first-party exposures are combined with other lines within blended products.

Delegated:

- From 1 January 2020, all Phase 1 binding authority agreements that incept on, or after this date must have affirmative cover or an exclusion. Lloyd's does **not** expect policies bound under binding authority agreements entered into before 1 January 2020 to comply until the binding authority agreement next renews.

Lineslips/consortia:

- For lineslips and consortia, Lloyd's expects changes to be made as soon as contractually possible after the 1 January 2020.

MARKEL®

Industry Response

AIG tackles silent cyber exposures across commercial lines

Catrin Shi 05 September 2019

The carrier will either affirmatively cover or explicitly exclude cyber across virtually all commercial P&C policies by January.

New Allianz Underwriting Strategy for Cyber

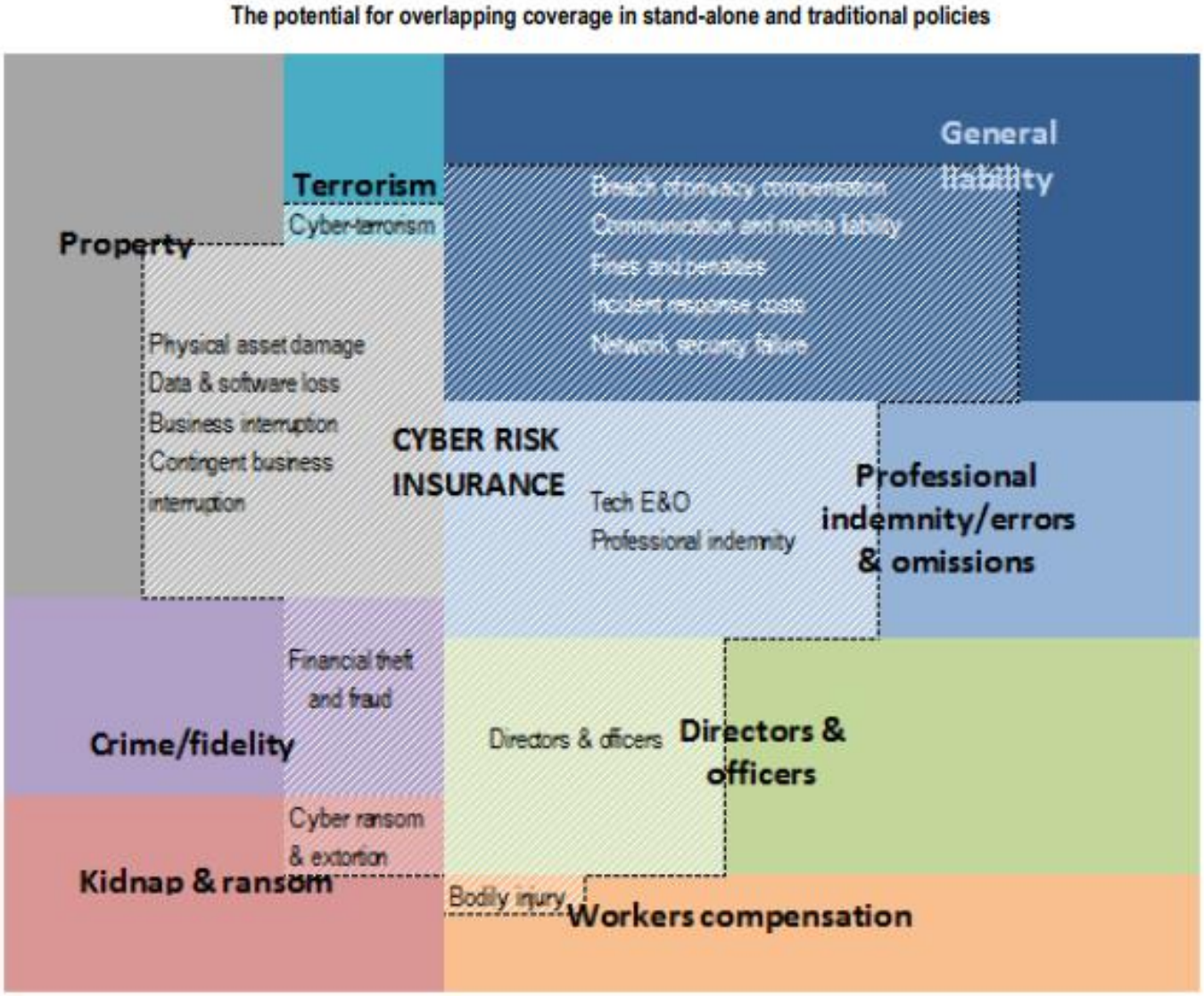
Group-wide, Allianz is reviewing cyber risks in P/C policies in commercial, corporate and specialty insurance segments and has developed a new underwriting strategy to address "silent" cyber exposures, ensuring that all P/C policies will be updated and clarified in regard to cyber risks. It has nominated AGCS to establish a **Center of Competence for Cyber** for the entire company.

"We will make it clear how cyber risks are covered in traditional policies and for which scenarios a dedicated cyber insurance solution is needed," Donavan says. The new strategy also responds to growing concern from regulators and rating agencies about cyber exposures in insurers' portfolios.

AGCS has already implemented the strategy for new business and will do so for renewal business, subject to regulatory and filing requirements in certain jurisdictions, in April. Other Allianz P/C companies will apply the strategy by January 1, 2020, latest.

MARKEL®

Cyber Across Product Lines



Source: OECD/CRO Forum

Cyber Across Product Lines

Source: AON

Cyber Across Product Lines

Internet of Things (IoT) – Exposure grows with 5G

- Internet connected and autonomous vehicles
- Smart security
- Home IoT
  - Often manufactured and sold with minimal or sub-standard security and privacy controls
  - Some susceptible to botnet/DDoS attacks
- Smart watches, fitness trackers and other wearables
- Machine to machine connected devices (M2M)
- Supply chains of the future
- Drones for industrial and search & rescue operations
- Smart cities: energy, transportation, parking and more
- Farm to tech table

Cyber Across Product Lines

"Internet of Bodies" – (IoB)

- Body external
  - Wearables: smart watches, fitness trackers, etc.
- Body internal
  - Pacemakers, cochlear implants, digital pills that go inside of our bodies to monitor control various aspects of our health
- Body embedded
  - Third generation of Internet of Bodies – embedded tech where tech and human body are melded together and have real-time connection to a remote machine

Casualty

Infrastructure Hacking

- Industries exposed: Utilities, Telecom, ISP's, related and contingent industries
- Breach of infrastructure could result in wide scale loss of power, access, or control of a critical safety or other mission critical systems

Data Breaches

- Industries exposed: Retailers, Financial Institutions, Healthcare, Payment Processors, and more
- Data loss is primarily a Personal & Advertising Injury exposure (thus excluded within common Access & Disclosure wording) - however plaintiffs bar have argued that **replacement of credit cards are property damage losses**

Medical Devices and Equipment

- Industries exposed: device manufacturers, healthcare facilities, hospitals, doctors office, etc.

Manufacturing

- Equipment / product automation
- Changing/altering product design / product specs
- Exposure for end product getting hacked resulting in physical damage / bodily injury

Casualty

Automobile hacking

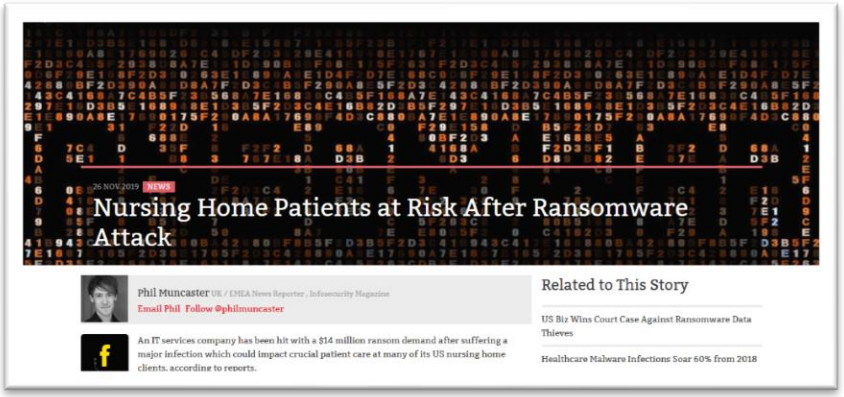
- Hack of Jeep in 2015 by a white hat/ethical hacker to show auto industry need to improve security and privacy controls (led to recall and woke up the automobile industry)
- Various motives to hack including terrorism
- Could result in physical damage, bodily injury - Think about the number of product lines that could be responsible as well as the number of parties liable
- Most (if not all) new cars are connected to the internet and Autonomous vehicles will be more prominent in the future
- New technology (such as Wi-Fi, lidar units, radar sensors and cellular connectivity), as well as the ability to cooperate with other vehicles and infrastructure, which will increase the volume of information collected, stored and transferred by vehicles
- Potential for change to provide more privacy and security regulation in future (CCPA, FTC, Alliance for Automobile Manufacturers)


ANDY GREENBERG SECURITY 07.21.15 06:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Healthcare Liability

- **Motives:** pure profit, competitors stealing information, cause chaos
- Value of medical records/PHI on darkweb is higher than PII, financial information and passwords
- Move to electronic health records including patient data and medical records
- A lot of regulatory exposure
- More and more IoT connected devices and equipment
  - Nearly full reliance on technology for operation
- Business interruption potential
- Bodily injury to patients – third party liability
- Privacy concerns with theft of a device, computer, phone
- M&A and outdated technology increases susceptibility of healthcare organizations
- Opening malicious links still problematic
- Ransomware



Life Sciences

Accenture: Life Science organizations are likely to lose USD 642 billion globally to direct cyber-attacks, over the next five years

- Drug manufacturers, biotech firms, medical device and supply companies, pharmaceutical and nutraceutical companies, clinical research and development facilities, academic institutions, clinical trial facilities
- Wide range of threat actors
  - Criminals - industry controls significant amounts of capital
  - Foreign states may look to disrupt critical drug and treatment supplies or steal technology to help their own domestic firms compete
- Typically hold highly sensitive information in relation to products and medical research - Wealth of PII and PHI
- Very reliant on third parties including IT providers, data collection, external advisors, analytic firms, contract manufacturing organizations (CMOs) and clinical research organizations (CROs)

Construction Liability

- Motives: pure profit, competitors stealing information, cause chaos
- Data of employees, client data, sub-contractor data & Intellectual Property (building specifications, architectural drawings)
- Business interruption and project delays
- Bodily injury or Physical damage
- Extortion and Wire transfer fraud
- Theft of a device
- Tamper with architectural design

- Increased reliance on technology for design, build and safety
  - Building Information Modeling (BIM)/project management/design software
    - Hackers have shown interest in building designs in recent years and sophisticated malware that targets computer-aided design programs has been identified
  - Cranes, drones, other machinery
- Third party liability - third-party vendors, clients, suppliers and subcontractors

Directors & Officers

"#CyberSecurity is frustrating for #CEO's because it is a race without a finish line." ~ Dan Glaser CEO Marsh & McLennan Companies on Bloomberg TV Daybreak http://bit.ly/2ZnjKVR #cyberrisk #leadership

Yahoo Settles Data Breach-Related Securities Suit for $80 million

By Kevin LaCroix on March 5, 2018

POSTED IN SECURITIES LITIGATION

YAHOO!

The newly disclosed $80 million settlement of the Yahoo data breach-related securities

FedEx Hit with Cyber Attack-Related Securities Suit

By Kevin LaCroix on June 28, 2019

POSTED IN SECURITIES LITIGATION

FedEx

One of the most watched and commented on corporate and securities litigation trends over the last several years has been the rise of management liability related lawsuits arising from cybersecurity-related incidents. While there has never been the

MARKEL®

Directors & Officers

Examples of scenarios and exposures include:

- Defense and Indemnity for Securities Class Actions
  - Requires material stock drop to evidence economic loss in addition to other thresholds that need to be met

- Defense and Indemnity Shareholder Derivative Claims
  - Limited success to date with broad protections including the business judgement rule and state exculpatory statutes – however, Yahoo had a settlement

- Active plaintiffs bar
- Failure to buy cyber risk insurance
- Fiduciary duty – duty of care
- Allegations that financial statements were materially false and misleading because failed to maintain adequate security measures
- Rating agency downgrade following a cyber breach
- **SEC cybersecurity disclosures and penalties**
- Inadequate collection and use of data and sale of data
- Note: Standing for injured third parties is difficult to prove (legal outcomes have varied)

Directors & Officers

Examples of Cases Against D&Os:

- **Zendesk** – October 2019 – securities class action – third party vendor breach of 15k customer accounts, 4% share price decline
- **Alphabet** – October 2019 – derivatives suit over YouTube COPPA – led to "massive fines and costly obligations"
- **Capital One** – October 2019 securities class action - 100M credit applications downloaded from cloud data server
- **FedEx –** June 2019 – securities class action stemming from losses from NotPetya attack for TNT Express - The complaint alleges that the company's share price decline over 12% on the news
- **Marriott** – December 2018 - securities class action - The complaint alleges that on the news of the breach of the guest information systems, the company's share price declined 5.5%.
- **Alphabet** – October 2018 - securities class action - Google+ breach – MC drop of $10B
- **Huazhu** – October 2018 - (Chinese hotel groups) - price of the company's ADRs declined over 12% in the five trading days following the news of the customer data leak – voluntarily dismissed
- **Chegg** – September 2018 – securities class action - shares fell 12% after news of unauthorized party access – voluntarily dismissed
- **Nielsen** – August 2018 – securities class action – GDPR related difficulties
- **Facebook** – March 2018 - securities class action dismissed without prejudice – Cambridge Analytica scandal and Earnings Miss/GDPR-readiness and compliance related – plaintiffs failed to adequately plead falsity and scienter
- **Intel** – January 2018 – securities lawsuit dismissal – design flaw in processor chips that are vulnerable to hacking

MARKEL®

Directors & Officers

Examples of Cases Against D&Os:

- **Advanced Micro Devices** – January 2018 – securities lawsuit dismissal – design flaw in processor chips that made them susceptible to hacking
- **PayPal** – December 2017 – securities lawsuit dismissal – securities vulnerabilities on TIO platform (company that PayPal acquired) - share price declined 5.75% - plaintive did not adequately plead scienter
- **Qudian** – December 2017 - (Chinese microlender) – securities class action - shares down 45% below IPO price after data leak and other developments
- **Equifax** – September 2017 – securities class action – CFO sold 13% of holdings days after breach was discovered – stock drop of 36% by September 15
- **Yahoo** – April 2017 - $80M settlement securities class action lawsuit and $29M fiduciary duty derivative suit and 35M SEC penalty
- **Wendy's –** December 2016 – derivative suit – breach of fiduciary duty – settled with $950k payment of attorney fees and agreement to adopt certain remedial and prophylactic technology and cybersecurity measures
- **Home Depot** – August 2015 - Derivative complaint -– breached duty of loyalty – settlement agreed to adopt certain cyber-security related corporate governance reforms and pay plaintiff attorney fees
- **Wyndham –** May 2014 - Derivative lawsuit – dismissed – used business judgment rule (D&O's acted in good faith or based on reasonable judgment)
- **Target –** February 2014 – derivative suit dismissed after Special Litigation Committee formed

MARKEL®

Errors & Omissions (Professional Indemnity)

- Social Engineering Fraud
  - Service providers that hold or transfer funds (title agents, real estate firms, etc.) could be targets
- IT software providers or holders of data
  - Potential risk of breach third party information held or processed
  - Software vulnerability to a breach in a product provided to clients
- Professional service firms in possession of high-value data
  - Accounting firms - sensitive financial information or corporate strategy information
  - Law firms - sensitive client information and documentation of legal strategies
  - Architects & Engineers - sensitive information – increasing use of BIM, project management and design software
- Professional standard of care - Duty of Care to Protect Sensitive Information
- Failure to fulfill contract obligations due to a cyber event
- Failure to deliver services to customers due to a cyber event
- Error in performance due to cyber event
- Includes legal defense costs
- Insurance broker E&O – Failure to suggest insured purchase a cyber policy?

MARKEL®

Kidnap & Ransom & Extortion

- Extortion payments and crisis management responses (ransomware)
- Potential business interruption coverage provided
- Some KRE insurers setting up Bitcoin wallets

Crime & Fidelity

- Fraudulent transfer of monies (i.e. CEO fraud scam/Business Email Compromise)
  - Social engineering
  - Both at times aided by employee negligence
  - Rogue employees acting alone
  - Deepfakes

Employment Practices Liability

- Coverage for breach of an Employee's PII/PHI Coverage under Invasion of Privacy grants
  - Illinois Biometric Information Privacy Act (BIPA)
- California Consumer Privacy Act (effective January 1, 2020)
- Allegations: *invasion of privacy*, emotional distress, libel/slander, failure to enforce corporate policies (class-wide quantification)

MARKEL®

Property

Physical Damage

Non-Physical

Property

- Physical Damage to Property caused by a cyber event
  - Fire, Explosion, Mechanical Breakdown, Smoke, collapse, etc.
  - Business Interruption

German Steel Plant (2014)

Baku-Tbilisi-Ceyhan pipeline (2008)

- Data Restoration - Cost to replace, restore, recreate damaged data
- Damage to Electronic Data Processing Equipment
- Business Interruption

MARKEL®

Property

- Non-Physical Damage caused by a cyber event
  - Denial of Service
    - Surge of data at the Insured
  - Service Interruption
    - Electricity, gas, fuel, steam, water, refrigeration, outgoing sewerage
    - Cloud computing service (i.e. Amazon Web Services)
    - Data, voice or video
  - "Bricking"
    - Rendering computer equipment inoperable
  - ….and resulting Business Interruption

Named perils which carve back cyber coverage – i.e. Silent Cyber

Theft

Riot & Civil Commotion

Malicious Mischief

Environmental

- Threat for contaminant releases that can result in physical damage, bodily injury and damage to human health, environmental remediation expense and significant legal liability claims
  - Catastrophic spills, Waste discharge, Air emissions
- High risk industries: pipelines, refineries, petroleum terminals, marine terminals, sewage plants, water plants and chemical plants
- SCADA system reliant industries such as energy, transportation, public service, chemical manufacturing
- Industrial industries dealing with hazardous materials such as power plants, refineries, factories, water treatment facilities or pipelines

Scenarios/Examples:

- Iranian attack on NY Dam in 2013– dam was 25 miles north of NYC
- Sewer discharge – In April 2000, a hacker caused the release of 800k liters of untreated sewage into waterways in Maroochy Shire, Australia
- Georgia Institute of Technology researchers created a ransomware capable of taking control of a water treatment plant and threatened to cut off the supply system and even poison the water supply for the entire town by increasing chlorine levels


WORLD + JUSTICE

Iranian Cyber Attack on New York Dam Shows Future of War

Marine

- Threats to vessels and cargo – modes of attack include insiders, targeted attacks on IT or OT, use of ransomware
- Motivations: stealing money, moving cargo, stealing information, causing disruption or loss
- Potential weaknesses include inadequacies in design, system integration and/or system maintenance as well as lack of cyber discipline
- Software vulnerabilities in:
  - Vessel navigation and propulsion system (GPS, AIS – Automatic Identification System, ECDIS – Electronic Chart Display and Information System) all vulnerable
  - Cargo handling and container tracking systems at ports and on board ships
  - Shipyard inventories and automated processes
- Scenarios:
  - Cyber-attack disabling a vessel transiting the Panama Canal resulting in blockage of a channel could have significant economic impact around the globe
  - Cyber-attack disrupting navigation of large cruise ship could result in media coverage and could, in the worst circumstances, lead to loss of life and property damage
  - Port of Antwerp (2011-2013) – Hackers worked with drug smuggling gang to identify shipping containers in which consignments of drugs had been hidden


BuzzFeed News How Pirates And Hackers Worked Together To Steal Millions Of Dollars In

TECH

How Pirates And Hackers Worked Together To Steal Millions Of Dollars In Diamonds

MARKEL®

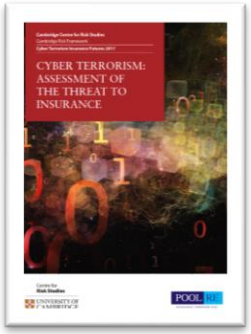
Aviation

- Cyber terrorism, malicious act or sabotage
- System failure or inadvertent cyber cause
- Extortion and loss of information
- Air traffic control (ATC) systems, flight management systems, global navigation satellite systems (GNSS)
- Technological advances offer more vulnerabilities/opportunities to exploit:
  - Tablet-based electronic flight bags (EFBs)
  - In-flight entertainment and Wi-Fi connectivity systems (IFEC)
  - NextGen - integrated use of the GPS network for aircraft navigation and ATC surveillance)
- Examples/scenarios include:
  - 2008 Spanair flight 5022 – 154 killed - central computer system infected with malware – if detected may have prevented plane from taking off
  - System failure – British Airways, Delta, United, Southwest (grounds for coverage under AVN60 Extended Personal Injury Cover, Aviation Liability Cover, Excess Non Aviation Cover
  - Network outage impacting Airport Operational Database (ODB)

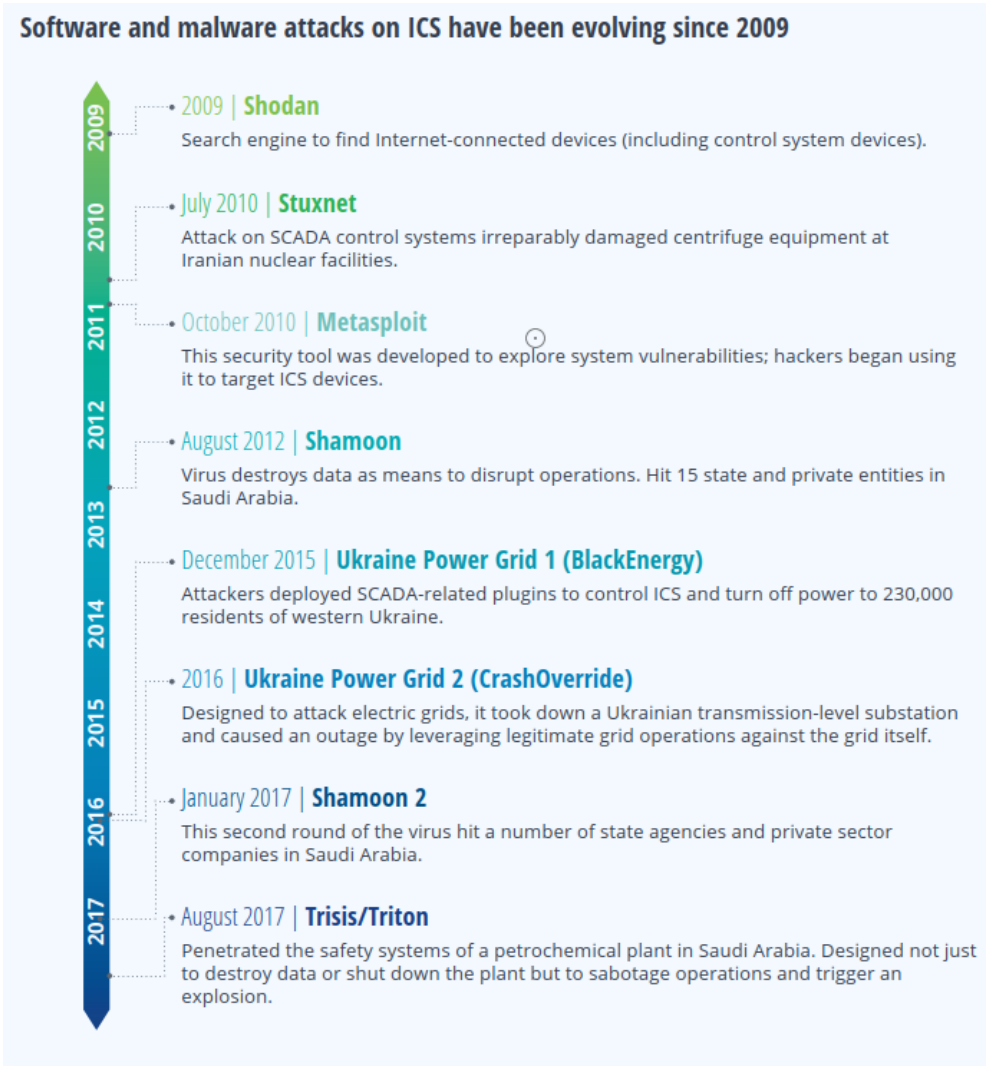
MARKEL®

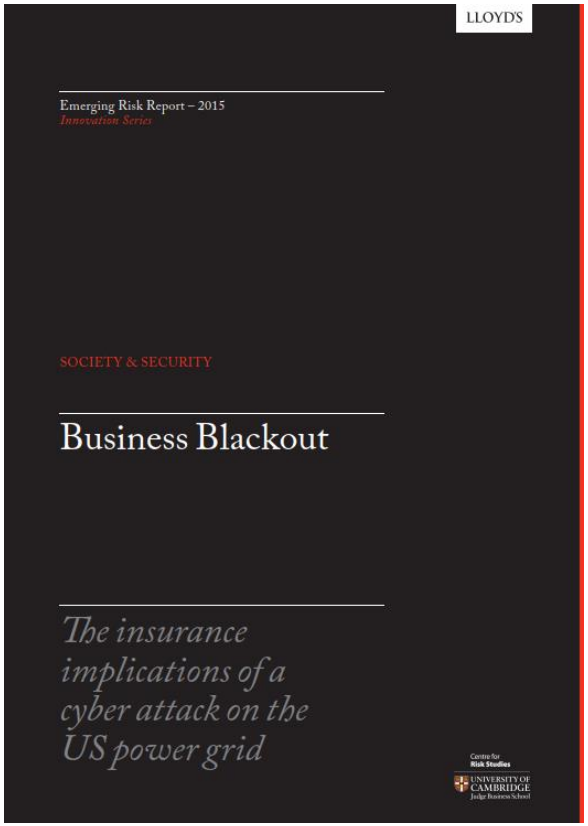
Terrorism

- IoT, Big Data and Quantum Computing created new and diverse security challenges
- Increased networking of facilities management and ICS has exposed new attack vectors
- Possibility to destroy both lives and property via remote digital interference
- Potential perpetrators are Non-State Terrorist Organizations and Nation State Cyber Teams
- Attribution issues – forensics take time and evidence can be destroyed if physical damage
- Scenarios (40 provided in Cambridge Study)
  - Chemical Reactor/Airplane/Rail Infrastructure Targets more concerning
- 2009 – Stuxnet worm – physical damage to Iranian nuclear centrifuges (U.S. and Israel)
- 2015 and 2016 Ukraine blackouts



Energy





https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout

Source: Deloitte

Energy

Actors:

- Internal: human error, disgruntled employees, or contractors
- Nation states and organized crime: becoming more active and could be intersecting

Motives: Steal PII and financial data, cause damage to property and operational systems

- Upstream and midstream: significant business interruption, property damage or bodily injury
- Downstream: data exposure risk that could result in litigation, expense and regulatory scrutiny, physical impact concerns

Potential Damages:

- Physical damage caused by the failure of ICS / vital safety systems
  - ICS and SCADA now routinely connected to the internet
- System or data issue causes a shutdown of one or more facilities - business interruption and additional expenses
- An incident which results in the total or partial destruction, encryption, corruption etc. of data or specialist software / programs including loss of valuable research data (seismic data, exploratory data, production data etc.)
- Liabilities arising from a contamination incident, injury or death
- Phishing and spear-phishing common in energy; Metasploit being used
- Target for ransomware attacks
- A lot of supply chain risk

Where To Go From Here?

The path forward is not linear given the dynamic nature of the market.

Several incentives to eradicate silent cyber and remove coverage ambiguity

- Provide **transparent coverage to insureds** and make sure they are protected
- **Prevent losses** associated with claims that were not priced for in the products
- Understand and **limit exposure to aggregation risk**
- Opportunity to **explore new business** and growth in the market
- **Reinsurers** increasingly want to understand level of exposure
- **Rating agencies and regulators** increasingly expect insurers to quantify and manage cyber risk

.

MARKEL®

Where To Go From Here?

1 Identification

- Review each insurance product line for exposure
- Review policy wording for coverage, gaps, exclusions
- Establish or revise underwriting questions and processes

2 Quantification

- Attempt to capture price for risk
- Build risk capture into systems

3 Management

- Train underwriters on cyber risk
- Decide on strategy (exclusions / sub-limits / opportunistic full limit)
- Update policy forms
- Update systems for data capture
- Aggregation monitoring / reporting

Challenges:

- Untested courts
- Evolving risk
- Evolving regulations
- Competitive environment
- Lack of claims data

MARKEL®

Questions?

Appendix: Lloyd's Bulletin Y5258 – Phase 1

Appendix 1 - Phase 1 'First-Party Property Damage' lines of business

The following Lloyd's classes of business are included in Phase 1 'First-Party Property Damage' lines of business:

- Energy Construction
- Energy Offshore Property
- Energy Onshore Property
- Nuclear
- Power Generation
- Cargo
- Fine Art
- Marine Hull
- Marine War
- Specie
- Yacht
- Difference in Conditions
- Property D&F (non-US binder)
- Property D&F (non-US open market)
- Property D&F (US binder)
- Property D&F (US open market)
- Engineering
- Livestock & Bloodstock
- Terrorism

Appendix: Developing Case Law

Mondelez International Inc. v. Zurich (Circuit Court of Cook County, IL)

- Issue: Can a policy exclusion for losses or damage resulting directly or indirectly from a **"hostile or warlike action in time of peace or war"** carried out by a government, sovereign power or military force be applied to a ransomware event?

- Policy Analyzed: "All Risks" Property Insurance Policy – policy has express coverage for cyber perils, including…
  - *"physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction"*

- Elements of the claim:
  - Financial losses suffered from the "NotPetya" ransomware attack
  - Two of Mondelez's servers were infected with NotPetya malware and "rendered permanently dysfunctional" 1,700 of its servers and 24,000 of its laptops
  - CIA and sister agencies in the UK, Australia and Canada have attributed "NotPetya" with the Russian military

Appendix: Energy

Month/Year	Company Affected	Details of the Cyber Attack	Region
Jan-16	PetroBangla	The website of the company was hacked few hours after the hacking	Asia-Pacific
Dec-15	Bharat Coking Coal Limited	The site was hacked for the 2nd time in 3 months	Asia-Pacific
Dec-15	Saudi Aramco	Company received fake invoices which resembled invoices of ONGC	EMEA
Dec-15	Ukrainian electricity distribution companies	About 80,000 customers in Ukraine's Ivano-Frankivsk region experienced power cuts	
Oct-15	British Gas	E mail addresses & passwords of 2,200 customers appeared online	EMEA
Oct-15	Oil & Natural Gas Corp	Company lost Rs 197 crores because of an email fraud	Asia-Pacific
Jul-15	Korea Hydro & Nuclear Power Corporation	The company's sensitive internal data was leaked online on 8th July 2015	Asia-Pacific
May-15	Charles Harvey Eccleston, former employee of Department of Energy	Eccleston was charged with an attempted email "spear-phishing" attack in January 2015 targeting Department of Energy employee email accounts	N.America
Apr-15	UP Power Corporation Limited	The company's online billing system was hacked and power bills of consumers was affected	Asia-Pacific
Dec-14	Indian Oil Corp Ltd	The company's website was hacked by a Turkish group named 'TurkGuvenligi'	Asia-Pacific
Dec-14	Korea Hydro and Nuclear Power Co Ltd	Hackers sent 5,986 phishing emails containing malicious codes to 3,571 employees of the nuclear plant operator to extract sensitive information	Asia-Pacific
Nov-14	Pemex	The mail box of 'Emilio Lozoya Austin', CEO of Pemex was hacked	LATAM

Source: Aon

MARKEL®

Appendix: Energy

Year	Company Affected	Details of the Cyber Attack	Region
2013	Austrian and German power grid	Power grid nearly broke down after a status request command packet, which was broadcast from a German gas company as a test for their newly installed network branch, found its way into the systems of the company and monitoring network.	EMEA
2012	Saudi Aramco	The cyber attack affected about 30,000 computers of Saudi Aramco. The malware used known as: 'W32.Disttrack' consisted of a dropper, a wiper & a reporter module. Every office was physically unplugged and isolated from the rest of the world. Payments were affected and so were oil production, drilling and other related activities	EMEA
2008	Multiple entities	A senior CIA official announced that cyber attacks had taken out power equipment in multiple cities outside the United States. Hackers threatened to extend the blackouts and demanded money from few energy companies	USA
2003	Ohio nuclear power plant	Ohio nuclear power plant's safety monitoring system went offline unexpectedly for several hours due to a Slammer worm infection. The incident didn't cause harm since the plant was offline to facilitate maintenance operations	USA
2001	California's power distribution center	Attacker infiltrated servers and tried to further penetrate the network. The objective seemed to disrupt the flow of electricity across California	USA
2000	Russian gas extraction company	Attackers used a Trojan to gain access to the system which controlled the gas pipelines	EMEA

Source: Aon

MARKEL®