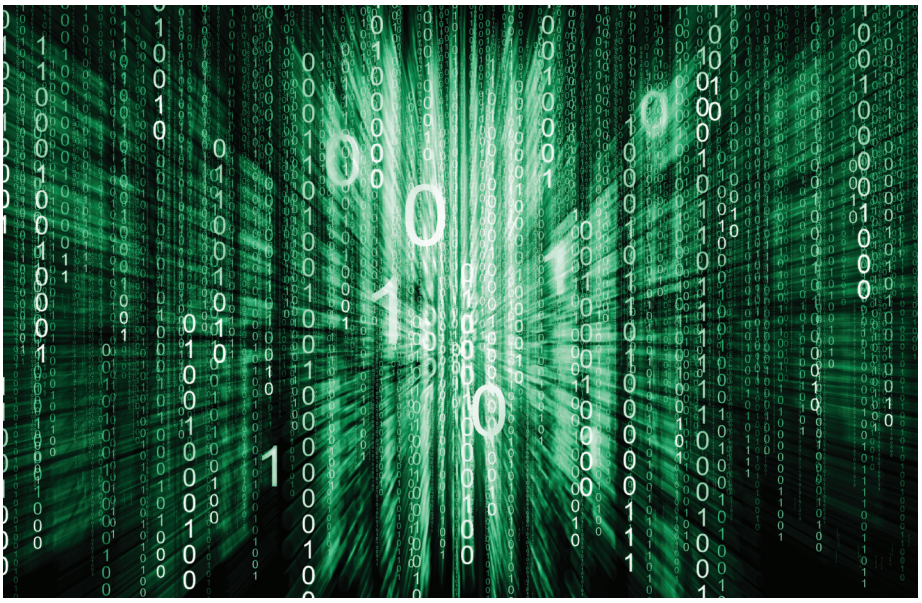
# What isn't Vulnerable to Cyber Attack?

**IT-based technologies have facilitated immense advances in practically all human endeavors. Huge upside, but with these capabilities comes a spectrum of (growing) risks relating to cyber attacks. The re/insurance industry has reacted and the market for cyber insurance continues to expand and evolve. Here we (1) review cyber risk, (2) explore it from a less publicized 'physical property' perspective with example losses from the energy sector, and (3) introduce insurance considerations for this important growth market. Upshot: cyber risk protection of all types is not just an 'add-on'; smart cyber risk solutions are the only way forward for a healthy, sustainable and effective cyber re/insurance market.**



## Ever-increasing vulnerability from the 'Internet of Things'

The modern world is becoming increasingly reliant on, controlled and interconnected through computers, networks and the internet, made all the more vulnerable by cloud and mobile technologies. It has been estimated, for example, that the world now has close to 25 billion connected IT devices (such as PCs, servers, routers, industrial control systems, medical machinery and operational technology). We live in a world where sensors can detect gestures, touch and changes in the environment, data can be transferred by radio frequency electromagnetic fields, where microelectromechanical systems (MEMs) can interact with their surroundings (e.g. microsensors) and where near field communication (NFC) chips are changing the way we make payments with mobile devices. So-called 'Internet of Things Applications' impact all sectors of our economies, for example:

- Manufacturing: tracking machinery and monitoring performance (wireless inventory tracking, control of industrial processes), tracking the flow of raw materials and supply chains.
- Retail: tracking shipments and logistics, optimization of supply chain through shelf sensors.
- Infrastructure and power generation: smart electrical grids, smart cities, traffic systems, emergency services.
- Health: monitoring and transferring data for chronic medical conditions (e.g. glucose levels), exercise.
- Consumer products and vehicles: security devices, mobile devices, advanced driver assistance systems (ADAS), monitoring driving history.

With the potential to cause major disruption and money to be made through data theft and extortion – and with remote chance of capture – cyber crimes are following suit, becoming ever more targeted and sophisticated. Indeed, from light bulbs and traffic lights to medical devices and critical infrastructure control systems, almost all electronic equipment can be hacked. And with so much interconnectivity and complex supply chains, the impact of an attack in one place can have far-reaching consequences. Cyber risk thus represents a major and systemic risk to business and critical infrastructure, impacting financial services, energy and water supply, communications, food, health and safety, transport and emergency services.

## Cyber risks

A cyber event can be instigated either from external parties (remote, unauthorized access) or by insider misuse:

- Web application attack
- Attack using crime ware (malware)
- Phishing attacks (faked legitimate sites to steal personal and password data)
- Logic bombs; small errors leading to major corruption over time (months to years) and almost impossible to identify.

Resulting in theft, disruption and/or damage to data and intellectual property, as well as to physical property:

- Data breach/espionage/misuse of data
- Loss or corruption of data and back-ups
- Denial of service/system breakdown/ loss of access to internet
- Physical damage/infrastructure failure
- Loss of production/loss of revenue/ quality issues
- Reputational damage
- Extortion.

Financially, cyber attacks result in multiple costs, including customer/third-party liabilities and lost revenues (direct and from subsequent reputational damage), notification costs, fines and penalties, legal fees, repair/reinstatement costs for data and physical property and increased costs of working, e.g. for crisis management and public relations.

## Risk management and regulation

This is not an unknown risk; most companies, large and small, apply anti-virus software and other security measures. There is, however, a significant difference in risk mitigation spend; a recent U.S. study[1] for example found that large enterprises allocate an average 12% of their IT budget on cyber security, as oppose to 4% by SMEs. Yet, SMEs represent an important section of our economies (for example, more than 50% of U.S. sales derive from SMEs) and often serve as important suppliers to major industries. SMEs are also a relatively soft target for hackers and could be ruined by even a relatively minor attack.

Beyond budget allocation, the phenomenal pace at which cyber risk is evolving means that, for all companies, identifying, measuring and implementing the full scope of necessary cyber security measures is a major ongoing challenge. Companies need to be able to prevent unknown as well as known attacks, as well as attacks from the inside. For risk assessment, it is also critical to have as much knowledge as possible regarding supply chain interconnectivity. In addition to IT security measures, risk can be mitigated by:

- Introducing a culture of cyber awareness
- Integrating cyber risk into the risk management framework
- Implementing effective crisis management to mitigate losses and recover as quickly as possible after an attack (in particular to reduce potentially devastating reputational damage).

As regards regulation for data breaches, the U.S. Securities and Exchange Commission (SEC) guidance, implemented in 2011, calls on public companies to address their exposure to cyber attacks and to discuss how they will respond financially to potential loss; 46 out of 50 states now have compulsory notification laws in place. All maintain that the data controller[2] is ultimately responsible for a breach.

The U.S.'s National Institute of Standards and Technology has also developed a framework for critical infrastructure that can be used by companies to evaluate their cyber risk exposure[3].

The EU is planning to implement a cyber security directive by Q3/2015. EU Member States must bring into force the necessary laws, regulations and administrative provisions. The Directive does not cover breaches of personal data, but rather systemic cyber attacks that compromise data systems. The following providers must adopt risk management practices and report any major security incidents affecting their core services:

- Operators of critical infrastructure (energy, health, transport, financial services)
- Enablers of information society services, such as app stores, e-commerce platforms, cloud computing, search engines and social networks
- Public administrations.

While regulatory requirements help to promote better identification and management of cyber risk, they also increase the re/insurance exposure across all business sectors. In addition, with U.S. and EU regulation stipulating that liability rests with the data controller, exposure is further increased by the trend to outsource data handling and storage, and by the increasing use of mobile technologies and cloud computing.

## Risk frequency and severity

Worldwide, cyber attacks have increased dramatically over the last few years, with the greatest concentrations in the U.S., U.K., Australia and Japan. The much-quoted 2014 Verizon report[4] analyzed security breach data from a cohort of 50 global organizations spanning 95 countries; it presents an hundred-fold increase in data breaches over the past decade.

It is often difficult to calculate the full financial severity of a cyber attack, but minimum costs arising out of major data breaches are generally in the hundred millions; for example, TJX (2006), theft of 24 million records, estimated cost $ 172 million[5]; Heartland Payment Systems (2008), theft of 130 million records, estimated cost $ 145 million[6]. A 2014 data breach study[7] reported a U.S. average (combined direct and indirect) cost of a data breach per record of $ 201[8] and an average organizational cost per breach for the U.S. of $ 5.85 million. In terms of insured costs, the average loss in 2013 was estimated to be just shy of $1 million[9]. The U.K. government has estimated that cyber attacks cost the U.K. economy approximately £ 400 million a year.

## Property scenarios from the energy sector

The energy sector has suffered a disproportionately large number of severe cyber attacks. For example in the U.S., 41% of all cyber attacks reported in 2012 that were directed at critical infrastructure targeted the energy sector[10]. Of the examples listed below, Natanz (2010) was in fact the first to bring the world's attention to the vulnerability of physical (rather than non-physical) property to cyber attack.

- Natanz, Uranium Enrichment plant, 2010 Stuxnet
- Chevron, 2010 virus
- Saudi Aramco, 2012 Shamoon virus
- RasGas, 2012 hacker attack
- Various powerplants, 2014 "Dragonflyhacker group".

[1] Advisen 2014 Cyber Risk Insights Conference – London.
[2] In general, data controller refers to a person (as recognized in law, usually organisations) who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. The U.K.'s Information Commissioner's Office (ICO). http://ico.org.uk.
[3] Framework for Improving Critical Infrastructure Cybersecurity (2014). The U.S.'s National Institute of Standards and Technology (NIST). www.nist.gov.
[4] 2014 Data Breach Investigations Report. Verizon Enterprise Solutions (2014).
[5] e.g. news items from www.businessweek.com; www.consumeraffairs.com.
[6] e.g. news items from www.bankinfosecurity.com; www.csmonitor.com.
[7] 2014 Cost of Data Breach Study: Global Analysis. Ponemon Institute (2014).
[8] The average cost per data breach (2014) varied by country from $ 51 to $ 201.
[9] Net Diligence 2013 Cyber Liability & Data Breach Insurance Claims.
[10] ICS-CERT Monitor (October-November-December 2012), page 5.

In terms of damage to physical property and the consequent business interruption, the virus in Saudi Armco, for example, resulted in the destruction of more than 30,000 PCs and 2,000 servers, with IT systems disconnected from the internet for two weeks. In 2010, the Stuxnet virus gained access to the (ring-fenced) operational technology of the plant; it recognized, targeted and manipulated part of the industrial control system responsible for spinning the plant centrifuges. The manipulation of operational technology represents a substantial property risk.

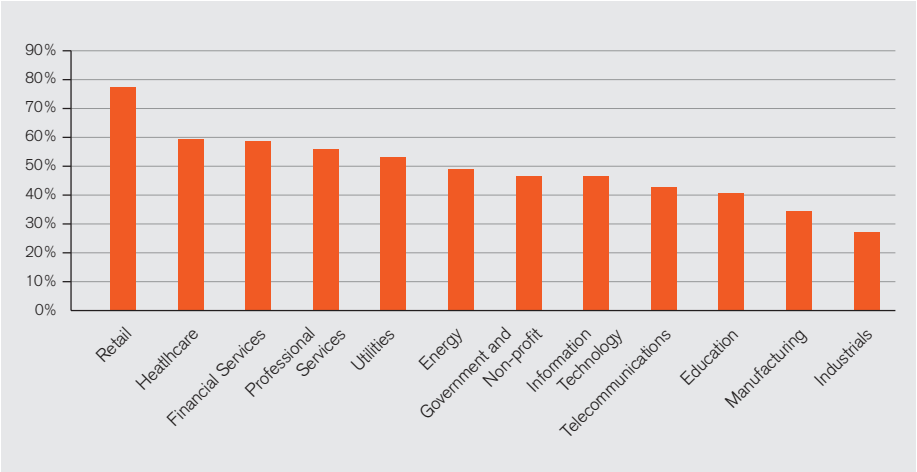



**Figure 1:** Results of a U.S. underwriter market survey showing the percentage of respondents reporting an increase in demand for cyber liability protection by industry sector. Source: PartnerRe and Advisen[11].

## Re/insurance

The resulting loss/damage categories from a re/insurance perspective:

- Third-party liability; all forms impacted, from GL to Professional Indemnity and D&O covers (failure to properly evaluate, manage and protect against cyber crimes)
- Property damage (loss of data and physical damage to machinery, servers, hardware, software and data, including back-ups)
- Business interruption losses following property damage
- Non-physical damage business interruption.

The cyber insurance market is steadily growing and to date there are over 60 insurers globally offering cyber insurance solutions on a stand-alone basis or by endorsement. Pricing and wordings vary significantly across global markets. The 2014 gross written premium is approximately $ 2 billion, this is expected to reach $ 5–10 billion as the worldwide demand for and availability of such products increases over coming years.

Interestingly, the penetration rates for cyber insurance mirror that of IT security spend; the higher the revenue of a company, the more likely it is to buy cyber insurance. Penetration is highest in the healthcare, retail, hospitality and financial service sectors.

Despite the vulnerability and significant loss potential, cyber insurance cover is almost totally absent for physical damage and limited for business interruption (non-physical damage and property damage). For these there remains a lack of clarity amongst insureds over the exact exposure potential, irritation at the limited availability of protection and confusion linked to non-standardized covers.

The result of all these factors is that insureds are increasingly asking for cyber protection to be added to their existing liability and property covers either through endorsement, or (and where we have particular concern), by removing the cyber exclusion.

## Cyber insurance: not just an add-on

Cyber risk has generally been excluded from both standard general liability (GL) and property re/insurance covers. However, in today's softer market and with demand for financial re/insurance protection for cyber risk on the up and with pressure from insureds, there is an increasing tendency for cyber exclusions – such as CL 380 or NMA2915 – to be removed from GL and property wordings. Given the systemic, complex nature of this risk, high exposure and current lack of data upon which to assess the risk and build a strong underwriting platform, this is a problematic approach.

A sustainable re/insurance market that offers insureds proper protection now and in a fast-evolving future is one that delivers smart insurance and reinsurance solutions. These solutions will need to be properly underwritten, either as stand-alone covers or endorsements, be based upon and encourage effective risk assessment and mitigation measures, and be supported by strong risk management and accumulation control.

Success will be heavily determined by the terms and conditions of the cover; adequate risk premium and occurrence limits supported by sub-limits and deductibles. This in turn requires greater understanding of the interconnectedness of risks, and critically, industry initiatives to access greater volumes of cyber loss data.

## PartnerRe cyber solutions

PartnerRe has developed specialty expertise in cyber risk protection for clients in worldwide markets and is active in cyber risk conferences and discussions – our aim is to share insight, to be proactive in developing a stable market and to create innovative risk solutions that meet the needs of our clients. If you would like to discuss this topic and find out how PartnerRe can help your business, please go to www.partnerre.com for contact and company information.

**Contributor**
Markus Bassler, Head of Energy & Special Risks, PartnerRe

www.partnerre.com

PartnerRe

[11] Cyber Liability Insurance Market Trends. Advisen Ltd. Sponsored by PartnerRe. October 2014.