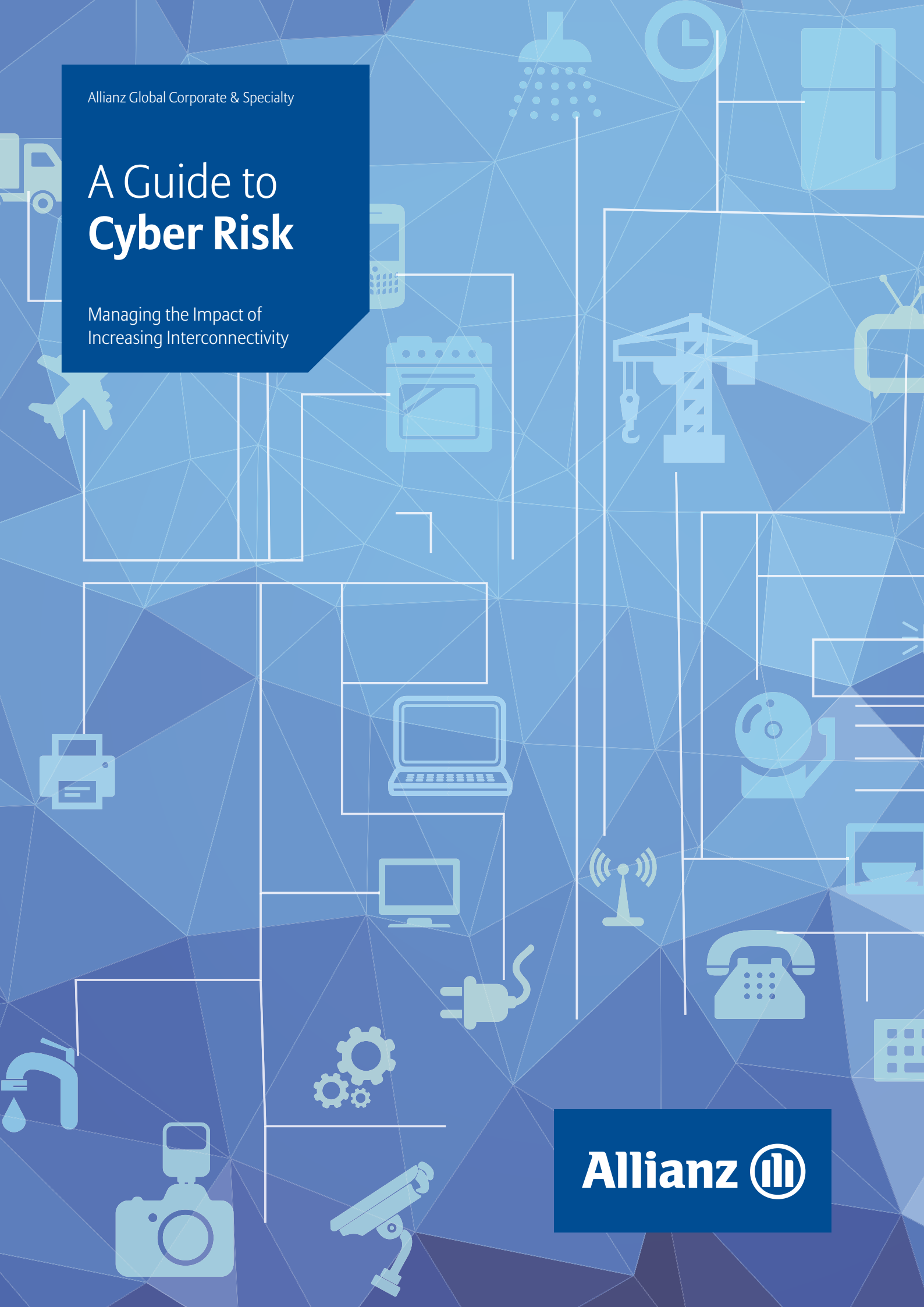
Allianz Global Corporate & Specialty

A Guide to **Cyber Risk**

Managing the Impact of Increasing Interconnectivity



Allianz

Scope of the Report

Cyber risk is now a major threat to businesses. Companies increasingly face new exposures, including first-and third-party damage, business interruption and regulatory consequences. With the operating environment for many industries changing dramatically, as they become more digitally-connected, this report examines cyber risk trends and emerging perils around the globe. It also identifies future mitigation strategies, including the role of insurance.

About Allianz Global Corporate & Specialty

Allianz Global Corporate & Specialty (AGCS) is the Allianz Group's dedicated carrier for corporate and specialty insurance business. AGCS provides insurance and risk consultancy across the whole spectrum of specialty, alternative risk transfer and corporate business: Marine, Aviation (incl. Space), Energy, Engineering, Entertainment, Financial Lines (incl. D&O), Liability, Mid-Corporate and Property insurance (incl. International Insurance Programs).

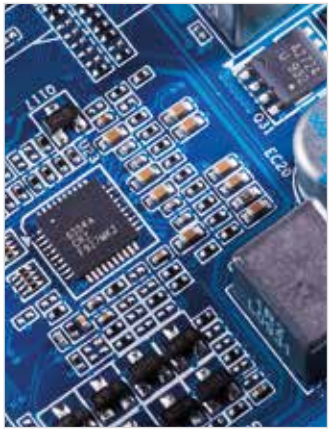
Worldwide, AGCS operates in 28 countries with own units and in more than 160 countries through the Allianz Group network and partners. In 2014 it employed more than 3,500 people and provided insurance solutions to more than half of the Fortune Global 500 companies, writing a total of €5.4bn gross premium worldwide annually.

AGCS SE is rated AA by Standard & Poor's and A+ by A.M. Best.

For more information please visit **www.agcs.allianz.com** or follow us on **Twitter @AGCS_Insurance**, **LinkedIn** and **Google+**.

All $ US$ unless stated

Contents



Executive Summary

$445bn

Estimated annual cost to the global economy from cyber crime[3]

$200bn+

Estimated annual cost to the world's largest four economies – the US, China, Japan and Germany

50%

The top 10 economies account for approximately 50%+ of cyber-crime costs

The cyber risk landscape today

Increasing interconnectivity, globalization and **"commercialization"** of cyber-crime are driving greater frequency and severity of cyber incidents, including data breaches.

Data privacy and protection is one of the key cyber risks and related legislation will toughen globally. More notifications of, and significant fines for, data breaches can be expected in future. Legislation has already become much tougher in the US, Hong Kong, Singapore and Australia, while the European Union is looking to agree pan-European data protection rules. Tougher guidelines on a country-by-country basis can be expected.

Business interruption (BI), intellectual property theft and cyber-extortion – both for financial and non-financial gain – risk potential increasing. BI costs could be equal to – or even exceed – direct losses from a data breach.

Attacks by hackers dominate the headlines but there are many **"gateways"** through which a business can be impacted by cyber risk. Impact of BI triggered by technical failure is frequently underestimated compared with cyber-attacks.

Vulnerability of industrial control systems (ICS) to attack poses a significant threat. To date, there have been accounts of centrifuges and power plants being manipulated. However, the damage could be much higher from security sensitive facilities such as nuclear power plants, laboratories, water suppliers or large hospitals.

Cyber security and protection best practice

Cyber risk is the risk most underestimated by businesses according to the **Allianz Risk Barometer**[1] but there is no **"silver bullet"** solution for cyber security.

In addition to damages paid due to loss of customer data and impact of BI, loss of reputation can be a significant cause of economic loss for businesses after a cyber incident.

Monitoring tools, improved processes and greater employee awareness can help companies to be more prepared.

Businesses need to identify key assets at risk and weaknesses such as the "human factor" or overreliance on third parties. Employees can cause large IT security or loss of privacy events, either inadvertently or deliberately.

Businesses need to create a cyber security culture and adopt a **"think-tank"** approach to tackling risk. Different stakeholders from the business need to share knowledge. Implement a crisis or breach response plan. Test it.

Cyber risk is constantly evolving. **"Hidden risks"** can emerge. For example, businesses should consider how merger and acquisition **(M&A)** activity and changes in corporate structures will impact cyber security and holding of third party data in particular.

Companies need to make decisions around which risks to avoid, accept, control or transfer.

1 *Allianz Risk Barometer surveys over 500 risk managers and experts from 40+ countries.*

Cyber risk and insurance – future trends and growth

The standalone cyber insurance market will continue to evolve but development will bring challenges, with many concepts and wordings yet to be tested, potentially resulting in litigation. This is not unusual with new products and can improve risk knowledge.

Education – both in terms of businesses' understanding of exposures and underwriting knowledge – must improve if insurers are to meet growing demand. Other challenges exist around pricing, modeling of risk aggregation and incidents resulting in physical damage.

The cyber insurance market is currently estimated to be worth around **$2bn** in premium worldwide, with US business accounting for approximately 90%. Fewer than 10% of companies are thought to purchase cyber insurance today. However, the cyber insurance market is expected to grow by double-digit figures year-on-year and could reach **$20bn+** in the next 10 years.

Growth in the US is already underway, driven by data protection regulation. Legislative developments and increasing levels of liability will help growth accelerate elsewhere, as will a growing number of small- to medium-sized enterprises **(SMEs)** seeking cover.

Sectors holding large volumes of personal data, such as healthcare and retail, or those relying on digitalized technology processes, such as manufacturing and telecommunications, are most likely to buy cyber insurance at present. However, there is growing interest among financial institutions and the energy, utilities and transport sectors, driven by the increasing perils posed by interconnectivity.

Data protection and liability risks dominate the cyber landscape today. Impact of BI from a cyber incident and further development of interconnected technology will be of increasing concern to businesses over the next decade and will spur insurance growth.

Businesses are also exposed to cyber risk through supply chains and, increasingly, will need to consider the impact of an incident in this area, such as the liability they could face if they cannot deliver their products or lose customer data, as well as the costs to resolve such issues. Companies will increasingly look to extend protection to their supply chains.

Emerging risks: impact of technology

"The Internet of Things" will have an increasing influence on the world in which we live and businesses operate. Estimates suggest as many as a trillion devices could be connected by 2020. New technologies create new vulnerabilities. Cyber criminals could exploit this increase in interconnectivity.

Businesses are driven by real-time data. Any interruption of the process chain – even for a minute – could cause a severe business interruption, impacting the balance sheet.

As technology evolves, older devices that remain in use could also create vulnerabilities, especially where they rely on outdated operating systems and unsupported software.

The use of outsourced services and storage – such as the **cloud** – brings risks, as well as benefits. One issue at a cloud provider could result in large BI and data breach losses for many.

The prospect of a catastrophic cyber loss is becoming more likely. An attack or incident resulting in a huge data loss or BI – and the subsequent reputational damage – could put a large corporation out of business in future.

A successful attack on the core infrastructure of the internet; for example main protocols such as Border Gateway Protocol (BGP) or Domain Name System (DNS), could be devastating[2].

A major cyber-attack or incident involving an energy or utility company could result in a significant outage, physical damage, or even loss of life in future, while a cyber war between two countries could disrupt internet services around the world.

Interest in protecting critical infrastructure is likely to see governments becoming increasingly involved in cyber security, resulting in greater levels of scrutiny and liability.

2 *Cyber Security In An Interconnected World: Recent Critical Events In A Nutshell, Allianz Group Economic Research*
3 *Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee*

The cyber risk landscape today...

5 top trends in **cyber risk**

- **Increasing interconnectivity and "commercialization" of cyber-crime driving greater frequency and severity of incidents, including data breaches**
- **Data protection legislation will toughen globally. More notifications and significant fines for data breaches in future can be expected**
- **Business interruption (BI), intellectual property theft and cyber-extortion risk potential increasing. BI costs could be equal to – or exceed – breach losses**
- **Vulnerability of industrial control systems poses significant threat**
- **No silver bullet solution for cyber security**

Cyber risk is complex and forever-changing. Attacks and incidents are increasing with costs climbing into the multimillions. There are certain risks that cause the most concern; most notably those around data breaches and the potential for significant business interruption.

$3.8m

The average cost of data breaches is rising for companies around the world, up from **$3.5m** a year earlier[1]

What is hacktivism?
The subversive use of computers and computer networks to promote a political agenda.

Security breaches

Over the past decade, data breaches involving personal data have become a major concern for many organizations, both in the private and public sector. Major corporations, governments and public services have all been targeted by cyber criminals or so-called hacktivists.

Since 2005 there have been 5,029 reported data breach incidents in the US, where organizations must report data breaches to regulators, involving more than 675 million estimated records, according to the Identity Theft Resource Center[2].

Statistics outside the US are patchy. However, there have been at least 200 breaches in Europe involving 227 million records since 2005, according to an estimate by the Center for Media, Data and Society at the Central European University[3].

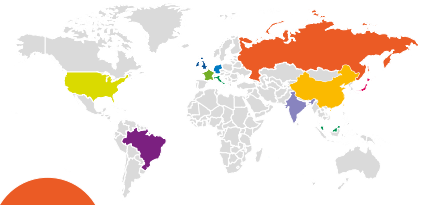
Some of the largest breaches include the likes of US retailers Target and Home Depot, health insurer Anthem, entertainment and electronics firm Sony and investment bank JPMorgan Chase.

The Target data breach in 2014, in which the personal details of some 70 million people may have been compromised, was one of the largest in history. It has been reported that it has cost the company well in excess of $100m, not including damage to reputation and loss of business, and was followed by the company's chief executive leaving the post [4].

1 *2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute*
2 *www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html*
3 *cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope.pdf*
4 *www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/*

How much does **cyber-crime** cost the world's leading 10 economies?

This **AGCS** atlas examines the estimated total cost to the global economy from cyber-crime per year, with a particular focus on the impact on the world's top 10 economies, according to GDP.



$445bn[1] annual cost to the global economy

[1] CSIS/McAfee

Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]	Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]
1	**US** $16.8trn	.64%	$108bn	6	**UK** $2.7trn	.16%	$4.3bn
2	**China** $9.5trn	.63%	$60bn	7	**Brazil** $2.4trn	.32%	$7.7bn
3	**Japan** $4.9trn	.02%	$980m	8	**Russia** $2.1trn	.10%	$2bn
4	**Germany** $3.7trn	1.60%	$59bn	9	**Italy** $2.1trn	.04%	$900m
5	**France** $2.8trn	.11%	$3bn	10	**India** $1.9trn	.21%	$4bn

Sources: [1]World Bank (2013) [2]Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee [3]Allianz Global Corporate & Specialty

42.8m

The number of detected cyber-attacks skyrocketed during 2014 – up **48%** at roughly **117,339** incidents per day[1]

1 *The Global State of Information Security Survey 2015, PricewaterhouseCoopers*

Increasing trend

The frequency and sophistication of cyber-attacks and incidents continues to increase and looks likely to do so for the foreseeable future.

"As recently as 15 years ago, cyber-attacks were fairly rudimentary and typically the work of hacktivists," says **Allianz Global Corporate & Specialty (AGCS) CEO, Chris Fischer Hirs**.

"But with increasing interconnectivity, globalization and the commercialization of cyber-crime there has been an explosion in both frequency and severity of cyber-attacks," he adds.

"In addition incidents on computer/network infrastructures (outages, disruptions of different sizes and scales) are also occurring. However they are not reported due to fears about loss of reputation or lack of legal requirements and, thus, don't make the headlines. Alternatively, businesses manage these internally due to lack of insurance," says **Georgi Pachov, Group Practice Leader Cyber, CUO Property, AGCS**.

Enter the darknet...
The **darknet** is an encrypted part of the internet that can only be accessed with specific software, configurations, or authorization – and is where an increasing list of criminal activities are traded anonymously.

Guns, explosives, counterfeit documents – including money and credit card numbers – alternate identities and even uranium are just some of the items available for sale. The darknet is where commercialization of cyber-crime also continues to evolve, with hackers trading and developing computer "bugs", creating further potential for future incidents.

Potential risk scenarios from cyber-attacks/incidents

- Critical data is lost
- Customers may be lost and business interrupted
- Property damage
- Theft
- Adverse media coverage/damage to reputation/ lower market share – 71% of customers said they would leave an organization after a data breach[1]
- Regulatory actions and associated fines and penalties
- Profits impacted/value of shares may fall
- Loss of trade secrets/confidential information
- Extortion
- Breach of contract
- Product recall
- Notification costs and other response costs; i.e. forensic IT
- Network security liability
- Directors' and officers' liability

Shifting regulatory landscape

Awareness of cyber risk is highest in the US, where strict data protection laws require companies to notify individuals of a breach.

Outside the US, data protection regimes differ by country, but there is now a general trend towards tougher rules as governments look to bolster cyber security.

"Legislation has already become much tougher in the US. Hong Kong, Singapore and Australia all have new data protection laws, and Europe looks to be heading in the same direction," says **Nigel Pearson, Global Head of Fidelity, AGCS** *(see map featuring commentary from law firm Clyde & Co on page 9)*.

The European Union (EU) is currently reviewing its data protection law, looking to introduce a new harmonized regime. While the exact scope and shape of the proposed regime is still hotly debated, it is likely to mean greater powers for regulators and more stringent rules for most EU member states.

Harsher penalties

For example, draft legislation has proposed mandatory reporting of a data breach to the regulator, and potentially to individuals affected by the breach. There are also proposals to impose larger fines for breaches of data protection laws – of between 2% to 5% of a company's global turnover.

Similar requirements in many US states have significantly driven up the costs of dealing with a data breach.

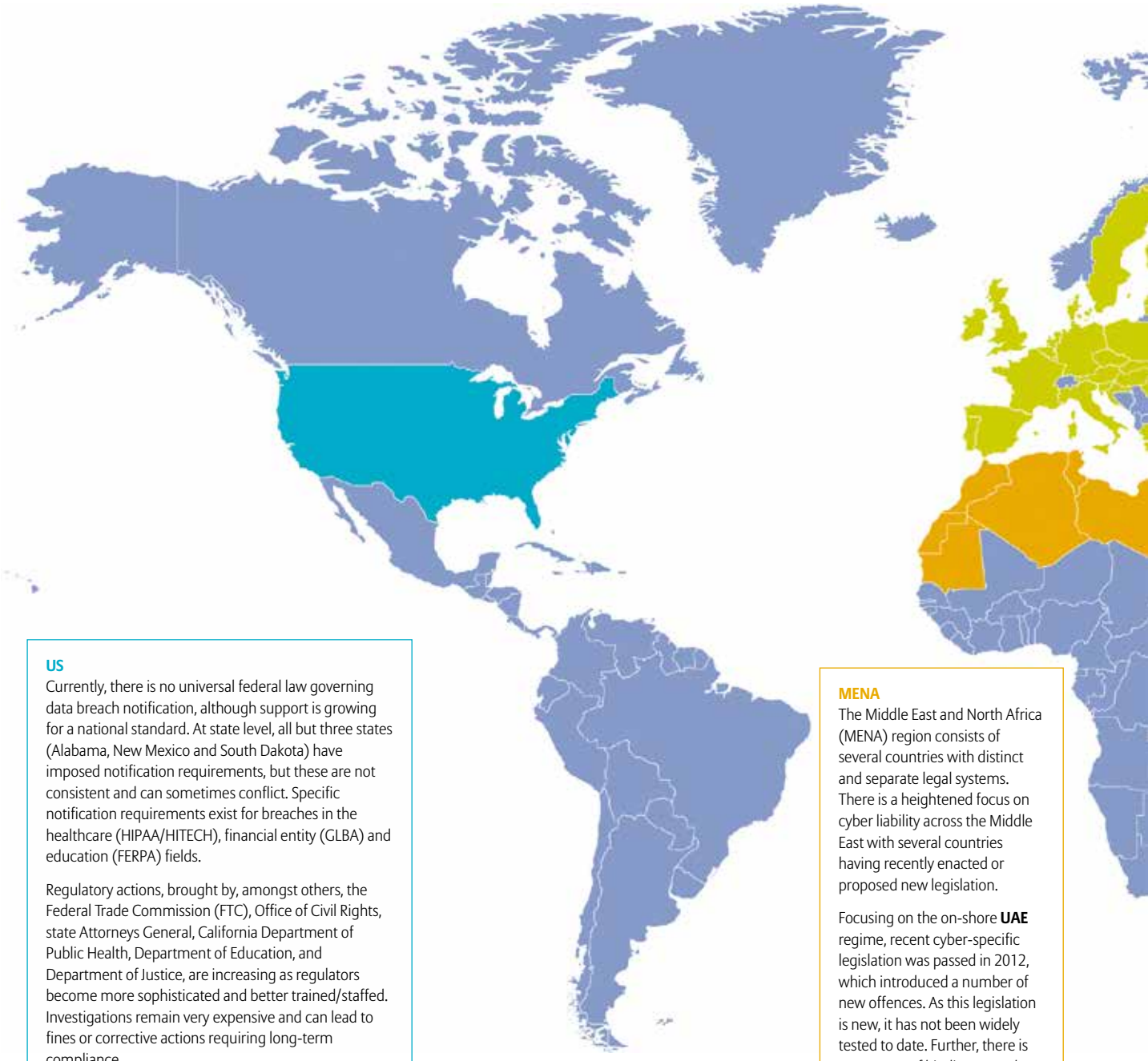
"In Europe we can expect tougher rules on a country-by-country basis," says Pearson. "Politically, it is difficult to be seen to be soft on data breaches. We will see more notifications and significant fines for data breaches in future."

Consumers are increasingly likely to seek compensation for the loss or misuse of their personal data, a view that appears to be shared by regulators and courts.

At the same time companies – conscious of both their statutory and corporate social responsibilities – are beginning to recognize the need to compensate those affected by a breach.

1 *Edelman Privacy Risk Index*

Clyde & Co Legal Snapshot: Around the World in Cyber Regulation



US

Currently, there is no universal federal law governing data breach notification, although support is growing for a national standard. At state level, all but three states (Alabama, New Mexico and South Dakota) have imposed notification requirements, but these are not consistent and can sometimes conflict. Specific notification requirements exist for breaches in the healthcare (HIPAA/HITECH), financial entity (GLBA) and education (FERPA) fields.

Regulatory actions, brought by, amongst others, the Federal Trade Commission (FTC), Office of Civil Rights, state Attorneys General, California Department of Public Health, Department of Education, and Department of Justice, are increasing as regulators become more sophisticated and better trained/staffed. Investigations remain very expensive and can lead to fines or corrective actions requiring long-term compliance.

MENA

The Middle East and North Africa (MENA) region consists of several countries with distinct and separate legal systems. There is a heightened focus on cyber liability across the Middle East with several countries having recently enacted or proposed new legislation.

Focusing on the on-shore **UAE** regime, recent cyber-specific legislation was passed in 2012, which introduced a number of new offences. As this legislation is new, it has not been widely tested to date. Further, there is no concept of binding precedent, so while the introduction of cyber-specific legislation is a welcome move, there is still uncertainty about application.

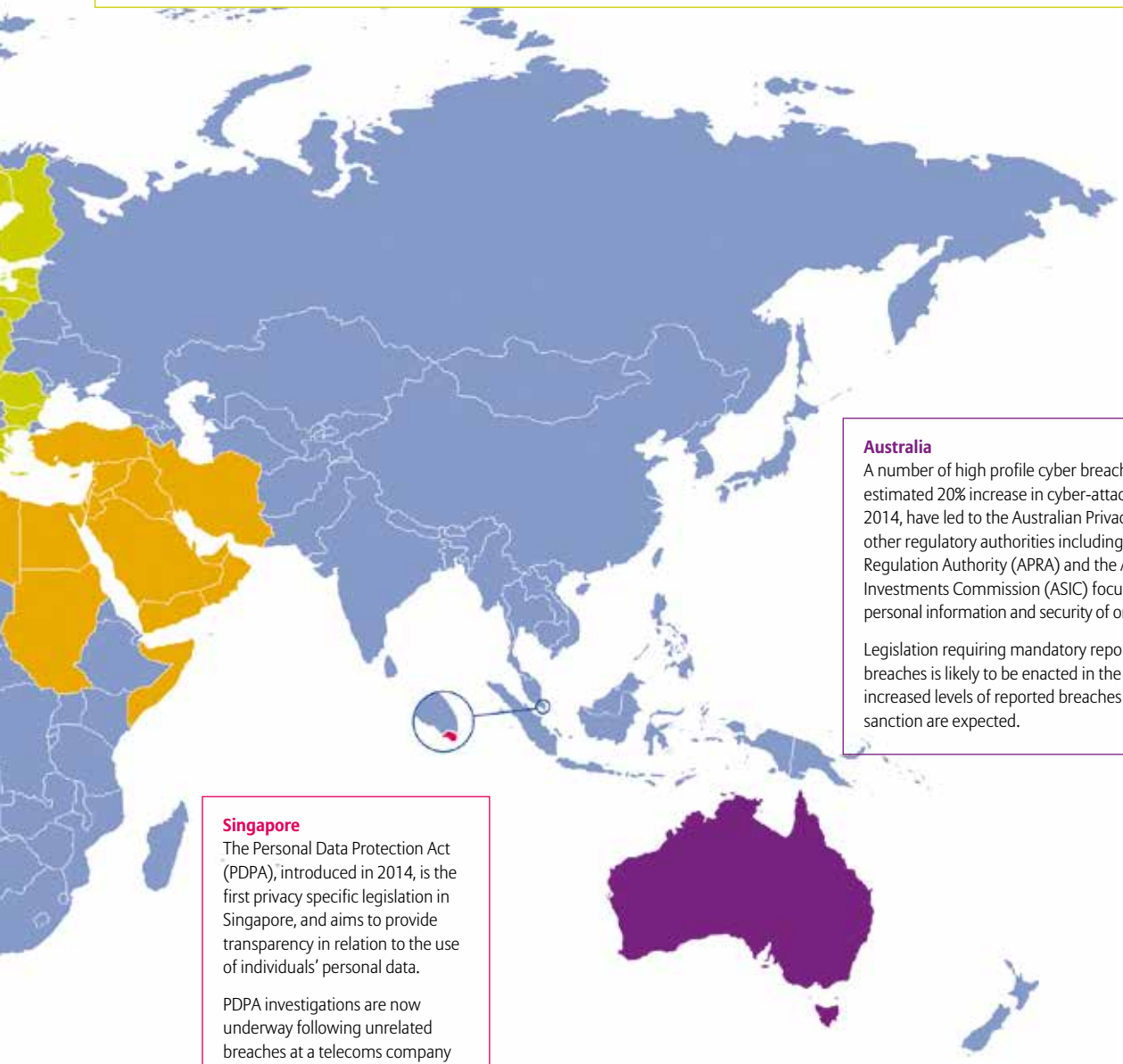
Commentary: *Clyde & Co*

EU

At present, data protection regimes within the EU vary, as existing legislation regulating personal data processing within the **EU (Directive 95/46/EC)** leaves member states free to set their own laws provided they substantially comply with the directive. The **General Data Protection Regulation** will, in due course, replace the directive, and will be directly effective in all member states; the intention being to harmonize data protection regimes within the EU.

While the changes proposed by the regulation are wide-ranging, three key developments are:

- **Notification** - if a personal data breach does occur, and there is a "high risk" for the rights and freedoms of individuals, the data controller must inform its supervisory authority and the individuals concerned without "undue delay". The imprecise threshold requirement means that there is considerable uncertainty around this key issue.
- **One-stop-shop** - any business operating in multiple EU member states will be subject to a single supervisory authority in the member state where their "main establishment" is located. The jurisdictional scope of this mechanism is controversial and the final formulation remains unknown.
- **Penalties** – the current proposals set out a three-tiered system, with the most serious breaches resulting in fines of up to €1m ($1.1m) or 2% of worldwide annual turnover. Compensation may also be payable to individual(s) who have suffered loss as a result of any data breach.



Australia

A number of high profile cyber breaches, coupled with an estimated 20% increase in cyber-attacks on businesses in 2014, have led to the Australian Privacy Commissioner and other regulatory authorities including Australian Prudential Regulation Authority (APRA) and the Australian Securities and Investments Commission (ASIC) focusing on the regulation of personal information and security of online business platforms.

Legislation requiring mandatory reporting of serious data breaches is likely to be enacted in the next year, and thereafter increased levels of reported breaches and fallout regulatory sanction are expected.

Singapore

The Personal Data Protection Act (PDPA), introduced in 2014, is the first privacy specific legislation in Singapore, and aims to provide transparency in relation to the use of individuals' personal data.

PDPA investigations are now underway following unrelated breaches at a telecoms company and a karaoke company, in which customers' personal data was accessed and/or leaked by hackers.

The PDPA introduces fines of up to $1m per breach.

Graphic: *Allianz Global Corporate & Specialty*

Business interruption an increasing concern

While data breaches are a major concern for organizations holding large volumes of personal data, security breaches highlight other threats to business, such as business interruption, intellectual property theft and even cyber-extortion.

With more companies increasingly reliant on technology, business interruption exposures are becoming ever more significant; particularly in sectors such as **telecoms, manufacturing, transport**, **media** and **logistics**.

For example, hackers took French broadcaster TV5 off air in April 2015, affecting 11 TV stations, social media, websites and email.[1] In June 2015, hackers grounded 10 planes belonging to a Polish airline (LOT)[2] after a denial-of-access attack blocked the sending of flight plans.

Meanwhile, in 2012, **"malware"** disabled tens of thousands of computers at oil company Saudi Aramco, disrupting operations for a week[3].

Of course business interruption can also be caused by technical failure or human error as well, as demonstrated by two high-profile recent examples.

Stocks worth $28trn in total were suspended for three and a half hours during July 2015 on the New York Stock Exchange, with authorities reporting that the glitch was not due to cyber terrorism or criminal activity.[4]

During the same month 4,900 United Airlines flights were impacted due to a "network connectivity" issue.[5]

"The impact of cyber business interruption, triggered by technical failure, is something which is frequently being underestimated by businesses relative to cyber-attacks," says Pachov.

What is malware?
Malware is an umbrella term for the many different types of malicious software, such as computer viruses and spyware, for example. Nearly one million new malware threats were released online every day in 2014, according to cyber security firm Symantec[6].

Top risks for business: The rise of cyber risk

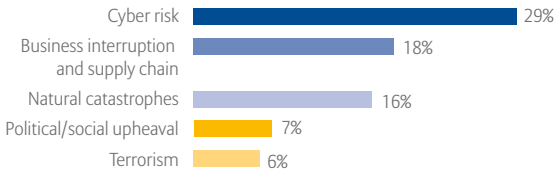
2013 **6%**
Ranked 15th

2014 **12%**
Ranked 8th

2015 **17%**
Ranked 5th

Source: *Allianz Risk Barometer*

Top risks for which businesses are least prepared



Source: *Allianz Risk Barometer 2015*. Figures represent a percentage of all eligible responses (292 responses in total). More than one risk selected.

Cyber risk is the risk most underestimated by businesses according to the **Allianz Risk Barometer**.

"Companies need to be clear about the impact a cyber-attack or incident could have on their supply chain, the liability they could face if they cannot deliver their products in time or if they lose customer data, any jurisdictional laws which might apply, as well as the costs for hiring lawyers, IT experts and public relations experts to resolve any issues," explains **Jens Krickhahn, Practice Leader Cyber & Fidelity at AGCS Financial Lines Central & Eastern Europe.**

"There is still the misconception that larger companies are more frequently the target of cyber-attacks because of the bigger financial rewards for criminals. But cyber-attacks have become an almost daily event, affecting small, medium and large businesses."

The Allianz Risk Barometer surveys over 500 risk managers and experts from 40+ countries.

▶ **www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2015_EN.pdf**

1 *www.reuters.com/article/2015/04/09/us-france-television-islamists-idUSKBN0N00HA20150409*
2 *www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot*
3 *www.infosecurity-magazine.com/news/saudi-aramco-cyber-attacks-a-wake-up-call-says/*
4 *www.theguardian.com/business/2015/jul/08/new-york-stock-exchange-reopens-shutdown*
5 *money.cnn.com/2015/07/08/news/companies/united-flights-grounded-computer/*
6 *money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/*

Industrial control systems

Recent years have seen growing concern about the vulnerability of **industrial control systems (ICS)**, which are used to monitor or control processes in industrial and manufacturing sectors, for example.

An attack against an ICS could result in physical damage, such as a fire or explosion, as well as business interruption.

"A number of ICS still used by manufacturing and utilities companies today were designed at a time before cyber security became a priority issue," explains Pearson.

Vulnerability of ICS was first highlighted by the **Stuxnet** computer worm in 2010. Stuxnet was reportedly developed by Israel to target Iranian nuclear facilities – the worm allegedly destroyed uranium enrichment centrifuges.

245

recorded incidents involving ICS in 2014. The energy sector reported the most incidents, followed by critical manufacturing[1]

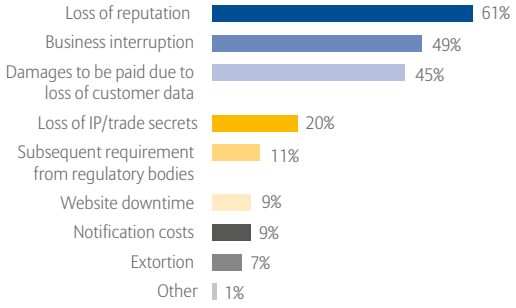
ICS are also vulnerable to both technical failure and operator error as well, which can be much more frequent and severe in terms of impact and are often not captured in cyber reports, Pachov adds.

While ICS are a particular issue for the energy sector *(see left)*, similar cyber-related physical damage and business interruption risks exist in other industries.

For example, car manufacturing plants rely on robots to make and assemble vehicles. Should a robot be hacked or suffer a technical fault, a production line could be interrupted for hours or days, at a potential cost of tens of millions of dollars per day.

And the potential cost of damages could be even higher from an incident involving security-sensitive facilities such as nuclear power plants, laboratories, water suppliers or large hospitals.

Which cyber risks are the main cause of economic loss?



Source: *Allianz Risk Barometer 2015*. Figures represent a percentage of all eligible responses to the questions (127 in total). More than one risk selected.

1 *Industrial Control Systems Cyber Emergency Response Team, US Department of Homeland Security*

Cyber security and protection...

⑤ top cyber risk mitigation tips

- Identify key assets at risk and weaknesses such as the "human factor" or over-reliance on third parties
- Create a culture of cyber security and a "think-tank" approach to tackling risk – different stakeholders from the business need to share knowledge
- Implement a crisis response or breach response plan. Test it
- Consider how merger and acquisition activity and changes in corporate structures will impact third party data
- Make decisions around which risks to avoid, accept, control or transfer

Businesses must understand how cyber risk impacts their operations, how it can be mitigated and then determine their own risk appetite.

Size doesn't matter...
Almost two-thirds of all targeted attacks hit small- and medium-size businesses, according to cyber security firm Symantec [1]. Small companies are increasingly targeted because they can provide a backdoor into companies with more robust systems.

Everyone is a target

Whatever their size or sphere of operation, all organizations need to consider their cyber exposures and prepare for a potential incident.

"Too often we find that people believe that cyber is only an issue for the big brands, banks and retailers," says **Rishi Baviskar, Senior Cyber Risk Consultant, AGCS.**

"In reality hackers are more likely to target the companies with the weakest security, irrespective of their size."

Broad risk spectrum

Depending on the nature of its business and the sector in which it operates, a company is exposed to its own set of cyber risks.

For example, a **financial institution** will hold a wealth of data on its customers, the theft of which would cause immeasurable damage to its reputation. Banks also face huge business interruption exposures through the use of electronic trading systems.

In contrast, a **utility company** will be exposed to risks associated with industrial control systems, where a hack could cause catastrophic damage to property or subsequent business interruption.

Meanwhile, a **pharmaceutical or tech company** will hold valuable intellectual property, and a **professional services company** will hold sensitive client data.

1 *www.telegraph.co.uk/technology/internet-security/11534709/British-companies-bombarded-with-cyber-attacks.html*

10 steps to cyber security

STEP 1 Implement an effective governance structure, maintain board engagement and produce appropriate information security policies which should include:

STEP 2 User education and awareness training

STEP 3 Monitoring policies and procedures for all networks and systems

STEP 4 Incident management procedures, including response and disaster recovery

STEP 5 Network security policies and procedures

STEP 6 Management and control of user privileges

STEP 7 Secure configuration guidance

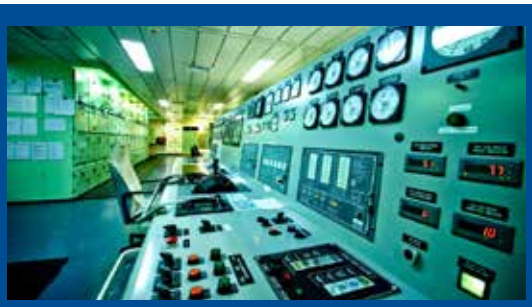
STEP 8 Malware protection procedures

STEP 9 Control of removable media usage

STEP 10 Monitoring of mobile and home working procedures

"It is estimated that approximately 80% of cyber-attacks can be prevented or mitigated by basic information risk management"

The UK Government Communications Headquarters (GCHQ)



CYBER THREAT IN FOCUS: **SHIPPING**

The shipping industry has some catching up to do in getting to grips with the scope and nature of cyber risk. Its interconnectivity means an attack or incident in a key location could have a severe impact. According to the International Maritime Organization there have already been numerous examples of cyber security issues:

- A hacker caused a floating oil-platform located off the coast of Africa to tilt to one side, thus forcing it to temporarily shut down
- Hackers infiltrated cyber systems in a port to locate specific containers loaded with illegal drugs and remove them undetected
- Somali pirates employed hackers to infiltrate a shipping company's systems to identify vessels passing through the Gulf of Aden with valuable cargoes and minimal on-board security. This led to the hijacking of at least one vessel
- Denial of service attacks (initiating a very high number of requests to a system to cause it to cease operating) against ports have been reported.

Furthermore, there have been a number of anecdotal accounts about hackers accessing computer systems/navigation software, subsequently causing hull damage.

Dr Sven Gerhard, Global Product Leader Hull & Marine Liabilities, AGCS believes a claim related to a future cyber-attack could be "tremendous", potentially resulting in a total loss of a vessel. It could even involve multiple vessels from the same company.

"If a virus intrudes into IT-based steering or navigation systems what will happen? Such cyber risks will become a focus topic for us as an insurer," he adds.

Risk identification and response

When identifying cyber risks, companies should consider both physical and digital security controls – such as password procedures – as well as which third parties have access to systems or those of cloud providers, advises Baviskar.

"Know your assets and prioritize them. If resources are limited, identify key assets at risk, as well as potential weaknesses, and put policies in place to protect them," he says.

Businesses should also not underestimate the "human factor", adds **Jens Krickhahn, Practice Leader, Cyber & Fidelity at AGCS Financial Lines Central & Eastern Europe**. "Employees can cause large IT security or loss of privacy events, either inadvertently or deliberately."

Cyber risk management is an emerging area, but companies can gain assistance from governments and third parties. It is also worth considering using a third party to test and audit cyber security.

As a senior cyber risk consultant, Baviskar helps underwriters understand and benchmark cyber risk exposure. This is achieved through desktop studies or workshops and dialogue with businesses for larger more complex risks.

When assessing a risk, cyber risk consultants consider a company's IT security and data processes. They will also look at business continuity plans, as well as breach response procedures.

Assessment of business interruption risk requires financial analysis of the health of the company, service/production processes and their bottlenecks, computer/network infrastructure management, as well as discussion of loss scenarios and modeling.

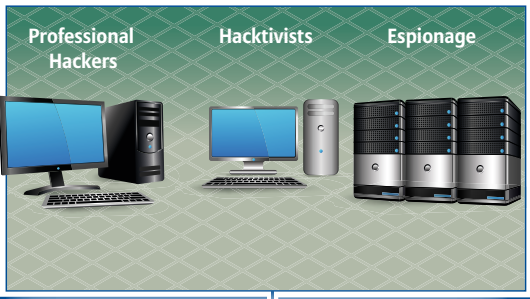
It also pays to plan ahead.

"Companies need a crisis response or breach response plan. Then test it," advises Krickhahn.

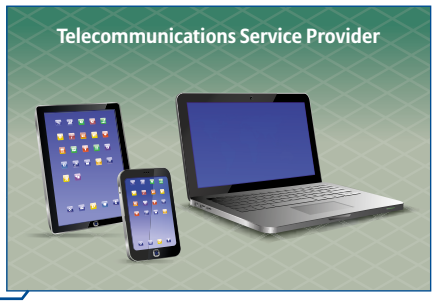
"It's better to draw up a plan in peace-time ready for the war. That way you will know who to contact, who does what, and how to communicate."

Cyber risk connected: The many ways in which a business can be exposed

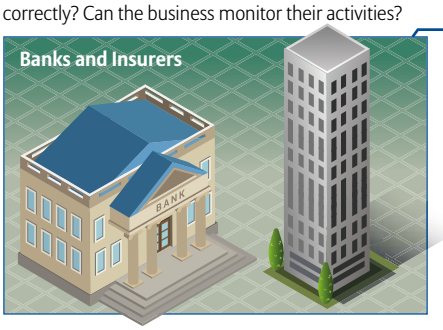
Have access to offices, networks and systems including critical access rights. Are these rights set correctly? Can the business monitor their activities?



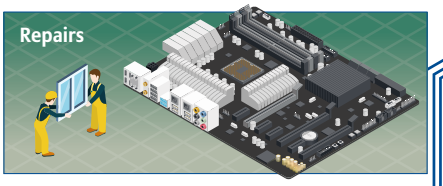
Professional hackers target businesses to make money. Hacktivists attack interfaces resulting in damage. Espionage of intellectual property rights is common.



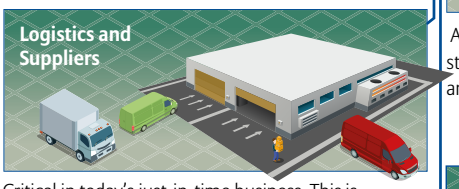
If a communication line goes down this can impact customers, partners, supply chain management and remote maintenance.



Possess confidential information about a business' strengths and weaknesses. If a cyber incident occurs such information could fall into the wrong hands.

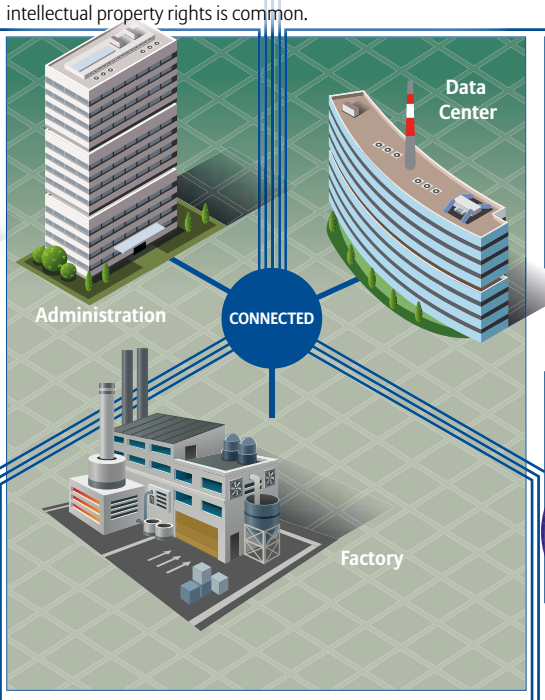


Many machines can be repaired online today. During repairs access to facilities can be hard to restrict. This could be abused to gain access to IT networks.

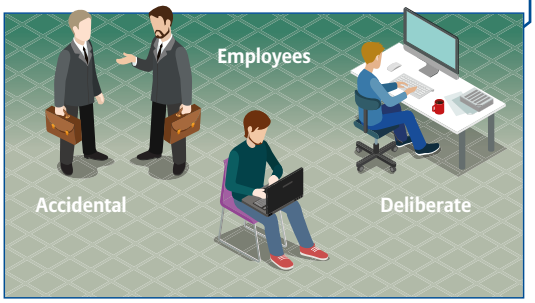


Critical in today's just-in-time business. This is mostly managed by internet-connected interfaces which can be easily attacked. Can the business send out a product if this happens?

Cyber incidents can be caused by service providers. Over-dependency can result in an inability to monitor actions.

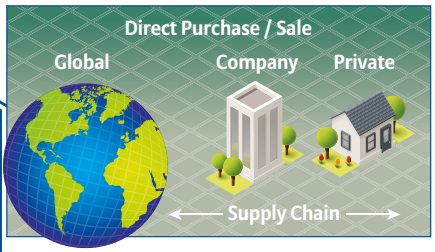


A factory can face a number of potential perils stemming from IT, growing use of cloud computing and increasing interconnectivity.

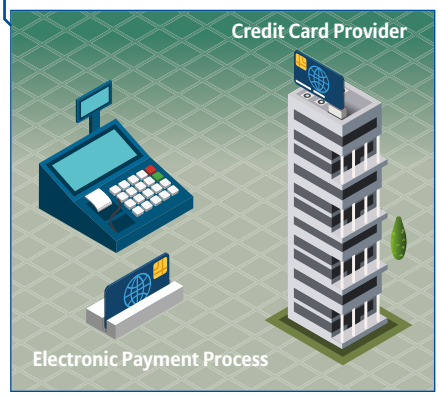


Employees can easily create outages (intended or unintended) or cause data leakages. Improving employee awareness of the risks involved is crucial.

Businesses depend on their customers and must protect IT facilities where sensitive and confidential data is located.



Supply chain management is critical but it's also interconnected via public-accessible interfaces, with hackers looking for vulnerabilities 24/7. What happens if a denial of service attack paralyzes the supply chain?



Gaining access to credit card data is a quick win for cyber criminals. Businesses are liable for the non-disclosure of such data.

This infographic illustrates some of the many "gateways" through which a business – in this case a factory – can be impacted by cyber risk due to increasing interconnectivity. Attacks by professional hackers or so-called hacktivists dominate the headlines but a recent study by the German Federal Association for Information Technology, Telecommunications and New Media (Bitkom) also revealed that in many cases (around 52%) – current or former staff members were responsible for cyber incidents.

Threat scenarios

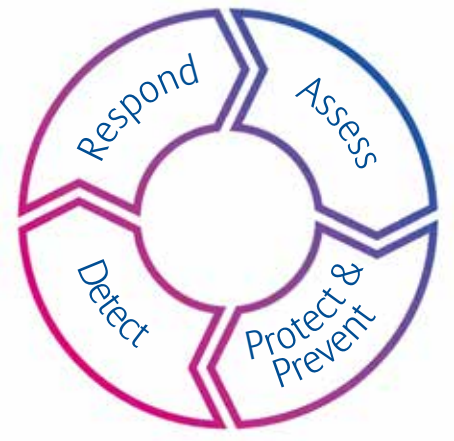
Of course identifying and evaluating threat scenarios is difficult. Different stakeholders from the business need to share knowledge – IT experts or production engineers can identify the scenarios, business continuity managers can quantify the duration, and financial departments the cost. Previously siloed knowledge needs to be incorporated in one **"think tank"**, including the set-up of IT, processes and risk transfer. Everything should be interlinked.

In Germany AGCS has partnered with T-Systems, the security specialist arm of Deutsche Telekom, and is running workshops with businesses with complex cyber exposures. These can help firms map their data and IT risks and make decisions around which risks to avoid, accept, control or transfer.

Such workshops can also help companies prioritize actions, according to Krickhahn. Following one such workshop, a business decided to create a centralized system to manage client data.

"Given merger and acquisition (M&A) activity, and complex company structures, it's not surprising that many companies struggle to quickly identify all the data they collect on third parties," he says.

Cyber security circle



A holistic approach to cyber security is necessary to safeguard companies.

CYBER THREAT IN FOCUS: **AVIATION**

The aviation sector relies on computers for almost every aspect of its business. With this growing reliance comes a wide range of cyber risks, including passenger data, business interruption exposures related to ticketing systems or air traffic control, as well as physical damage and liability arising from aircrafts' dependency on technology.

"New generation aircraft are highly-exposed to cyber risk due to the prevalent use of data networks, onboard computer systems and navigation systems," says **Ludovic Arnoux, AGCS' Global Head of Aviation Risk Consulting**. "Data breaches and cyber-attacks are perceived to be growing risks." In June 2015 Polish airline LOT had to cancel around 10 foreign and domestic flights after hackers reportedly accessed its computers. This year has also seen a number of airlines report that their passenger data networks have been accessed.

"In the next five to 10 years, cyber will become the biggest focus of the aviation industry," says **Henning Haagen, Global Head of Aviation at AGCS**. "Cyber risks are not currently excluded in aviation insurance policies. However, the industry and its insurers will need to develop their understanding of the risk to prevent losses and risk accumulation."

Cyber insurance continues to evolve...

⑤ top trends in **cyber insurance**

- **Exclusions in traditional policies will become more commonplace. Standalone cyber product to be the main source of liability cover**
- **Cyber concept and wordings will be tested, potentially resulting in litigation**
- **Cyber insurance market needs volume and diversification. More segmentation in future with insurers specializing in certain sectors**
- **Lack of education is an obstacle to growth – both in terms of businesses' understanding of exposures and underwriting knowledge**
- **In the event of a cyber security incident a speedy response and use of third party experts can mitigate losses**

Now into its third major phase of development, cyber insurance is no replacement for robust IT security. However, it has an important role to play as part of a holistic risk management strategy, creating a second line of defense to mitigate cyber incidents.

In 2001 Allianz was one of the first insurers to offer a specialist first party cyber policy, later extended to include third party cyber risks in 2004.

Y2K origins

Standalone cyber insurance can trace its roots to "**Y2K**" and the infamous "**Millennium bug**".

Concerns that programming issues associated with the Year 2000 date change would cause widespread computer system failure prompted many companies to first assess the potential for cyber risk to their businesses. As companies became more aware of their cyber exposures they began to look to their property and casualty insurers to provide cover, explains **Jens Krickhahn, Practice Leader, Cyber & Fidelity at AGCS Financial Lines Central & Eastern Europe**, who has underwritten IT and cyber risks for over 16 years.

Initially, insurers such as AGCS offered separate property and liability covers for these emerging cyber risks. However, this early cover was relatively limited compared with today's standalone product offering.

Data protection

The second phase of development of the cyber insurance market came with rising privacy and data protection legislation, particularly in the US.

This saw the development of standalone cyber insurance products focused on the costs associated with data breaches. These policies evolved to include instant access to expert response services and crisis management.

The third phase of development – currently ongoing – sees an increasing awareness among organizations that cyber risks are not only about protecting consumer data and that breaches are not limited to the US.

Over time, the cover offered under a cyber insurance policy has become broader and more standardized. "A cohesive cyber insurance market is developing," says **Nigel Pearson, Global Head of Fidelity, AGCS**.

Areas of Cover

AGCS provides a number of different insurance coverages to ensure that a company is protected in the event of a data loss or cyber security incident – **Cyber Protect, Cyber Protect Premium** and **Cyber Protect Premium Plus.**

Allianz can commit up to €100m in cover. ($111m)

Cyber Protect

Risk	Details
Privacy and Data Breach cover	Defense costs and damages for which the Insured or Outsourced Service Provider is liable, arising from a loss of data
Business Interruption and Restoration Costs cover	Loss of business income (and restoration costs) caused by a targeted attack against the company's computer system
Network Security Claims cover	Defense costs and damages for which the Insured is liable, arising from a targeted cyber attack
Media liability claims cover	Defense costs and damages for which the Insured is liable, arising from the publication or broadcasting of digital media content
Regulatory costs cover	Defense costs for a claim by a regulator arising out of the loss of data
Regulatory fines and penalties cover	Monetary fines and penalties levied by regulators (to the extent that they are insurable) arising from a loss of data
Notification costs	In accordance with legal and regulatory requirements following a loss of data
Response costs	Fees and expenses for: • Forensic investigation following a loss of data • Identifying and preserving lost data • Advice on legal and regulatory duties • Determining the extent of indemnification obligations in contracts with third party service providers • Credit monitoring services and other remedial actions required after a loss of data
Hacker theft cover	Indemnity for stolen funds due to malicious activities of a third party
Cyber extortion cover	Indemnity for the resolution of a credible threat to compromise the Insured's data or systems
E-payments	Defense costs, damages and contractual penalties in respect of a breach of Payment Card Industry Data Security Standards
Crisis Communication cover	Public relations expenses of a panel of experts to mitigate any negative publicity from a covered event
Consultant services cover	The expenses of an IT expert to determine the amount and extent of a loss covered under this policy.

Cyber Protect Premium

Additional protection such as extended business interruption.

Cyber Protect Premium Plus

A coverage composed on the basis of Allianz Cyber Protect to be tailored for a specific business' demands.

Data breach cover

Over the past decade, an important element of cyber insurance has been the development of privacy and data breach cover.

The cornerstone of most standalone cyber insurance has been the cover for third party liabilities – such as legal or regulatory actions – as well as first party costs associated with responding to the breach. These can include the cost of notifying individuals, credit monitoring, IT forensics, public relations and crisis management and communication.

"Cyber insurance gives access to experts, such as legal, IT forensics, crisis communications and more, to help policyholders navigate their way through a breach in a professional way. This can limit reputational damage and ensure there is life after the crisis," says Krickhahn.
In addition to this core cover, cyber insurance can also provide other useful liability coverages for the digital age. For example, media liability cover protects against litigation arising from defamatory content published on a website or through social media.

It is also possible to insure against a data breach that occurs at an outsourcing partner, such as data stored with a cloud service provider.

Cyber-crime cover, including theft of funds and cyber extortion, is also available.

Business interruption protection

One of the biggest developments in cyber insurance in recent years has been the addition of more meaningful business interruption insurance for cyber-related events.

It is now possible to purchase standalone cyber cover that either combines first party business interruption insurance cover with data breach liability or includes only a first party business interruption. It covers partial or complete business interruption following a cyber attack or operational or technical failure.

"In the context of cyber, business interruption cover can be very broad. Not only can it cover 'business IT' computer systems, it can extend to industrial control systems used by energy companies or robots used in manufacturing, for example," explains **Georgi Pachov, Global Practice Group Leader Cyber, CUO Property, AGCS**.

"With technological advances businesses are driven by data flows in real-time: logistics are tracked from supplier to customer, products are assembled using online parameters, calls are delivered over internet protocol, power is transmitted by means of demand. Any interruption of the process chain – even for a minute – could cause a severe business interruption, impacting the balance sheet of a company. Big data, data analytics, artificial intelligence, the 'Internet of Things' *(see page 27)* – it's all about managing, understanding and making smart decisions based on the data in order to gain competitive advantage," Pachov adds.

It is also possible, in certain circumstances, to insure against contingent business interruption **(CBI)**, such as the failure of IT or operational technology infrastructure belonging to a third party.

However, CBI cover for cyber exposures poses a significant risk of accumulation, so insurers can only offer limited cover, and only after detailed risk analysis requiring additional data from the insured.

Cyber shake-up

Cyber risks have emerged and evolved rapidly in just a few decades, while many traditional insurance products have yet to fully adapt.

In some cases, traditional insurance products may unintentionally extend cover to cyber-related losses, although such cover is largely untested and would be limited to only certain cyber exposures.

"Traditional property and casualty insurers are now looking to examine the cover extended to cyber risks. Exclusions in traditional policies are likely to become more commonplace. Standalone cyber insurance will increasingly be seen as the main source of comprehensive cyber liability cover," says Pearson.

Protection gap

One gap that currently exists between traditional and standalone cyber insurance is for physical damage resulting from a cyber-incident. For example, a fire or explosion could result from a compromised industrial control system controlling an industrial process or oil pipeline.

Physical damage resulting from a cyber-event is typically excluded under standalone cyber insurance. However, physical damage resulting from a cyber-attack is not explicitly covered under property insurances, and in many cases will also be excluded.

"One of the cyber challenges is to identify what exactly caused a physical damage," says Pachov. "An explosion or large fire can be caused by an incompatible software, operational error or cyber-attack but often it is impossible to locate the origin of the damaged equipment."

Incident response

In the event of a cyber security incident or loss of data an appropriate and speedy response is required to manage the incident successfully. AGCS has a panel of organizations with expertise in their fields who can help to resolve an incident with a full range of services, including: IT forensic services, (including notification services, credit monitoring services etc, as needed) media crisis management services and specialist legal services.

Once an incident is identified a business should immediately inform its insurer. In such an instance AGCS would then suggest appropriate experts that the impacted business can engage to work closely with (within the ambit of its crisis management plan) to bring about a speedy resolution of the incident. AGCS experts can provide pre-loss training and services to support information security policies if required. AGCS also has in-house expertise of engineers in Allianz Risk Consulting, who can help businesses to understand the full extent of their exposures.

For more information

- www.agcs.allianz.com/services/financial-lines/cyber-insurance/

Litigation on the way

Standalone cyber insurance will continue to evolve as it responds to changes in both cyber risk and regulation. However, such development will bring challenges. There are a number of different policies in the market and, many have concepts and wordings that have yet to tested.

"As time passes we may well see more litigation in this area. There will be uncertainty about how courts will interpret some of the concepts. This is not unusual with new products and will result in a body of knowledge for underwriters," Pearson adds.

Talent shortage

And the cyber insurance market is not without other challenges. For example, as demand picks up, insurers will need a larger pool of expertise to draw on *(see box below)*.

"There is currently a lack of knowledge in the insurance industry," says Pearson. "We are learning quickly but there is a shortage of talent and skills. The industry needs to up its game in terms of risk assessment and expertise."

Obstacles to cyber insurance growth

While the cyber insurance market is growing rapidly, certain factors are holding back even more rapid development. Businesses' ability to understand their own exposures, the ever-evolving nature of cyber risk and awareness of the different data protection laws globally all present challenges.

Education of businesses, brokers and underwriters is key. This year AGCS hosts its second cyber academy for underwriters, underlining the importance of raising the level of knowledge of underwriters and the industry in general.

Aggregation risk

Perhaps the biggest challenge for insurers is to manage the risks they take on as the cyber insurance market grows. An increased pool of premium and diversity of risk will be welcomed, but insurers will need to control their exposure to systemic cyber risks, like malware or a breach/outage at a large cloud service provider.

Of particular concern is aggregation risk. However, the data and modeling tools that are common place for understanding catastrophic property exposures do not yet exist for cyber risk.

Insurers are looking to use realistic disaster scenario testing and modeling to get a better understanding of cyber risk and what it means for their balance sheets, but this will take a few more years to develop and improve, particularly as cyber risk keeps evolving.

Greater segmentation and specialization

One likely result of a lack of claims data, and the challenge of understanding and assessing cyber risk, is likely to be greater segmentation, with some insurers seeking to specialize in certain sectors, Pearson predicts. Individual insurers are likely to better define where they have appetite and tailor their products accordingly.

"There is lots of capacity in the market, but there is still not enough data to fully understand the risk. So pricing volatility will continue and market segmentation will increase," he says.

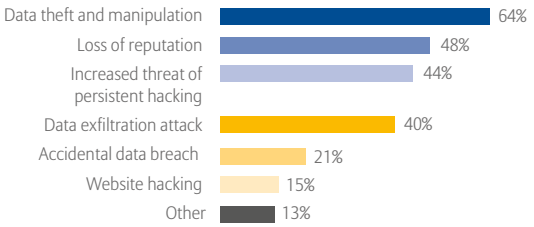
Role of insurance

Insurance is not a replacement for good cyber security. However, it can provide protection should the worst happen.

"Insurance brings additional risk mitigation and compensation in the event of a claim. With a property risk, you would install sprinklers to mitigate fire losses, but you would also buy insurance in the event of the building burning down. The same concept applies with cyber risk" explains Krickhahn.

"However, once you have purchased insurance, it does not mean that you can ignore IT security. The technological, operational and insurance aspects go hand-in-hand."

Which cyber risks do companies fear the most?



Source: *Allianz Risk Barometer 2015*. Figures represent a percentage of all eligible responses to the questions (127 in total). More than one risk selected.

Cyber risk **2025 - the next 10 years...**

⑤ Future **cyber risk trends**

- **Cyber insurance market could be worth $20bn+ by 2025**
- **Liability and data protection risks dominate market today but demand for, and take-up of, business interruption cover will grow over next decade**
- **Businesses will be increasingly exposed to – and focused on – supply chain cyber risk**
- **Financial institutions, energy, utility, transport and telecommunications sectors to lead widening demand for cover**
- **A catastrophic cyber loss is increasingly likely. Governments, businesses and insurers will need to collaborate to protect critical infrastructure**

Growing awareness of broader cyber risks, such as impact of business interruption, as well as regulatory change, will propel future rapid growth of cyber insurance. Meanwhile, as technology becomes even more engrained in everyday life and business, new risks will emerge.

Growth trajectory

The cyber insurance market has grown rapidly over the past decade, prompted by the introduction of mandatory notification requirements in a growing number of US states.

California was the first to introduce mandatory notification, which has now spread to over 90% of US states. As a result, the cyber insurance market is now estimated to be worth around **$2bn** in premium worldwide, with US business accounting for approximately 90%.

"The cyber market is growing by double-digit figures year-on-year, and could reach **$20bn** or more in the next 10 years," says **Nigel Pearson, Global Head of Fidelity, AGCS**, who notes that fewer than 10% of companies are thought to purchase cyber insurance today.

"Growth in the US is already underway as data protection regulations help focus minds, while legislative developments and increasing levels of liability will see growth accelerate in the rest of the world."

Widening demand

Growth will also come as a broader range and size of companies purchase cyber insurance. As awareness of the risks grow, they will increasingly examine their risk transfer options.

For example, sectors that hold large volumes of personal data, such as healthcare and retail, or sectors relying on digitalized IT/operational technology processes, such as logistics, manufacturing and telecommunications, are currently most likely to buy cyber insurance. However, there is growing interest among financial institutions, and the energy, utilities and transport sectors, driven by the increasing perils posed by interconnectivity.

Early adopters have tended to be larger companies with more sophisticated risk management, but an increasing number of small- to medium-sized enterprises (SME) will also purchase cyber insurance in future.

Business interruption

Growth in the cyber insurance market will also be driven by increasing demand for business interruption (BI) coverage.

"When discussing cyber risk many people focus on the liability and data protection risks. But for many companies this will not be the most critical cyber exposure," says **Georgi Pachov, Global Practice Group Leader Cyber, CUO Property, AGCS**.

"Awareness of BI risks and insurance related to cyber and technology is increasing. Within the next five to 10 years BI will be seen as a key risk and a major part of the cyber insurance landscape."

Supply chain impact

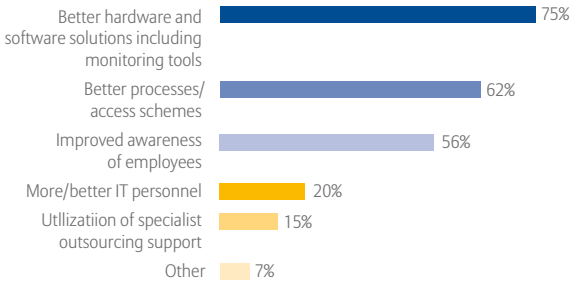
Today, many companies are concentrating on managing and insuring cyber risks within their own organization. However, they will increasingly look to extend insurance cover to their supply chains, Pachov predicts.

"Business exchanges with partners are increasingly electronic," explains **Jens Krickhahn, Practice Leader, Cyber & Fidelity at AGCS Financial Lines Central & Eastern Europe**.

"Even if a company is confident in its own IT controls, it is still exposed to cyber risk through its business partners, contractors and supply chains," he says.

Companies need to be clear about the impact a cyber-incident could have on their supply chain, the liability they could face if they cannot deliver their products in time or if they lose customer data, any jurisdictional laws which might apply, as well as the costs for hiring lawyers, IT experts and public relations experts to resolve any issues.

Protecting against cyber risks – which areas are most important?



Source: *Allianz Risk Barometer 2015*. Figures represent a percentage of all eligible responses to the questions (127 in total). More than one risk selected.

A large loss is on its way

While there have been some very large data breaches, there has yet to be a major cyber event of truly catastrophic proportions. "There is the potential for a catastrophic cyber-attack or a major cyber-risk aggregation event, but exactly what it will look like is difficult to predict," says Pearson.

The impact could be severe. An attack or incident resulting in a huge data loss, BI or reputational damage could potentially put a large corporation out of business. A major data breach or network outage for a cloud service provider could cause business disruption for hundreds of companies. Another catastrophic scenario could result from a successful attack on the core infrastructure of the internet. Other scenarios could see an incident involving an energy or utility company resulting in a significant outage, physical damage or even loss of life in future, while a cyber war between two countries could disrupt services around the world.

A catastrophic cyber event could generate significant losses. However, at the same time it would also raise awareness and ultimately boost demand for cyber insurance, Pearson predicts.

Private/public cyber collaboration

Unsurprisingly, such concerns about the economic impact of cyber risk, and risk to critical infrastructure in particular, has attracted the attention of governments. In the US and Europe, governments have been encouraging companies to build their resilience to a cyber-attack, promoting cyber security standards and greater levels of co-operation, including sharing data.

"Interest in protecting critical infrastructure is likely to see governments becoming increasingly involved in cyber security, with much greater levels of scrutiny and liability," Pearson concludes.

Emerging risks: impact of technology...

⑤ Interconnected cyber threats

- **Estimates suggest a trillion devices could be connected by 2020**
- **"The Internet of Things" will exacerbate cyber vulnerability, bringing increasing potential for physical loss and data breaches**
- **Cyber criminals will exploit increase in interconnectivity between machines in the supply chain, creating new exposures**
- **As technology evolves, aging hardware also becomes vulnerable to attack**
- **Cloud computing can create systemic risk**

The cyber risk landscape of tomorrow will look very different to that of today.

What is the "Internet of Things"?
Estimates suggest that as many as a trillion devices will be connected by 2020. The "**Internet of Things**" describes a future where all the devices we use – from cars to wearable devices – are connected to the internet. While this could make our lives easier, such interconnectivity also potentially increases the threat and impact of cyber risk.

Developments in technology and how these are employed will be the key driver behind the cyber risk landscape in future.

The growing popularity of mobile devices, like smart phones, watches, and glasses, is likely to increase cyber risk.

The "**Internet of Things**" will see technology become embedded in smart devices around the home, such as domestic appliances, heating or lighting systems and entertainment. Networked technology will also become more commonplace outside the home, from smart cars to wearable devices.

"Predictions suggest that a trillion devices will be connected by 2020, which could lead to a significant increase in cyber vulnerability," says **Rishi Baviskar, Senior Cyber Risk Consultant, AGCS**.

The "Internet of Things" will become a much bigger issue for cyber security as more and more devices link to the internet. For example, Chinese students hacked a Tesla Motors electric car, as part of a competition, in 2014, remotely controlling the car's locks, horn, headlights and skylight while it was in motion[1].

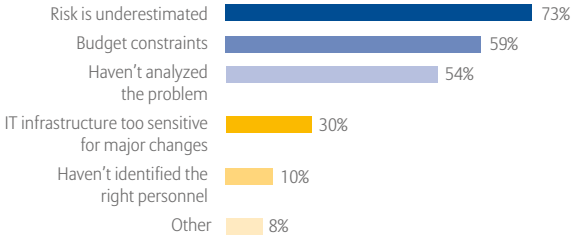
It also emerged last year that some 1,000 smart-appliances, including fridges and TVs, were hacked and instructed to send spam-emails as part of a botnet attack[2].

"This is an area already exercising the minds of underwriters," explains **Nigel Pearson, Global Head of Fidelity, AGCS**. "The "Internet of Things" could bring increased potential for physical loss or data breaches.

"Cyber criminals are already migrating to new platforms, such as smart devices, with mobile wallets increasingly being used for financial transactions, for example. Understandably, there are concerns around potential exposures created, as more sophisticated attacks occur."

1 *www.nydailynews.com/autos/chinese-university-students-successfully-hack-tesla-model-s-article-1.1896540*
2 *www.independent.co.uk/life-style/gadgets-and-tech/news/could-your-fridge-send-you-spam-security-researchers-report-internet-of-things-botnet-9072033.html*

What is preventing companies being better prepared against cyber risks?



Source: *Allianz Risk Barometer 2015*. Figures represent a percentage of all eligible responses to the questions (127 in total). More than one risk selected.

Smart devices are not restricted to consumer goods – factories, supply chains, cities and infrastructure are also likely to look to new technologies.

"Some estimates suggest that as many as 50 billion machines will be exchanging data on a daily basis in the near future," says **Jens Krickhahn, Practice Leader, Cyber & Fidelity at AGCS Financial Lines Central & Eastern Europe.**

"IT and technology is becoming increasingly more important. Business and society will face many new exposures currently unknown to us today," says Krickhahn.

As technology evolves, older devices that remain in use could also create vulnerabilities, especially where they rely on outdated operating systems and unsupported software.

"Many firms are already running software that is no longer supported by developers. Now we are seeing that hardware will increasingly become out-of-date and need replacing. Everyone talks of software, but hardware limitations also create vulnerabilities," adds Baviskar.

The use of outsourced services, like cloud computing and cloud data processing and storage, is another area of concern.

"The problem, for insurers, is that cloud service providers act as data and systems aggregators. So if one of them has an issue, it could result in large business interruption and data breach losses for many companies," says Pearson.

"Risk managers will need to stay on top of technological trends and anticipate how these will impact their organizations going forward in terms of cyber risk exposure," concludes **Paul Schiavone, Regional Head Financial Lines North America, AGCS**.

Human factor risk higher in the cloud

According to Goldman Sachs cloud infrastructure and platform spending will grow to $43bn in 2018, up from $16bn last year[1]. Yet a Ponemon Institute study in the US said 66% of IT experts believed increasing use of cloud computing will result in less security[2]. Use of the cloud would diminish their company's ability to protect confidential data and critical internal software solutions, they said.
The "**human factor**" – either deliberately or inadvertently – is often regarded as the greatest threat to cyber security. This risk may be even higher in the cloud, where the perpetrator could access vast quantities of confidential information. Lack of standardization of the cloud means it can be difficult to assess the security levels of different providers.

1 *news.investors.com/technology/011615-735080-amazon-aws-leads-in-cloud-msft-googl-crm-rising.htm*
2 *Data Breach: The Cloud Multiplier Effect, Ponemon Institute*

Contact Us

For more information contact your local Allianz Global Corporate & Specialty Communications team

Johannesburg
Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 11 214 7948

London
Jonathan Tilburn
jonathan.tilburn@allianz.com
+44 203 451 3128

Munich
Heidi Polke-Markmann
heidi.polke@allianz.com
+49 89 3800 14303

New York
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 646 472 1510

Paris
Florence Claret
florence.claret@allianz.com
+33 158 858863

Rio de Janeiro
Juliana Dias
juliana.dias@allianz.com
+55 21 3850 5958

Singapore
Wendy Koh
wendy.koh@allianz.com
+65 6395 3796

Credits

Editor: Greg Dobie (greg.dobie@allianz.com)
Journalist: Stuart Collins
Contributors: Clyde & Co – Around The World In Cyber Regulation *(page 9)*
Design: Mediadesign
Photos: Shutterstock

Disclaimer & Copyright

Allianz Global Corporate & Specialty SE, Fritz-Schaeffer-Strasse 9, 81737 Munich, Germany
Commercial Register: Munich HRB 208312

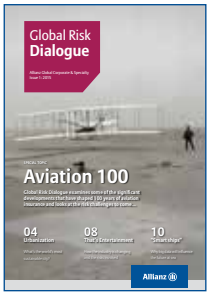
www.agcs.allianz.com

September 2015

Further Reading

Hurricane Katrina 10: Catastrophe management and global windstorm peril review

Global Aviation Safety Study



Global Risk Dialogue: The AGCS magazine

Global Claims Review

Safety and Shipping Review

The Weather Business

www.agcs.allianz.com

www.agcs.allianz.com