Allianz

Allianz technology professional indemnity

Technology: so what's the big deal?

Since 2005, when internet broadband started to take off, the digital universe has grown 22-fold and this phenomenal growth is set to continue. By 2020, as the size of the digital universe doubles every two years, the data universe will reach 40 zettabytes, a 14-fold growth from 2010; equivalent to 57 times the amount of all the grains of sand on all the beaches in the world.

The technology sector is at the core of this growth and among the world's biggest - accounting for almost a combined US$6trillion in quoted market capitalisation, equivalent to approximately 13% of the world's market capitalisation – and it continues to expand strongly relative to the world economy. Global IT expenditure spending is estimated by Gartner in 2013 at close to US$4 trillion and this is expected to grow at an annual average of 4% from 2011-2017, despite the subdued economic outlook and lingering effects of the global recession.

The more technology and data there is, the more there is to lose. Much can be done to mitigate the risks, manage the threats and financially protect the business with relevant insurance.

Technology companies are exposed to data privacy legislation because of client data they hold and also because of the products and services they provide to clients.

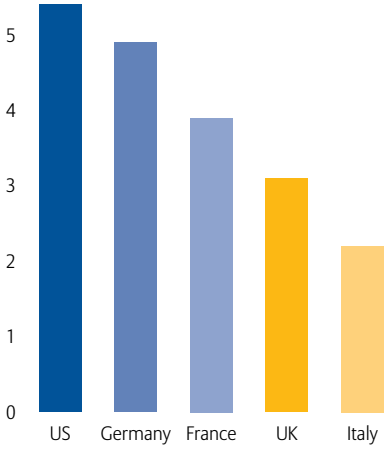
Why data security and privacy matters?

Regulation of the digital universe can best be described as patchy; organised as it is along national lines, but in sharp contrast to a global cyberspace. This potentially could create plenty of problems with adverse financial and reputational consequences for technology companies in particular.

This is most significant is the US, where in the majority of States, companies that suffer a data breach involving personally identifiable information have to notify clients and could be responsible for compensation. Europe has moved more slowly so far in this direction, but a proposed EU General Data Privacy Protection Regulation would unify data protection across all member states and impose severe penalties of 5% of global annual turnover or 100m whichever is the greater. Its adoption is expected in 2014 and enforcement from 2016.

Average organisation cost of a data breach

(2012 – US$m)



Source: Ponemon Institute

Where is the data breach threat?

In 2012, while 35% of the information in the digital universe required protection, less than 20% had appropriate level of security; protection was weaker in emerging markets than developed markets and attacks on smaller companies were growing faster than on larger ones.

The top cause of all data breaches is hacking, though accidental loss and theft or loss of a computer are also other important causes. Hacker data breaches are responsible for 79% of identities exposed.

In 2012, 18% of data breaches that could lead to identity theft were in the technology sector, but when these data breaches were measured in terms of the total number of identities exposed this share jumped to 37%, making the technology sector the number one sector for data breaches.

Symantec reported a 42% increase in target attacks in 2012 and an average of 116 per day; more than 600,000 identities were exposed in an average breach and the median number of identities stolen was 8,350, this was more than a three fold increase over 2011. Some 50% of attacks targeted larger businesses, but the strongest growth was among smaller businesses – those with less than 250 employees - which accounted 31% of total attacks. As well as smaller companies being more vulnerable to attack for their own assets, they are also being used as watering holes or hijacked for subsequent attacks on larger organisations.

What are the potential liabilities for technology companies?

As well as the risk and liabilities arising from data breaches, there are three main categories of risk where liability can arise for technology companies. All three can be considered "catastrophe loss" in nature, meaning that claims tend to be infrequent but with high severity.

Breach of contract.

This occurs when a company suffers a financial loss due to breaching the terms of contract. Dependent on the type of work undertaken, almost any fault in service offering by a company could cause a breach of contract and therefore trigger a third party liability, this is the most common area of risk for technology companies.

Security.

Security failure can cause financial losses for third parties for which a company is responsible. For example, a security provider that failed to stop an unauthorised person (or virus) from gaining access to a client's computer system, which causes a financial loss to a third party.

Similarly the reverse is true and a company may fail to grant authority to someone who should have access to the system.

Media and intellectual property rights

Media claims generally occur because of defamation that causes damage to a third party and is a result of something that a company might have published, including adverts, blogs, twitter feeds and news articles. It includes breach of trade mark, digital rights violations, database rights, breach of confidential information or a breach of copyright which includes software code.

Technology companies must consider all of these risks in the context of their activities. The technology segments and exposure risk matrix, further in this document, provides a guide on the likelihood of claims types by technology industry segment.

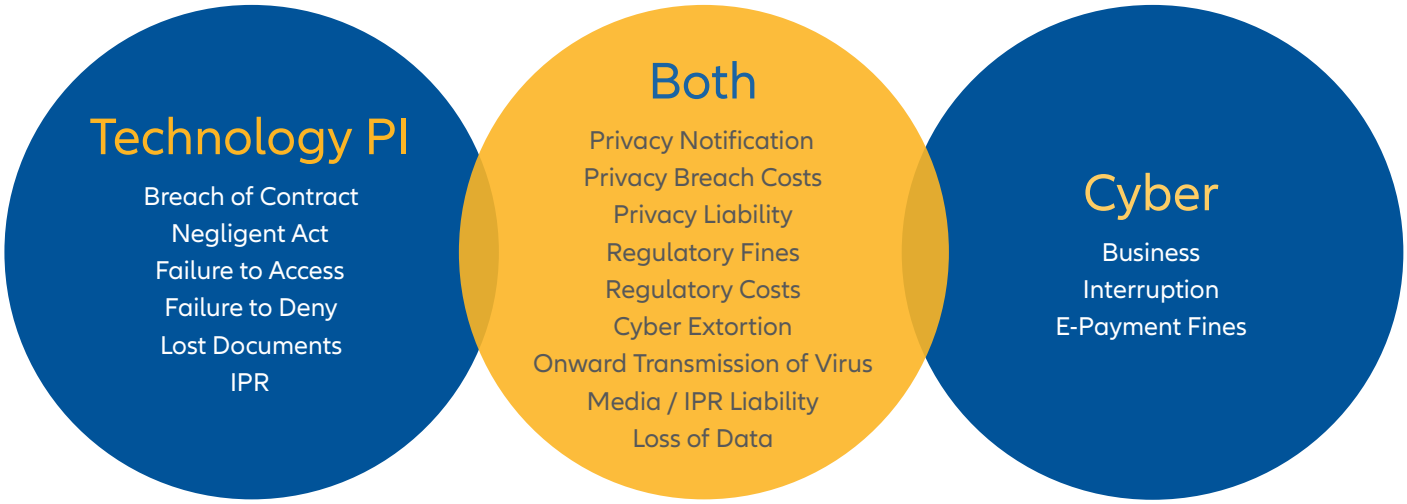
What are the 10 steps technology companies should adopt to mitigate their risks

1. Ensure all contractual work is thoroughly checked by the legal department.
2. Consider limiting liability where possible, either to a monetary figure or a percentage of fees paid.
3. Ensure contracts are signed off at the correct level.
4. Carefully consider if contractual obligations are realistic achievable.
5. Ensure the company has up to date response and disaster recovery plans that are tested at least annually.
6. Appropriate and regular training for all staff is essential, including internal guidelines.
7. Ensure Data Security is understood and internal guidelines and process' are in place and kept to.
8. Include stage gates with user acceptance testing at regular, short intervals to ensure long term projects stay on track.
9. Clear client dialogue will avoid later disputes.
10. Risk needs to be on the agenda at the highest level of any company as end to end risk management starts at the top.

Why is Technology PI different to Cyber?

What's the difference?

Professional indemnity insurance for technology companies sits at the intersection of professional indemnity insurance and cyber risk insurance. Potential exposures, risks and coverage needs however will vary across the spectrum of the technology sector.



The cover

Technology Professional Indemnity provides a bespoke cover for technology companies which responds to their specific needs and addresses those risks they face in providing products and services.

Cover	Details
Breach of contract	Defence costs and damages for which the insured is liable arising from breaching a client contract
Failure to access	Defence costs and damages for which the insured is liable for failing to enable access to a computer system or telecommunications device
Failure to deny access	Defence costs and damages for which the insured is liable for failing to stop unauthorised access to a computer system or telecommunications device
Virus cover	Defence costs and damages for which the insured is liable for passing on a virus to a third party
Lost Data liability	Defence costs and damages for which the insured is liable for losing, corrupting or erasing third party electronic data in their care and the costs to recreate such lost electronic data
Lost documents	Costs and damages for which the insured is liable for losing or destroying third party hard copy documents in their care and the costs to recreate such lost written data
Privacy and Data Breach cover	Defence costs and damages for which the Insured or Outsourced Service Provider is liable, arising from a loss of data
Media liability claims cover including IPR	Defence costs and damages for which the Insured is liable, arising from the publication or broadcasting of digital media content
Regulatory costs cover	Defence 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
Cyber extortion cover	Indemnity for the resolution of a credible threat to compromise the Insured's data or systems
Reputational Crisis Costs	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

Technology segments and exposure risk

The following table shows the estimated risk levels of technology segments and the risk covered on a scale of 1 to 5. We see the highest risks overall in software as a service and Third Party Liability and the lowest overall in Hardware, Media and Media Liability.

Risk Covered:	Client Industry:							
	Software Provision	Software as a Service	Hardware	Telecom	BPO / Service	Consulting	Media	Total
Third Party Liability	5	5	4	3	3	5	2	27
Network Security	4	4	1	2	2	3	1	17
Failure to Access	1	3	3	4	4	1	1	17
Media Liability	1	1	1	1	1	1	3	9
Privacy	3	3	2	5	3	3	4	23
Total	14	16	11	15	13	13	11	

1 = low risk, 5 = high risk
Source: Allianz

Why Allianz?

Allianz Global Corporate & Specialty (AGCS) is Allianz SE's dedicated brand for corporate and specialty insurance customers. AGCS (consisting of Allianz Global Corporate & Specialty SE and affiliated companies operating under the AGCS brand) provides insurance and risk management consultancy across the whole spectrum of marine, aviation (incl. space), alternative risk transfer and corporate business, including Energy, Engineering, Entertainment, Financial Lines (incl. D&O), Liability and Property insurance, including International Insurance Programs.

Worldwide, Allianz Global Corporate & Specialty has a global network in over 200 countiress and territories. It employs around 4,400 people and provides insurance solutions to more than three quarters of the Fortune Global 500 companies, writing a total of €9.3 billion gross premium worldwide annually (2020).

For more information visit
www.agcs.allianz.com