

newsletter

Critical information infrastructures (CII)

The interdependency of the critical infrastructures of information and communication technologies is forever on the rise. This development is confronting many key infrastructures of the state, society and the economy with new threats and vulnerabilities, which are, in turn, leaving their mark on the insurance risk landscape.

Definition

According to the definition provided by the BSI (Federal Office for Information Security) critical infrastructures are organisations and facilities of key importance to public interest whose failure or impairment could result in detrimental supply shortages, substantial disturbance to public order or similar dramatic impact. Critical infrastructures include power supply systems (power stations and networks), water supply systems, transportation and emergency services.

Critical information infrastructures (CII) are infrastructures based on information and communication technologies (ICT), ie telecommunications facilities, networks, computers and related software.

Terms of reference

Our society has become dependent on information and communication technologies (ICT) in many areas given their increasing prevalence in all areas of our lives. This dependency is especially high in segments where the use of internet and radio-based information technologies is on the rise. A whole raft of other factors are leading to additional hazard dimensions and presenting critical infrastructures with highly complex risks:

- Cross-company networks
- Corporate mergers
- Rationalisation
- Cross-border links
- Globalisation of value chains
- More fierce competition (cost pressure!)

These dependencies mean that local disruptions can trigger unforeseen chain reactions with massive, far-reaching consequences. (Examples of this are the widespread power cuts in the European power grid in Italy in 2003 and in wide areas of Europe in 2006.)

Scenarios and hazards

Critical infrastructures are exposed to a multitude of hazards, with possible scenarios ranging from natural perils, technical failure, accidents to targeted attacks of criminal or terrorist origin. Against the backdrop of the debate on climate change, experts are expecting an increasing number of cases of extreme weather (serious storms, torrential rains, long hot periods), which would in turn have a particularly adverse effect on critical infrastructures.

These exposures are accompanied by another potential source of threat - man-made hazards: in addition to sabotage and crime, system and network disruptions in particular can threaten the availability of infrastructures and result in major loss events. The interconnection within and between the infrastructure sectors via information technology plays a key enabling role in this respect. The increasingly complex nature of globally networked IT systems, the short innovation cycles specific to the individual industries and the trend towards the standardisation of IT solutions make the entrance of information technology into the critical infrastructure area a special risk factor.

Attacks on CII, examples

We have already witnessed one-off attacks on critical infrastructure IT systems:

- *Attacks on water supply (Queensland/ Australia, April 2000): In seek of revenge, an employee who was fired by the authorities of one town used his laptop and a wireless network to hack into the water supply control system of his former employer. He opened the sluice gates and a huge quantity of waste water poured into the local river system.*
- *The Slammer computer worm got into the controlling network of nuclear power station Davis-Besse (Ohio) at the beginning of 2003, blocked the digital controlling system, putting the station out of action for almost five hours. Damage was avoided due to the existence of an analogue backup system.*

Conclusion

Critical infrastructures were until recently still relatively independent of each other as most of them were devised and created on the basis of proprietary systems. This status is in flux and being replaced by systems that draw increasingly on information and communication technologies. The use of Internet technologies plays a key role in this respect, as these technologies have made infrastructures that were hitherto protected against global data networks vulnerable to new potential risks such as computer viruses, denial of service or hacker attacks. The interdependency of information technology critical infrastructures is set to increase. Telecommunication and power supply represent the core infrastructures in this respect.

This means that a critical infrastructure that lacks sufficiently protected IT systems no longer fulfils its function – neither today nor in the future. The Global Risk Report of the 2008 World Economic Forum cites an attack or system failure in critical information infrastructures as being one of the biggest global risks we are faced with today. The failure of IT-dependent infrastructures in particular and a resulting domino effect can lead to widespread outages in various infrastructure sectors. The loss potential is correspondingly high that results from the outages and failures of critical information infrastructures.

**Information for
the underwriter**

The mutual dependencies, in particular those of energy supply and information technologies, can snowball in the form of a cascading or domino effect and develop into especially high cross-company and cross-border loss potential. It is therefore important when identifying risk to evaluate critical infrastructures increasingly from the perspective of the ICT systems used, ie in terms of their reliability and availability.

The growing proliferation of IT and networking in the area of critical infrastructures raise the probability of major failures and outages occurring in the future which, given their interdependency, will have a knock-on effect on virtually every other type of infrastructure. Often the consequences or consequential damage that can be caused by an outage in the infrastructure area can be many times greater than the actual damage itself to the infrastructure in question.

On the insurance side, failures and outages in infrastructure can have an impact on liability and property covers in many insurance products. Examples are liability arising from the failure to supply or business interruption arising from the failure of external networks. Loss scenarios have a considerable accumulation potential should the outage take on major dimensions. Such loss accumulation scenarios can only be identified and evaluated to a limited extent on the basis of their inter-dependencies and system complexities. This presents a major challenge for risk engineering and product development.

As a consequence of the dynamic development of information technologies, CII structures today are subject to a constant and accelerated change process. Given this background, technical advances and regulatory developments have a significant influence on the security aspects of CII and from the insurers' point of view should be monitored constantly.

Contact

AssTech GmbH
Postfach 1211
85766 Unterföhring bei München
Telephone + 49 89 3844-1585
Telefax + 49 89 3844-1586
info@asstech.com
www.asstech.com