

Data Centres – An Underestimated Risk?

by Leo Ronken, Gen Re, Cologne

Increasingly, IT infrastructures are moving to cloud-based solutions. By 2024 cloud solutions[1] will account for more than 45% of IT spending.[2] The reasons? Lower costs, enhanced data analytics and more opportunities for collaboration. These developments are being fueled by the increasing digitalisation of corporate processes, along with a growing demand for the constant operational readiness and availability of IT systems and infrastructure. As a result, data centres are also increasingly becoming the central nervous system for the economy.

Such a concentration of data, however, involves high risk. The failure of a data centre has far-reaching consequences, such as risks to the security and availability of the stored data. In addition, such a failure – especially if it cannot be remedied at short notice – can result in major financial damages and loss of reputation not only for the operator of the data centre, but also for the companies connected to it, up to and including business closures. From an insurance perspective, both adequate Property cover and insurance against the consequences of a business interruption (BI) therefore play fundamental roles.

The causes that may lead to a data centre failure can be manifold, ranging from a cyber incident to classic damage caused, for example, by fire, water, natural hazards or vandalism. The following article focuses on classic causes of damage, especially damage caused by fire. Recommendations concern fire protection measures and determining the exposure from the perspective of a Property underwriter.

Types of data centres

Data centres have physical premises that store data and applications from one or more companies and process them on a large scale. The term data centre refers to the organisation that administers and manages the IT, using a network of computing and storage resources for that purpose.

Content

Types of data centres	1
Damage assessments	3
Effective protective measures	4
Underwriting considerations	6
Summary	7

About This Newsletter

Created for our clients, our Property Matters publication provides an in-depth look at timely and important topics affecting commercial and personal lines of property insurance.

A distinction is made between external and internal data centres; there are data centres of service providers and then there are a company's own (in-house) data centres. Both use comparable computer systems and infrastructures.

Essential components for the operation of a data centre/IT network include:

- Servers (hardware consisting of CPU, main memory, hard disks)
- Active network components (routers, switches, firewalls, controllers with active power connection)
- Passive network components (cabling, plugs, sockets without their own power connection)
- Racks (metal enclosures to house the server hardware as well as the network components)

In addition, components for operating a data centre include infrastructure, energy supply, air-conditioning, ventilation technology and corresponding safety equipment.

A wide range of smaller, larger, and even global providers offer different IT solution structures to manage data and processes. They can be roughly described as follows:

- Hosting/Decentralised servers – Companies use servers or server racks from the data centre provider.
- Cloud service – Companies map the entire IT structure of an internal data centre onto the data centre of a service company.
- Managed services – Instead of the entire IT structure, only individual services of a cloud provider are used.

The different types of cloud-based solutions include:

- Private clouds
  The cloud infrastructure is operated only for one institution by the institution in question or a third party. In this case, the IT structure with completely isolated access is assigned to just one end user or user group.
- Public clouds
  A provider offers the cloud infrastructure, and it is used by the general public or a large group; for example, an entire industry sector. Public clouds are usually based on IT infrastructures that do not belong to the end user. The largest public cloud providers include: Amazon Web Services, Alibaba Cloud, IBM Cloud, Google Cloud and Microsoft Azure.
- Community clouds
  The cloud infrastructure is shared by several institutions that have similar interests, and it is operated by one of these institutions or a third party.
- Hybrid clouds
  Multiple cloud infrastructures are used via a standardised interface. It is a single IT environment consisting of several areas connected via LAN (Local Area Network), WAN (Wide Area Network), VPN (Virtual Private Network) and/or APIs (Application Programming Interface). They can have very complex structures. IT systems automatically become a hybrid cloud when applications can be freely migrated between several separate but interconnected environments.

Data centres/cloud offerings are operated with different service models, which can be roughly differentiated as follows:

- Infrastructure as a Service (IaaS)
  IT resources – such as computing power, data storage or networks – are offered as a service. An IaaS provider offers on-demand access to key IT resources, such as computers (virtual or dedicated hardware), networks and storage via the Internet. A cloud customer buys/rents these virtualised and highly standardised services and builds its own services on top of them for internal or external use; for example, to run an operating system with applications of their choice.
- Platform as a Service (PaaS)
  A PaaS provider provides a complete infrastructure and offers the customer standardised interfaces. For example, the platform can provide multi-client capability, scalability, access control, database access, etc. However, the customer has no access to the underlying layers – such as the IT operating system and hardware – but the customer can run its own applications on the platform, and the cloud operator usually offers his hardware and software tools for developing that capability.
- Software as a Service (SaaS)
  This is a cloud-based service that provides access to a standard software product that is operated and managed by a cloud service provider. All applications that meet the criteria of cloud computing fall into this category. There are no limits to the range of offerings. Examples include: contact data management, financial accounting, word processing or collaboration applications.

The service models also differ regarding the customer's influence on the security of the services offered. With an IaaS, the customer has full control over the IT system from the operating system upwards, as everything is operated within his area of responsibility. With PaaS, the customer only has control over applications running on the platform. With SaaS, the customer hands over control to the cloud service provider.

Other common distinctions arise from their purpose, e.g., emergency data centre, backup data centre.

Common to all types of data centres is the guarantee of highest possible reliability and availability of their services. The term availability refers to the probability that a system can actually be used as planned at a given time. Availability is measured as the ratio of downtime to the total time of a system.

$$\text{Availability (in procent)} = \left(1 - \frac{\text{downtime}}{\text{production time + downtime}}\right) \cdot 100$$

In the 1990s the Uptime Institute in the U.S. introduced the tier classification as a worldwide standard for availability.[3] The Tier 1 classification constitutes an availability of 99.671% or, in other words, a maximum permitted downtime of 28.8 hours per year up to the Tier 4 classification with an availability requirement of 99.995% (max. downtime of 26.3 hours/year), including maintenance times. The higher the user requirements on the availability of a data centre, the higher the costs for meeting the necessary security and redundancy requirements.

Damage assessments

Data centres contain a large number of devices with high electrical power consumption, corresponding power supply units and connecting cables, which are susceptible to fire, especially in the event of defects or overload. Specifically, significant air conditioning and ventilation technology is required in a data centre to dissipate the enormous heat generated by the servers. The combination of that technology, and the high heat caused by increasing integration and packing density in processors and ITC systems as well as other electrical devices, makes it difficult to detect and successfully fight a fire using conventional fire protection measures, such as passive fire detection sensors and fire extinguishing systems.

If, for example, a fire breaks out in a data centre and is not immediately detected and successfully extinguished, it is likely that data will be irretrievably destroyed and can no longer be retrieved by the user. This causes considerable damage not only to the operator of a data centre, but especially to its users. In addition, there are enormous costs to repair the damage as quickly as possible and to restore the availability of the data centre. According to a Statista publication, 25% of the 1,200 respondents to a survey said the average hourly cost of critical server downtime in 2019 and 2020 was between USD 301,000 and USD 400,000, with 15% (2019) and 17% (2020) incurring more than USD 5 million.[4]

Fire is still one of the main causes of data centre failures. The high density of electrical power, sometimes several megawatts, increases the potential fire hazard caused by arcing, short circuits, smouldering fires or defective components, among other things.

A recent major loss, probably in the hundreds of millions of euros, occurred on 10 March 2021 in a data centre of a large data cloud provider with more than 100,000 servers in Strasbourg, France. The fire broke out in one of the four data centre buildings, consisting of five floors with a floor area of 500 square meters and approximately 12,000 servers. The cause is still not clear. Initially, a technical defect was suspected.[5] After some time, the fire spread to a second data centre and completely destroyed several server rooms. As a result, all data centres at the site had to be shut down, which led to millions of websites being offline.[6] In some cases, this caused a complete loss of all user data, as a large number of users had refrained from having their data regularly backed up by the cloud provider due to cost considerations. On 19 March 2021 a second fire occurred in the battery rooms of the partially damaged data centre.[7] As a result, it was decided not to reconnect this data centre to the network.

More than 100 specialists were deployed in order to limit the damage. After installing an additional 15,000 servers, the hope was that the data centre could be restarted on 22 March. However, of the original four data centres, only two could be restarted, on 26 March 2021.[8] Undamaged or cleaned racks from the destroyed data centres were used in the two remaining data centres. One challenge was to remove the soot from the equipment and boards; it takes about seven hours to clean one server.[9]

According to fire protection experts, the construction of the buildings and the lack of automatic fire extinguishing systems contributed significantly to the extent of the damage.

The waiver of a regular backup of application data does not seem to be an isolated case, as research by Bayerischer Rundfunk, the Bavarian broadcasting company in Munich, has revealed. According to this research, other cloud operators and their customers also partly forgo essential security and fire protection measures for cost reasons.[10]

Effective protective measures

A wide variety of security requirements are placed on a data centre in accordance with the agreed availability requirement, depending on the required security level. These range from access, data and fire protection to protection against natural hazards, terrorist attacks and political threats. The protection requirements can be so high that the data centres are housed in bunkers and expanded into high-security wings.

The Trusted Site Infrastructure (TSI)[11] and EN 50600[12] criteria catalogues provide orientation for the effective protection of IT systems. The need for protection in a data centre relates to personnel, equipment, data and availability. A rough distinction is made between two approaches:

- Conventional fire protection measures, e.g., the establishment of fire compartments, fire monitoring and sprinkler systems. The maxim followed here is that damage to the equipment is not necessarily prevented but limited.
- Operation mode-specific fire protection measures aimed at protecting the data and availability of the data centre as well as its services. In particular, the aim is to prevent a fire (e.g., by selection of building materials and components, reduction of the oxygen concentration in the rooms concerned), to detect and combat a fire in its early stages (e.g., installation of early fire detection systems or an automatic gas extinguishing system) or to limit the effects of a loss on the availability of the data centre and the security of the data through redundant systems, supply structures and alternative locations.

In order to keep the scope of this article manageable, the advice and recommendations presented below focus on measures against the source, spread and consequences of a fire.

Structural fire protection measures

Structural measures are intended to prevent or limit the spread of fire or smoke and its expansion across several rooms or buildings. Essential building blocks of structural fire protection are the type of construction, complex/fire walls, fire-resistant walls as well as the fire-resistant partitioning of penetrations of all kinds by fire-protective partitions.

Design

As far as possible, no combustible building materials and components should be used for the construction of the building and its furnishings. They would increase the fire load and lead to a faster spread of fire, smoke and heat radiation, which damage or destroy sensitive IT equipment. If the fire has engulfed a building, it can usually be assumed that the data centre will suffer major damage, if not total loss. In such a case, the fire brigade can only concentrate on protecting the neighbouring buildings.

Fire walls/complex partition walls

Fire walls and complex partitions divide a building into sections so that a fire cannot spread to neighbouring sections. Thus they constitute an important structural fire protection measure, as they often prevent the total loss of a building and its contents by confining the fire to the outbreak area, and by this enable the fire brigade to fight the fire more effectively. Especially in the case of data centres, a building should be divided into different complex/fire sections in order to save part of the IT structure.

Technical rooms

Technical rooms provide the infrastructure for the operation of IT. This includes water, heating, power supply (e.g., transformers, sub-distribution, emergency power supply), ventilation/air conditioning, telecommunications and network technology. They should each be housed in their own fire-resistant room so that a fire in one room cannot spread further.

Wall and ceiling openings

Penetrations through walls and ceilings of fire protection or fire-resistant walls should each be sealed off by appropriate measures in order to prevent the spread of a fire. This also applies to installation ducts, pipelines, windows, doors as well as water and gas pipes. Cable and other supply ducts can be additionally protected by fireproof cladding/installation to ensure functional integrity for 30 to 90 minutes. Furthermore, care should be taken to ensure that the protective measures are not only fire but also smoke proof. Depending on the application, a wide variety of options are available, e.g., fire protection cushions, intumescent materials, ductwork made of non-combustible material, use of fire-retardant electrical lines and cables, cable bulkheads.

Technical fire protection measures

Technical fire protection measures are essential for a data centre, as they should either prevent a fire from starting (e.g., oxygen reduction system) or detect, fight and ideally extinguish a fire as quickly as possible in order to minimize the potential damage as much as possible.

Automatic fire extinguishing systems

Automatic fire extinguishing systems, conceived and designed for the special requirements of a data centre, should be considered an absolute necessity with regard to the high safety standards at a data centre, because they prevent, or at least detect and fight, an incipient fire automatically. Due to the presence of electrical/electronic components, sprinkler or fire extinguishing systems using water should not be installed. Inert gas fire extinguishing systems flood the affected area with a non-flammable gas such as carbon dioxide, nitrogen or inert gas mixtures. This lowers the oxygen concentration in the room and smothers the flames. When planning an extinguishing system with gaseous extinguishing agents, room pressure relief must be taken into account in order to dissipate the resulting short-term increase or decrease in pressure.

Oftentimes computer rooms are protected by oxygen reduction systems, unless a permanent staff presence is required. An oxygen reduction system creates a permanently oxygen-reduced atmosphere by letting in nitrogen. This eliminates the possibility of an open fire. In order to maintain the constant reduction of the oxygen, the room should be designed as tightly as possible so that nitrogen does not have to be permanently supplied on a large scale.

A challenge for fire protection in data centres is posed by closed server cabinets that have an integrated cooling system and operate in recirculation mode. Smouldering fires can almost no longer be detected, as only a very small amount of the smoke penetrates to the outside. At the same time, gaseous extinguishing agents cannot penetrate these cabinets from the outside. For such server cabinets, compact fire detection and extinguishing systems should be used, e.g., integrated in the form of a 19-inch rack.

Automatic fire detection

In order to detect a fire as quickly as possible, an automatic fire alarm system should be installed in all rooms with direct fire alarm notification to a permanently manned location, e.g., control room of the data centre, fire brigade. So-called smoke aspiration detectors are particularly effective, as they constantly aspirate the air in the room or rack and check it for potential smoke particles. They are largely immune to false alarms and react to even the smallest amounts of smoke. Smouldering fires caused by contaminated cables can thus be detected and reported before a fire breaks out.

Conventional fire detection systems (point or line detectors), on the other hand, where sensors are installed near or on the ceiling of buildings, may not respond in the early stages of smoke and fire, as the smoke is usually delayed in reaching the vicinity of the fire detectors by the installed ventilation and air conditioning technology.

Organisational and operational measures

Organisational and operational measures include all measures with which the operator of the data centre attempts to reduce the possibility of a fire occurring, e.g., through employee training and safety instructions or, in the event of a loss, an emergency plan for the fire brigade and for the safety of employees. This supports fast and effective firefighting as well as quick restoration of the data centre.

A variety of options are available, which will only be briefly touched upon here, as they largely apply to many types of operations. Among others, these include the designation of rescue and attack routes for the fire brigade, emergency shutdown plans, IT restart plans, fire protection regulations, operating instructions, signposting/marking of locations for initial firefighting equipment (e.g., fire extinguishers, wall hydrants), instructions for avoiding unnecessary fire loads, smoking bans, permits for work involving fire hazards, instruction of outside companies, visitor regulations, and training of employees in safety issues.

Business interruption measures

Due to the high availability requirements as well as the expected high downtime costs per hour, measures for a data centre require special attention in order to avoid or minimise a possible interruption of operations. Depending on the required availability of a data centre, it may even be necessary to maintain a second, spatially separate data centre in parallel. In that case the applications and data are permanently mirrored so that in the event of a failure of one data centre, the second data centre can take over operation almost seamlessly.

The core measures should include a regular backup process in order to have necessary data and programmes available again as quickly as possible. The backup strategy is based on the data security and availability requirements, which may

range from weekly data and programme backups to daily, hourly or even permanent backups. The backups should be stored at a location other than the data centre. One might even consider permanent backups being made via data centres that are geographically distant from each other in case of a major loss event (e.g., an explosion, natural disaster or a loss event that affects regions, countries or continents), thus ensuring the secure availability of the data and applications.

In order to keep the implications of a loss at a data centre as low as possible, a business continuity plan (BCP) is essential. A BCP specifies all important steps and the persons responsible in the event of a loss. The goal is to restore operations as quickly as possible. Such a plan should be regularly reviewed and tested.[13]

Further protective measures

Of course, a fire is only one potential source of considerable damage at a data centre. As already pointed out, many other criteria must be taken into account for a comprehensive security concept in order to exclude or reduce a potential risk for a data centre and its services. Since a comprehensive presentation would go beyond the scope of this article, the following includes just a few examples of additional risks that should be taken into account:

- Political, natural (earthquake, flood, hail, storm, landslide, subsidence), infrastructure and neighbourhood hazards
- Sabotage, data misuse and hacking (cyber incidents)
- Unauthorised access, burglary or theft
- Damage caused by vibrations, chemicals
- Leakage, e.g., cooling liquids, tap water

Underwriting considerations

When insuring a data centre, special attention should be paid to Business Interruption insurance and the risk of damage caused by fire and water. In addition, natural hazards in exposed areas can pose an essential threat. For exposure-oriented underwriting, an up-to-date inspection report should always be available, preferably not older than two years, because technology, infrastructure and especially business interruption scenarios are subject to constant change.

Property risk

For the assessment of the Property risk, the following information should be available at a minimum:

- Type of data centre and description of its performance/ services including the required availability
- Site address
- Layout and occupancy/use of the individual buildings
- Value of the buildings/facilities including infrastructure
- Potential natural hazards at the data centre site
- Protective measures for Flexa (losses due to fire, lightning, explosion, aircraft) as well as other hazards that fall under the requested insurance cover (e.g., fire, water, burglary, theft, sabotage, natural hazards). This includes the specifications of the construction type, building materials and components used, presence of complex/fire compartment separations as well as fire-resistant separated areas, technical, operational, organisational preventive as well as defensive protection and safety measures.

Business Interruption risk

In addition to the description and assessment of the Property risk, particular attention should be paid to the Business Interruption risk. The special exposure characteristics that should be addressed include:

- Expected or contractually agreed availability of the data centre
- Replacement time for damaged IT systems, e.g., servers and infrastructure systems necessary for the operation of the data centre, such as transformers, power, ventilation, air conditioning, communication and network technology
- Time for the reconstruction of the buildings, rooms, server systems as well as the energy and other necessary infrastructure, in particular, the restoration of the communication and network technology, including restart tests
- Downtime until the planned emergency measures take effect (business continuity plan) and customers can be served again accordingly, e.g., switching to an alternative/backup data centre
- Backup strategy and the time needed to restore the backups
- Extent to which a loss event caused by the failure of the data centre may result in contractually agreed penalties

Insurance contract

Next it is worth taking a look at the wording of the underlying insurance contract, including the inclusion/exclusion clauses as well as the agreed first-loss sums. In particular, the following topics should be considered in this context:

- Are cyber incidents and their consequences, as well as other perils, covered by the existing insurance contract? E.g., terrorism, civil unrest, electronics, energy failure, consequential financial loss, intentional acts, data protection breaches, contractual penalties and consequences of non-physical damage events.
- To what extent can other insurance contracts – e.g., liability, electronics, data/software, burglary/theft, fidelity, cyber, but also regress/impact agreements, also from third parties that have a business relationship with the data centre operator – accumulate in the event of a loss? The latter cannot be determined beyond doubt, so the resulting uncertainty about possible accumulation scenarios should be included in the capacity considerations.

Type of indemnity

Furthermore, the type of indemnity should be included in the underwriting considerations:

- Type of compensation (e.g., daily rate, single sum)
- Duration of the compensation payment (liability period)
- Agreed additional costs, e.g., for the use of other facilities, the application of other working procedures, retrofitting or rehabilitation, necessary reprogramming, as well as the use of labour and services for crisis management until the complete restoration of normal operations
- Contractually agreed penalties due in the event of a claim as well as costs for the restoration of reputational losses suffered
- Forensic costs for searching, finding the causes of damage and restoring the data as well as costs for necessary experts to determine the obligation to pay compensation and indemnity

Summary

Among other hazards, a fire event represents a massive potential threat to the availability of a data centre. While preventive fire protection measures can significantly reduce this risk, Property insurance underwriters are increasingly interested in determining the actual hazard exposure for a data centre in order to make an informed underwriting decision. This includes taking into account so-called ancillary as well as natural hazards. It is therefore important that an up-to-date survey report is available for exposure-oriented underwriting, as the technology, infrastructure and, in particular, business interruption scenarios of data centres are subject to constant change.

As data centres increasingly become the central hub for the economy, a data centre failure has far-reaching consequences, not only for the operator of the data centre, but also for the companies connected to it. For this reason, it is increasingly important that data centres have optimum protection to prevent damage of any kind.

Further reading

Cornerstone Paper, Security Recommendations for Cloud Computing Providers – Minimum Requirements in Information Security https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile&v=8

About the Author

Leo Ronken *is a Senior Underwriting Consultant for Gen Re's Global Underwriting department in Cologne. He may be reached at +49 221 9738 939 or leo.ronken@genre.com.*

Endnotes

1 The term cloud computing is not uniformly defined in this context; a definition by the U.S. standardisation body NIST (National Institute of Standards and Technology) describes the term sufficiently, as a model that allows convenient access on demand anytime and anywhere via a network to a shared pool of configurable computing resources (e.g., networks, servers, storage systems, applications and services) that can be made available quickly and with minimal management effort or service provider interaction. The NIST Definition of Cloud Computing, https://csrc.nist.gov/publications/detail/sp/800-145/final.

2 Gartner Research, Cloud Shift Impacts All IT Markets, 26 October 2020.

3 www.uptimeinstitute.com/tiers.

4 Average cost per hour of enterprise server downtime worldwide in 2019, published by Thomas Alsop, 7 December 2020, https://www.statista.com/statistics/753938/worldwide-enterprise-server-hourly-downtime-cost/.

5 Christian Schubert: Millions of websites affected by fire at cloud operator, FAZ 11 March 2021, https://www.faz.net/aktuell/wirtschaft/digitec/brand-bei-cloud-betreiber-millionen-von-webseiten-betroffen-17238989.html; https://www.reuters.com/article/us-france-ovh-fire/fire-breaks-out-in-ovh-building-in-strasbourg-france-idUSKBN2B20NU.

6 Data centre fire: Why a cloud strategy is so important, 7 April 2021, https://www.handelsblatt.com/technik/it-internet/it-dienstleister-brand-im-rechenzentrum-warum-eine-cloud-strategie-so-wichtig-ist/27074336.html?ticket=ST-2013868-D2EGJuwQcuHBElHfpaHF-ap1.

7 OVH to Shutter Second Strasbourg Data Center After Smoke Incident, Rich Miller, 20 March 2021, https://datacenterfrontier.com/ovh-to-shutter-second-strasbourg-data-center-after-smoke-incident/.

8 Philipp Anz, 26 March 2021, First OVH data centre in Strasbourg resumes operations, https://www.inside-it.ch/de/post/erstes-ovh-rechenzentrum-in-strassburg-nimmt-betrieb-wieder-auf-20210326.

9 RZ fire in Strasbourg not yet dealt with, 14 April 2021, https://www.inside-channels.ch/de/post/rz-brand-in-strassburg-ist-noch-nicht-bewaeltigt-20210414.

10 Is data in the cloud really safe? | BR24, https://www.br.de/nachrichten/netzwelt/sind-daten-in-der-cloud-wirklich-sicher,SRq2lbb.

11 https://www.tuvit.de/de/leistungen/rechenzentren-colocation-cloud-infrastrukturen/trusted-site-infrastructure/.

12 https://www.din.de/de/meta/suche/62730!search?query=DIN+EN+50600.

13 For further information on this topic as well as tips for creating a Business Continuity Management (BCM) plan, See article: More Valuable Than Ever, General Reinsurance AG August 2020, https://www.genre.com/knowledge/publications/pmint20-3-de.html

The people behind the promise.®

genre.com | genre.com/perspective | Twitter: @Gen_Re

General Reinsurance AG
Theodor-Heuss-Ring 11
50668 Cologne
Tel. +49 221 9738 0
Fax +49 221 9738 494