UNDER LOCK AND KEYCHAIN

Protecting the vast amount of data we now produce every day demands an incredibly specialised type of property, and the surveying skills to match

Words *Katie Puckett*
Illustration *Jonathan Petersen*

They could be as vast as an Amazon distribution centre, as energy-hungry as a steelworks, and as critical as a power station or hospital. Yet many of us will never have seen a data centre — or at least that is what you may think. And that is exactly how their owners want it.

"You've been past a lot more than you know," says Darren Hill MRICS, associate director in JLL's EMEA data centre team. "But that's the whole idea. You're not supposed to know where they are."

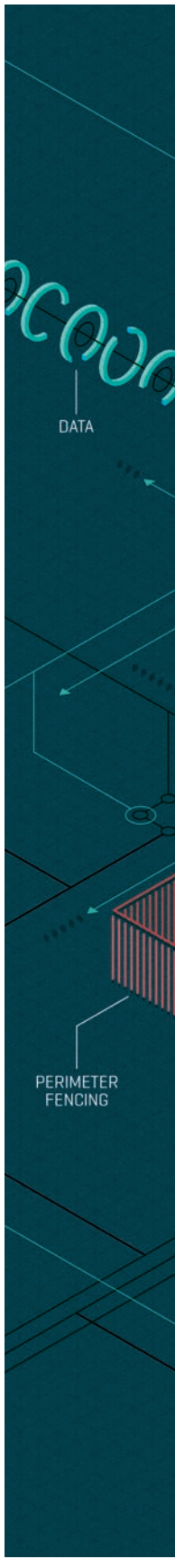
The reason for this is simple. Data centres are the internet. They are "the cloud". They are the huge, humming sheds through which every email, Google search, Netflix movie, online transaction and Donald Trump tweet must pass as it circles the earth. Just a few minutes of downtime could be disastrous for the companies, governments and financial markets that rely on them, so data centres are designed to be constantly operational, and protected from every conceivable threat — natural or manmade. Anonymity is the first step in a rigorous high-security philosophy that leaves nothing to chance.

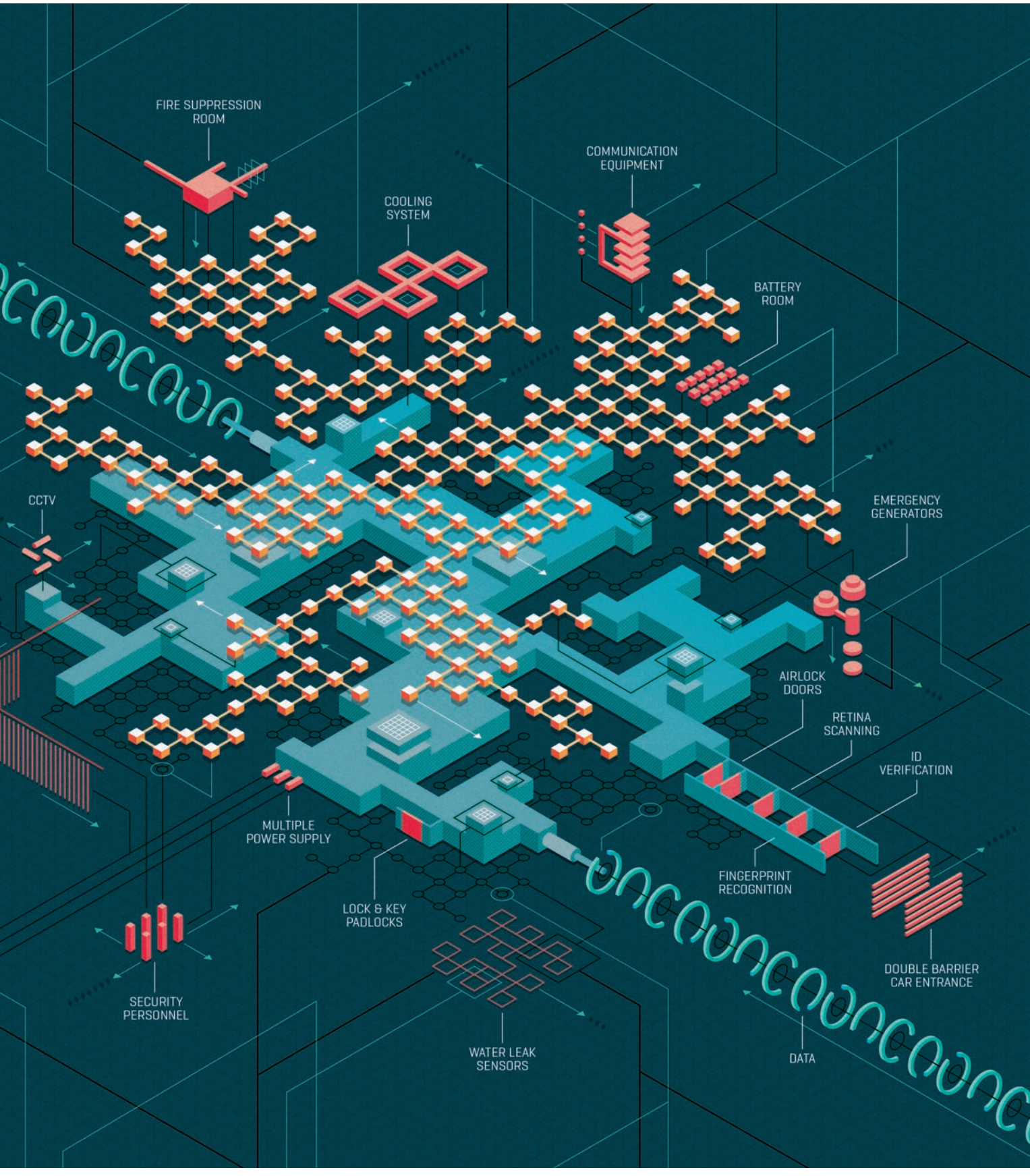
"Data centres are one of the most expensive building types on the planet, and the IT equipment that's in them is massively important to the businesses that use them," says Andrew Jay MRICS, head of data centre solutions at CBRE. "So the people who are responsible for that equipment are paranoid — they're paid to be paranoid. The goal is that once a server is plugged in and powered up, the next time it will be turned off is when it's at the end of its life."

Physical security is just one aspect of ensuring a data centre remains operational. They must have security of power supply, adequate cooling to keep the equipment within operating temperature range, and they must offer a windproof and watertight environment, even in extreme weather or during seismic events. Jay explains the data centre developer's philosophy: "They would start by saying: 'Let's have a really good power supply — but assume that gets cut off, let's have a second one, from a different substation. But actually, what if they're both turned off at the same time — let's have some generators. But let's assume that when I need the generators, they don't all start, so we'll have some back-up generators.' It's the same with the cooling system, and with the connectivity to the building. They go to the 'nth' degree on everything." From there, it is not hard to see that the security systems must be pretty substantial (box, overleaf).

Once you get into that paranoid mindset, where does it end? In fact, as the market has matured, resilience has been codified into globally recognised industry standards, such as those set by the Telecommunications Industry Association (TIA) or the Uptime Institute (UTI). UTI "tier 3" data centres are "concurrently maintainable", so any part can be taken down for repairs or maintenance without affecting the running of the facility. Tier 4 have two completely separate paths, for power, cooling and network. Retrofitting older centres is not necessarily viable: "It's very hard to turn a tier 2 into a tier 3 — you need to have done it from scratch," says Mark Trevor MRICS, head of Cushman & Wakefield's data centre advisory group. Governments may also have their own specifications, such as the UK's "business impact levels" — IL3 being for restricted or high-level government information and the highest, IL6, for use by the secret services.

Site selection is critical. A data centre cannot be on a floodplain or under a flight path, needs to be as far from any hazard as possible, but have excellent power and network connections. Jay finds that the role of the RICS professional is often to mediate between the many specialists involved — translating the security experts' concerns for the commercial team, and vice versa. So if, for example, the security expert baulks at a prospective site next to a main road, Jay knows it is because there is a risk of ram-raiding or explosions caused by passing »




FIRE SUPPRESSION ROOM
COMMUNICATION EQUIPMENT
COOLING SYSTEM
BATTERY ROOM
CCTV
EMERGENCY GENERATORS
AIRLOCK DOORS
RETINA SCANNING
ID VERIFICATION
MULTIPLE POWER SUPPLY
FINGERPRINT RECOGNITION
LOCK & KEY PADLOCKS
DOUBLE BARRIER CAR ENTRANCE
SECURITY PERSONNEL
WATER LEAK SENSORS
DATA

petrol tankers: "Our skill is that we can speak the language of all different interest groups and bring them together."

But there is a limit to how many of these remote sites there are, particularly as the era of big data puts ever greater demand on the space required to process, analyse and store the world's information. According to IBM, every day we create 2.5 quintillion bytes of data — a quintillion is 1 followed by 18 zeros — and 90% of all the data that exists today has been created in the last two years.

The big consumers of data centre space are the three "hyper-scale" providers: Amazon, Microsoft and Google. They can locate their vast facilities anywhere in the world, dictated by a variety of factors. The Nordic countries can attract power-hungry tech giants with cheap, green energy and the free cooling of a cold climate. US firms have also flocked to Dublin for its low rate of corporation tax.

Meanwhile, there is a parallel trend for "edge" data centres close to population centres, which can deliver large amounts of data where it is needed with as little latency as possible — minimising the buffering on your Netflix stream. This is where achieving anonymity is hardest. Many such facilities are concealed in nondescript buildings with mirrored windows or suspicious amounts of plant or communication equipment on the roof. "The perfect scenario is a shed in acres of open land, surrounded by high fencing and armed guards," says Hill. "But you're just not going to get that in many places around the world, especially not in big cities."

The strongest growth area for data centres is Asia-Pacific, home to some of the world's most youthful populations yet to fully come online. Indonesia, for example, has more than 260 million people and a median age of just 28. "Smartphone penetration is below 50% but it still totals something like 50 million users," says Paul Dwyer MRICS, JLL's regional lead for data centre services.

> *"The perfect scenario is a shed in acres of open land, surrounded by high fencing and armed guards"*
>
> **DARREN HILL MRICS** JLL

Alongside its great potential, this region also presents a range of climatic, seismic and geopolitical threats, as well as the prospect of rolling blackouts in some places. But the paranoid data-centre mindset stands developers in good stead when entering new markets — they already build fortresses with multiple back-up systems, which negates a lot of these issues. "There are many codes of practice, and larger data centre providers have their own standards to meet," says Paul Johnson, regional director for Faithful+Gould in Hong Kong. "It would be catastrophic if the power went down, but there are a multitude of tests during the commissioning stage to ensure that it will not."

Due diligence when choosing a site is even more important, however. "It's about being a little bit more cautious and managing a raised risk profile," says Dwyer. "Some places are more stable than others. In Indonesia, we'd be looking at back-up supplies of fuel and deliveries. It's inevitable that power is going to go down, so we look at what we need to do to stay online."

The region's four primary markets are Tokyo, Singapore, Hong Kong and Sydney, but there is considerable development in countries such as Malaysia, Vietnam, Thailand and the Philippines, as the centre of demand shifts. Shanghai could be added to the primary list, Dwyer suggests, with some caveats. "It's not somewhere where you'd put your first or only deployment in Asia-Pacific. You wouldn't look to do too much due to the barriers to entry to mainland China. You'd want to hold most of your critical information outside the border."

Tokyo has lost market share to Hong Kong and Singapore over the last five years, partly because they are better located for emerging markets in south-east Asia, but also because it is so seismically active. "Tokyo is moving most of the time," says Dwyer. "There's a lot of good technology that can help but, ultimately, if something big enough happens, nothing is going to withstand it." Companies are now prioritising development in Osaka, he adds. "It's on a separate tectonic plate to Tokyo, and it's got a separate power grid, so it's a very suitable disaster recovery location."

But local threats are only half the story. What data centre operators are not responsible for is the cyber-security of the information within — arguably a much greater risk, as illustrated by the unprecedented cyber-attack last October that disrupted services across Europe and the US. After all, if you had the choice of mounting a *Mission Impossible*-style break-in, or hacking from the comfort of your armchair, which would you choose? ■

SECURITY CHECK

Think you can break into a data centre?

Even visiting a data centre is a pretty tall order. There may be as many as eight layers of physical security, "and that's before you even get to the room that holds the server racks", says JLL's Darren Hill MRICS. "Essentially, there's no real limit to how well you can secure a data centre." This is what you are up against.

Prior notification All visits must be notified at least 24 hours in advance, along with details of a passport or other official photo ID. Prepare to show this many times when you get on site, too.

Perimeter fencing Robust, high, ram-proof and topped with razor wire – if not electrified – the fencing around data centres leaves nothing to chance. The whole site will be monitored by CCTV, with no blind spots.

Vehicle traps Do not expect to just drive your car through a single barrier. There will be two, trapping you inside until the guards are satisfied that you are who you say you are. This will be mirrored by airlock doors inside, too – if you make it that far.

Biometrics Well-drilled security personnel are on site 24/7 – but to eliminate human error, visitors must also pass technological checks such as fingerprint recognition or retina scans. Access logs will be retained.

Everything else Even if you manage to clear the reception area, you may still struggle to get anywhere near the all-important equipment. Server racks can be fitted with an almost limitless number of security add-ons, depending on what they contain and how risk-averse the owner of the data is – from a single padlock, via a lock and key, to dedicated caging with additional biometric checks.