How Critical is Your Data? What Value Should You Place on IT?

Given enough time, the right tools (and a bus pass), anybody with minimal skills can break into any building.

This may be for purposes of theft, industrial espionage, malicious damage or acts of terrorism to deny access to data or cripple national infrastructure. In this uncertain world, these are now conceivable threats.

It is impossible to eliminate every threat, but we can certainly put measures in place to significantly slow down an attack until reinforcements arrive, prevent surreptitious access or reduce the effects of blast damage. High concentrations of data held in a data centre must be analysed in the light of its value or criticality against the cost of putting reasonable protection measures in place. It may be that the most critical data requires a higher level of protection than others.

Security Principles & Vulnerable Areas

Our ancestors had the right idea about good security – seen in the principles of castle building. It is all about the layers – moats, outer walls and the strongest walls for the inner keep. The principle is still valid today.

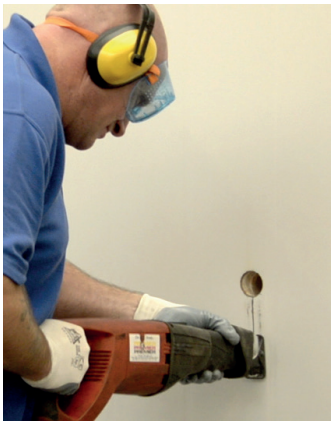
A modern high security data centre may have impressive looking steel fencing and then a solid looking shell of the building with cameras, detection systems, etc., but you still need your inner keep to protect critical systems and data. Electronic security will provide detection – but you still require physical security to provide protection. This is even more critical in cases where the attackers are not worried about detection or capture.

You can now go to your local DIY store and pick up powerful battery or petrol driven cutting tools with the latest technology blades that will cut through solid steel like a knife through butter.

Typical 2–3mm thick high security steel fencing may deter some and slow down others, but with the right tools it can be breached in seconds. The same applies for car park 'modular container solutions'.

The average ISO container is built on a very sturdy frame – but the sheet steel of the sides is less than 2mm thick. For standard commercial or industrial buildings, steel cladding may be less than 1mm thick. Again no contest against modern power tools.

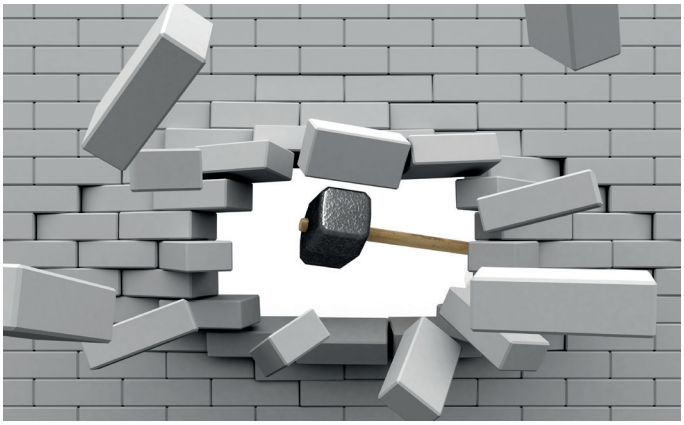
Note that standard internal 'whitewall' panels used in many major data centres have steel skins of only 0.5 or 0.7mm – with the core material offering no resistance. These can be easily cut with an axe and of course with powered tools in seconds.



Favoured areas of attack are doors and windows. The average non security rated doors offer little defence to those with the correct tools and knowhow.

Particularly vulnerable are emergency push bar exit doors. These can be easily manipulated to gain access. An average mag lock with access control can be overcome by reasonable force or surreptitiously. A quick spray with hair lacquer by a visitor would allow later re-entry.

Brick or block walls have an inherent weakness in the joints – meaning a simple sledgehammer can make short work of getting through. You are only as secure as your weakest point of entry!



Commercial & Government Security Standards

The commercial standards for the protection of building elements are set by the **Loss Prevention Certification Board (LPCB)** – an organisation established by the UK insurance industry. Hence meeting the requirements of the standard will not only protect your critical assets but will be seen favourably by your insurance companies or those of your clients. The standard is **LPS1175** and is graded from **SR1 to SR8**. As you rise through the grades the attack/test time increases and the toolset used is upgraded with more powerful tools. Hence SR1 will use a very basic toolset (screwdrivers, pliers, etc), rising to tools with a higher mechanical advantage and then on to powered cutting tools at SR4, SR5, etc.

For Government or Government contractor assets, where there is a security requirement, the standards are set by **The Centre for the Protection of National Infrastructure (CPNI)**. For details of this standard please contact CPNI.

Note that these standards and recommended levels within the standards are constantly being revised, as ever more powerful tools and blades arrive on the market and the perceived threats increase. Hence future proofing to a higher standard is always a good idea – particularly for a new build.

The Solution

The outer layers of secure fencing and detection should be still in place as a first line of defence.

For physical security of the building fabric you should choose or nominate a specialist company able to offer advice on security ratings. It is also important that the installation is carried out by a specialist company who understand the standard, their product and how to install it to meet the standard – including the protection of service entry points.

For new builds, the specialist company should work alongside the architects from early design stages, to ensure standards are met in the most efficient way. In many cases you may need different levels of security for different areas of the build. Hence choose a product that offers a range of levels that can be integrated to create a consistent appearance such as the **ModuSec System** from Remtech – see www.moduSec.com. This fire rated product has a similar appearance to standard 'whitewall'. However the core includes a range of anti-cutting materials to slow down any attack and tongue and groove joints are strengthened with mechanical locking.

LPS 1175 and Government CPNI ratings are available across a range of grades with a full design and build service for walls, ceilings, support steelwork, doors and protection grilles for service entry. Blast, ballistic and EMC protection options are also available.

The security rating needs to be chosen in relation to the impact level (IL) rating, the vulnerability of the site or façade and the potential response times of security personnel.

Note that if the build is carried out by a main contractor following on from a design and build tender, they may not offer an appropriate certified solution. The process often means that the cheapest solution is the one put forward to win the contract. Some traditional 'built up' solutions rely on the installation fixings being correctly carried out – which is not always the case. A certified modular factory made system with specialist installers overcomes this issue. The standard must be specified and controlled by the owner or end user.

Any additional cost of a certified security solution over the lifetime of the building is generally a fraction of the overall build, M & E fit out and hardware cost. This additional cost must be weighed against the criticality or value of your current or future data – to best ensure continuity of service and protection against ever increasing threats.

Mike Lawrence B.Sc (Hons) Civ Eng
Director of Remtech (Computer Security) Ltd.

For further information or advice
Call 020 8786 8787 or
email sales@remtech.com