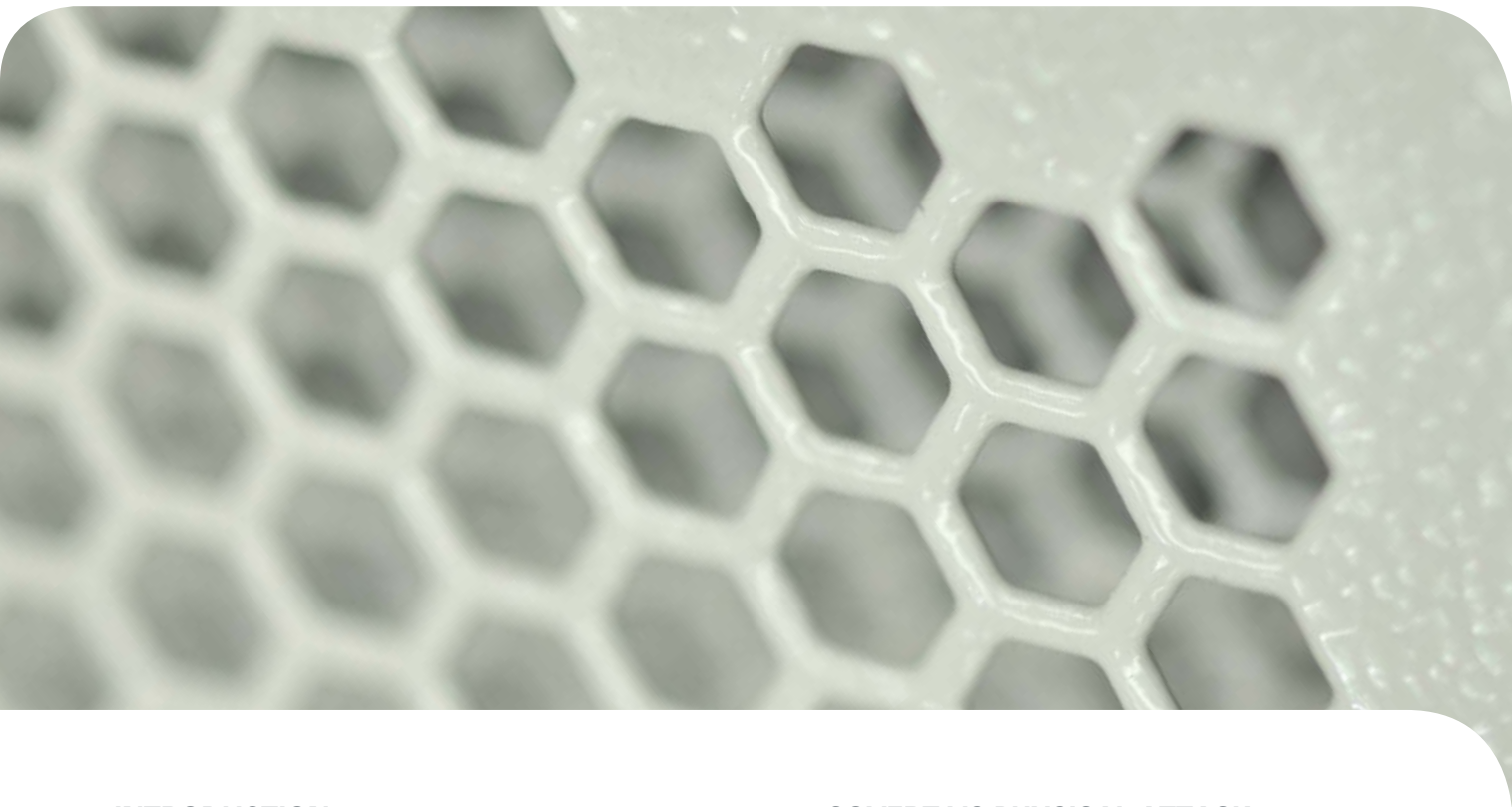


B&R Enclosures Pty Ltd
A guide to data cabinet security



INTRODUCTION

When ordering or designing a data cabinet, it is important to understand the different forms of security available, to ensure you get the most out of your cabinet.

Data cabinets are one of the last lines of protection for your equipment. With multiple levels of security in place in a data centre, the main security measures in a cabinet are to ensure any attempts at forced entry are visible. In contrast, in outdoor applications, a cabinet is often the first and only line of defence, and must be kept secure from physical attacks. In these different environments, very different security measures are required.

Security measures can range from the material the cabinet is made from, to the hinges and locks used on the doors. This article is a guide to cabinet security, explaining the merits and limits of different forms of security in certain applications.

COVERT VS PHYSICAL ATTACK

Throughout this article, we will be discussing whether cabinets are resistant to “covert” or “physical” attack. Individual cabinets in a data centre environment often do not require very high physical security. This is because they will already be protected by multiple layers of external security, such as restricted entry and general building security. Cabinets in these areas will require resistance to “covert” attacks. A cabinet resistant to covert attack will not necessarily be able to resist forced entry, however any attempts at entry will be clearly visible.

Data cabinets are also often required in areas with low additional security, such as by the road side, or associated with external equipment. In these applications, a cabinet must have high resistance to “physical” attacks, ensuring the impact of vandalism or forced entry are minimised.

DIFFERENT FORMS OF SECURITY

Cabinet frame

Material type and thickness of frames and panels has a significant effect on the level of security a cabinet provides.

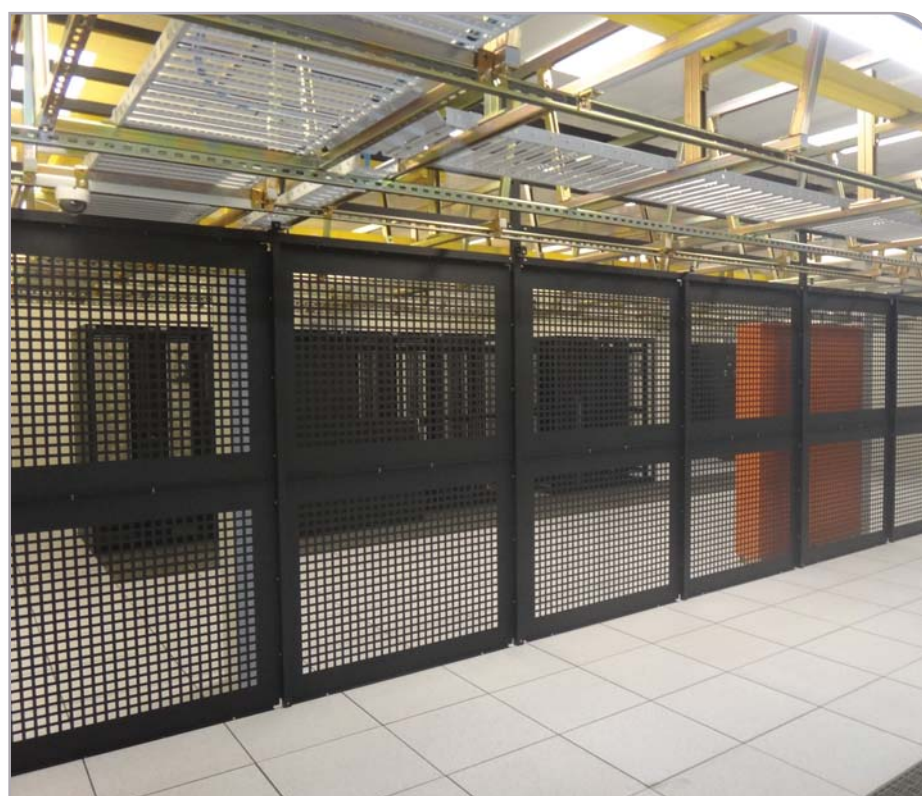
Two millimetre zinc coated steel, 2.5mm marine grade aluminium, or 1.5mm 316 stainless steel is recommended for cabinets in external applications. Samples of these thicknesses and material have been proven by B&R Enclosures to pass testing to IK07, equivalent to two joules impact, or an impact of 500g mass dropped from a height of 400mm.

For cabinets installed in data centres, the main priority is a high resistance to covert attacks. Therefore, while they are still manufactured from high quality materials, they will not be able to resist a significant physical attack.

In high security areas, such as government organisations, guidelines need to be met to ensure a cabinet can resist entry to intruders with varying levels of technical expertise. According to SCEC (Security Construction Equipment Committee), 1.6mm mild steel is required for these situations.

The quality of a cabinet's design can be tested through static, seismic and stiffness testing. These tests indicate how a cabinet will behave when subjected to various different weight loads. In particular, seismic testing offers an indication to the level of resistance a cabinet will have against someone attempting to disturb the cabinet by rocking or shaking it.

Cabinets requiring high physical security are also designed with internally secure cladding and panels. This ensures that any external panels can only be removed from the inside.



Security for data centres: Data Cages

Data cages are a useful layer of security in co-location environments where multiple tenants share a room. Data cages offer a physical barrier between equipment and people. To guarantee complete isolation, cages can also be installed beneath the floor, ensuring intruders are not able to enter through the raised floors common in data centres.


Doors

In general, mesh panel doors are the best option in data centre environments as they offer the security of a sealed cabinet, while still allowing air to flow through equipment. In high security government departments and agencies, cabinets with mesh panels of up to 40% open area are permitted. For standard applications, meshing with 63% open area is recommended, offering a balance between physical security and superior airflow.

Clear polycarbonate inserts offer equipment visibility while maintaining physical security for the cabinet. However, these doors restrict airflow and other measures should be taken to ensure equipment is kept cool.

For protection against physical attack, different measures are implemented. Cabinets in external environments will almost always require a high IP rating to protect from harsh weather. This means a plain, unvented door is mandatory, which increases the cabinet's resistance to physical attack.

Doors can also be fully recessed into the frame of the cabinet. Recessing the door so that it is flush with the frame ensures there are no points at which a tool could be used to lever the door ajar. This design is recommended in cabinets needing high resistance to physical attack.

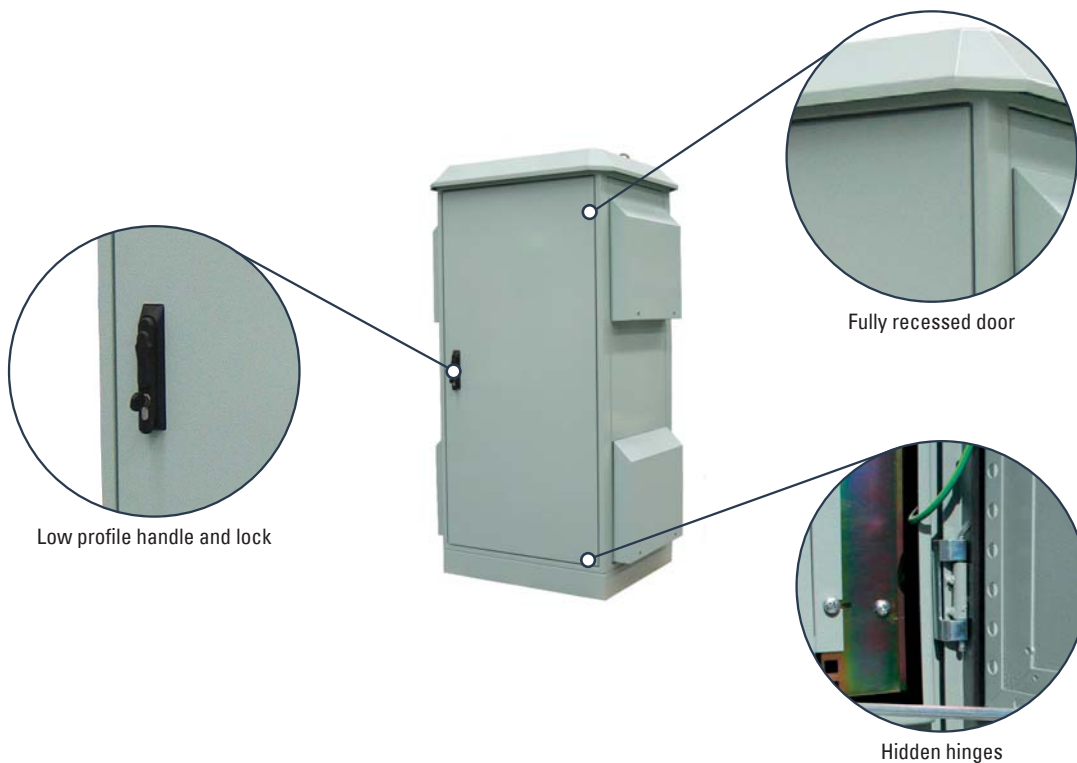


Read our paper on managing airflow in a data centre.

Hinges

Hidden hinges are a simple measure to improve physical security in a cabinet, as they decrease the risk of intruders bypassing the lock to gain access to a cabinet. To further enhance physical security, cabinets installed in areas with public access will typically be designed with concealed hinges and recessed doors.

SCEC approved cabinets require visible hinges to maintain their high resistance to covert attacks. To ensure these visible hinges do not cause a security hazard, additional features are included to prevent the door from being removed if the hinges are damaged.



Locks and handles

Lock type is a significant point of difference in determining the level of security a cabinet offers. As previously discussed, in data centre environments, the room the cabinets are installed in is the security seal. However, cabinets still require some form of lock to ensure only the intended user gains access.

For smaller cabinets, a single latch cam lock will be sufficient to keep the cabinet secure. Taller cabinets require two- or three-point locking. Two-point locking fixes the door in the top and bottom of the cabinet and is a standard level of security in a data centre environment. Three-point locks have an additional latch located at the door handle, and are recommended for heavier security applications. They are also required for external cabinets with high IP ratings, to ensure a tight seal is maintained around the door.

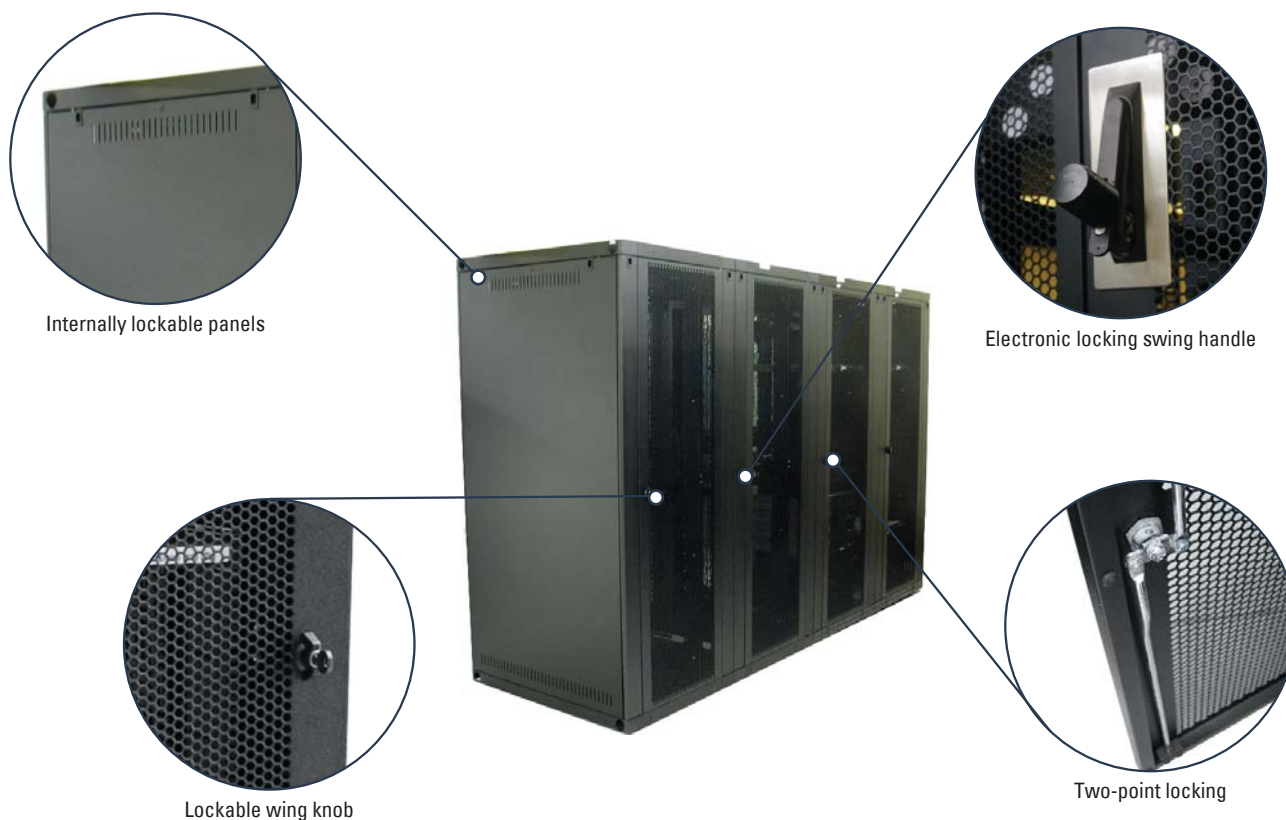
SCEC approved cabinets require specific locks according to their class. Class C cabinets are installed with three-point cam locks, where the Class B cabinets must have electronic combination locks.

Electronic locking is an additional layer of security for data centres. Electronic locks track the movement of personnel as they swipe through doors, increasing traceability throughout a centre. It can also monitor whether a door has been left open for longer than it should, and send out an alert accordingly.

Replacing keys with electronic swipe cards also ensures that losing keys is no longer an issue. With electronic locking, a swipe card can simply have its permissions removed, removing the risk of unauthorised personnel having access to data cabinets. Electronic locking is useful in environments where a wide range of personnel require access to a centre, as it offers peace of mind that any unauthorised action is easily traced.

Handles are another variable when considering the security of a cabinet. Basic wing-knob handles are appropriate for smaller cabinets, but larger cabinets with heavier doors – or with two- or three-point locks – require a T, L or swing handle that will offer better leverage and make the door easier to open.

For special application cabinets, B&R offer a low profile handle and lock. This lock has been designed to be vandal resistant by minimising the profile of the lock external to the door. This design makes it difficult to tamper with the lock, as there is a very small profile to work with.



RECOMMENDATIONS

The level of data cabinet security required varies greatly depending on the application and location of the cabinet.

For cabinets in a data centre environment, moderate physical security will suffice, but resistance to covert attack is a high priority.

For use in high security government departments and agencies, B&R's **CQr Guardian** offers high resistance to covert attacks. A SCEC approved product, CQr Guardian has been developed with a range of Class B and Class C cabinets suitable for secure network applications. Both classes of cabinets are fitted with three-point locking; Class B cabinets come with electronic combination locks, while Class C cabinets use Bi-lock technology.

The **Ausrack Plus** range is a cost effective solution for data centres. With a variety of options available, Ausrack Plus can be adapted to suit any level of security required. Available with two-point locking, Ausrack Plus offers a secure solution for your data centre.

For external applications, B&R's **Field FC** cabinet has been designed to minimise the effects of vandalism. The Field FC is manufactured using components which have been thoroughly tested to withstand impacts of up to two joules of energy. Fully recessed doors paired with three-point locking and low profile handles make the Field FC a great solution for outdoor data applications.





Head Office

51 Stradbroke Street Heathwood QLD 4110 Australia
PO Box 1151 Browns Plains BC QLD 4118 Australia
T: +61 7 3714 1000

QLD Office – Sales & Warehouse

51 Stradbroke Street Heathwood QLD 4110 Australia
PO Box 1151 Browns Plains BC QLD 4118 Australia
T: +61 7 3714 1111

North QLD Office – Sales & Warehouse

Unit 4 / 780 Ingham Road, Mount Louisa QLD 4814 Australia
PO Box 7615 Garbutt QLD 4815 Australia
T: +61 7 4727 1900

NSW & ACT Office – Sales & Warehouse

7 Metters Place, Wetherill Park NSW 2164 Australia
PO Box 90 Riverwood NSW 2210 Australia
T: +61 2 9915 9555

Newcastle – Distribution

Ross Joice Agencies Pty Ltd
109-111 Broadmeadow Road Broadmeadow NSW 2292 Australia
T: +61 2 4961 4433

Tasmania – Distribution

W P Martin Pty Ltd
85 Elizabeth Street Launceston TAS 7250 Australia
T: +61 3 6331 5525

VIC & TAS Office – Sales & Warehouse

50-52 Sunmore Close Heatherton VIC 3202 Australia
T: +61 3 9552 0552

SA & NT Office – Sales & Warehouse

505 Grand Junction Way Wingfield SA 5013 Australia
T: +61 8 8417 6222

WA Office – Sales & Warehouse

6 Montgomery Way Malaga WA 6090 Australia
T: +61 8 6310 4777

National Sales

T: 1300 Enclosures (1300 362 567)
F: 1300 796 599

E: sales@brenclosures.com.au

brenclosures.com.au

Disclaimer

This technical paper has been prepared specifically for customers of the publisher and as a general reference only. B&R Enclosures Pty Ltd engages in a policy of continuous development and improvement of its products and reserves the right to alter, add and/or delete specifications of any products or equipment without notice and without incurring liability. The publisher and any party associated with the production of this technical paper do not accept any responsibility or liability whatsoever (to the extent permitted by law) for any inaccuracy, error, misinformation or misleading statements, whether negligently caused or otherwise, contained in this publication. This publication is protected by copyright and may not be reproduced or copied (using any method of reproduction or copying), sold, transmitted, circulated or otherwise forwarded to third parties, in whole or part, without prior written consent of the author. All registered trademarks and product names appearing herein are the property of the respective owners.