One of the most important, but sometimes overlooked, areas of PCI compliance is the physical security of servers, storage, and network components. Rackmount Solutions offers a variety of cabinets for stores, hospitality locations, offices, and data centers that meet or exceed PCI Data Security Standards for physical security.

EXECUTIVE SUMMARY

Keeping cardholder information safe and secure is the key tenet behind the PCI Data Security Standard. Merchants and payment card processors must protect cardholder data wherever it is stored, processed or transmitted – in the data center, the network, the store, the hotel, the restaurant and at the point of sale.

A recent study by the Ponemon Institute found that 69 percent of all security breaches were due to malicious employees or non-malicious employee error. One of the best ways to protect cardholder data from internal threats is to ensure that all server, storage and networking components are physically secure.

PCI compliant enclosures from Rackmount Solutions can help eliminate physical threats to computing and network equipment due to acts by malicious employees/contractors or through employee error.

69% of all security breaches were due to malicious employees or simple employee error.
PCI – KEEPING CARDHOLDER INFORMATION SAFE AND SECURE

The PCI Data Security Standard is the framework that enables a safe, secure payment environment. Comprised of twelve requirements (and six goals), the standard is used by merchants and payment card processors to protect and secure cardholder data.

And although it’s specifically spelled out in the requirements, PCI compliance isn’t just for the data center. Stores, offices, hospitality locations, kiosks, and even mobile device software must be PCI compliant to participate in the secure payments environment.

THE BIG THREAT – INTERNAL SECURITY

When merchants and payment card processors think about threats to cardholder data (and PCI compliance), they usually focus on external threats – hackers, viruses and worms. However, a recent study by the Ponemon Institute and Vontu Inc. contained some surprising results.

Their survey of 163 companies (many of them Fortune 1000) revealed that of the companies reporting serious data security breaches, 69 percent were the result of either malicious employee activities or simple employee error. In fact, the leading cause of all reported security breaches was non-malicious employee error (39%). The survey also found that 27 percent of all breaches involved customer information.

Clearly, securing cardholder data from internal threats is of ever increasing importance. It’s not always about being hacked externally.

PHYSICAL ACCESS SECURITY – THWARTING THREATS FROM WITHIN

One of the simplest, and most effective, ways to prevent security breaches due to malicious internal activities or employee errors is to secure the physical access to all server, storage and networking components.

Enclosures with covers, panels and doors that are keyed or incorporate electronic locks can drastically reduce breaches due to malicious employees (or visiting vendors or contractors) as well as simple employee errors such as:

- Equipment reset or power down
- Inadvertent cable moves or disconnections
- Reconfiguration of incorrect components or cabinet contents

And, keyed covers, panels, and doors are necessary elements of an overall PCI compliance strategy that requires restricted physical access to cardholder data.

PCI DATA SECURITY STANDARD GOALS AND REQUIREMENTS.

BUILD AND MAINTAIN A SECURE NETWORK
1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

PROTECT CARDHOLDER DATA
3. Protect stored data
4. Encrypt transmission of cardholder data across open, public networks

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

IMPLEMENT STRONG ACCESS CONTROL MEASURES
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

REGULARLY MONITOR AND TEST NETWORKS
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

MAINTAIN AN INFORMATION SECURITY POLICY
12. Maintain a policy that addresses information security for all personnel
IPC COMPLIANT ENCLOSURES

Our Cruxial™ line of enclosures include options for keyed security covers, panels and doors, we also offer optional Emka® or Kaba® electronic locks for the doors.

RACKMOUNT SOLUTIONS –
WE KEEP THE THREAT OUTSIDE THE BOX

At Rackmount Solutions we offer some of the widest variety of PCI compliant enclosures in the industry. All of our enclosures include solid steel frame construction and durable steel and aluminum ventilation panels that keep threats out while still allowing computer equipment to properly ventilate.

Our Cruxial™ line is available in configurations from 14U to 48U and includes enclosures for:

Data Centers: The Cruxial™ RS and RSP series are available in over 864 configurations. They come standard with PCI compliant keyed doors, but can also be configured with Emka® or Kaba® electronic locks.

Co-Location or shared enclosure configurations: The Cruxial CoLoCab™ is designed to keep equipment from multiple departments or companies safely and securely separated within a single enclosure. It can be configured with 2, 3, or 4 locking doors as well as an optional vertical security panel for ganging more than one enclosure.

Office or non-air conditioned environments: The Cruxial Cooler™ is a PCI compliant enclosure that also includes its own air conditioning unit – along with keyed or optional electronic door locks.

We also offer PCI compliant wall mount, portable and desktop enclosures that all include keyed access to critical computer and networking equipment. Designed to meet the needs of stores, hospitality locations, and remote offices, our selection of wall mount and desktop enclosures includes:

Fixed configurations: Including the Linier™, SBX™ and SWR-8 Security™ lines.

Vertical configurations: The VRS/P series mounts servers and other components in a vertical position with two keyed access points to limit entry.

Swinging configurations: The DWR™ and Linier™ swinging wall mount enclosures provide easy access to equipment and cabling while locking securely after setup or reconfigurations.

Server side mount configurations: The GL24WE mounts servers sideways on the wall – and includes a keyed door.

Corner configurations: The KH 19-3-700-12 is a 12U enclosure that fits into the corner of a wall. It also includes keyed access doors.

Portable, table top configurations: Our TableRack™ series is available in 3U to 15U configurations and of course, come with keyed doors for access security.

Whether it’s a data center, store, hospitality location or office, Rackmount Solutions can provide a PCI compliant, economical enclosure that meets the unique needs of your electronic payments business.
KEEP CARDHOLDER DATA UNDER LOCK AND KEY

PCI COMPLIANT ENCLOSURES FROM RACKMOUNT SOLUTIONS

CONCLUSION

Merchant or card processor; data center, store, hospitality location or office; your company needs PCI compliant, keyed and electronically secured enclosures to protect cardholder data as it is processed and transported over the network. Rackmount Solutions has a wide variety of PCI compliant enclosures. From 42U and 44U full cabinet solutions to 3U portable table top configurations, our enclosures can help you simplify your PCI compliance strategy while ensuring that cardholder data is kept under lock and key.

Since 2001, our customers have known we are more than a supplier of parts and pieces. Our mission has always been to listen to our client’s specific needs and deliver high performance products through continuous product innovation and operational excellence. We are Focused on U™.

ISO 9001: 2008 CERTIFIED
› Measures and documents product quality, on-time deliveries and customer satisfaction.

INC 500|5000
› Recognized as one of the fastest growing private companies in America.

OUR GSA SCHEDULES ALLOW DIRECT CONTRACTING WITH GOVERNMENT AGENCIES & PRIME CONTRACTORS.

IT 70 - INFORMATION TECHNOLOGY #GS-35F-0208R 71 - OFFICE FURNITURE #GS28F-0011T 81 I B - SHIPPING/PACKING SUPPLIES #GS-02F-0214W

CALL 1-866-207-6631 FOR ASSISTANCE AND SPECIAL PRICING.

OUR PRODUCTS ARE MADE IN THE U.S.A. OF AMERICAN PROCESSED STEEL AND MEET ALL QUALIFICATIONS FOR THE BUY AMERICAN ACT & THE AMERICAN RECOVERY AND REINVESTMENT ACT

2805 E Plano Pkwy, #200 Plano, Texas 75074 MAIN 972 272 6631 FAX 972 276 6484 TOLL FREE 1 866 207 6631

DATACENTER/IT NETWORK/TELECOM INDUSTRIAL/ELECTRONIC MILITARY/AEROSPACE

© 2013 Rackmount Solutions, Inc. All Rights Reserved. Rackmount Solutions, Focused on U and Crucial are trademarks owned by Rackmount Solutions, Inc. All other trademarks are the property of their respective owners. Rackmount Solutions clients may make one attributed copy or slide of each figure contained herein.

Additional reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

WWW.RACKMOUNTSOLUTIONS.NET 4