

PROCESSOR

Cover Focus Articles

 [Click To Print](#)

General Information

March 28, 2008 • Vol.30 Issue 13

Page(s) 8 in print issue

Data Center Physical

Experts Weigh In With Tips For Maximizing Physical Data Center Security In The SME

Like a museum packed with fine art, data centers represent the ultimate score for cyber thieves. Yet while firewalls and other security software can help stop the ever-rising surge of Internet-borne threats, these tools are useless in the face of physical threats. While small and midsized enterprises continue to pour resources into server security, thieves using classic burglary techniques could be walking in the back door and helping themselves to gigabytes' worth of sensitive company information.



“All small to midsized businesses need to keep physical security in mind, no matter their industry,” says Craig Chambers, president and CEO of Cernium (www.cernium.com). “With thousands, if not millions, of dollars at risk in terms of personnel, equipment, and customer data, SMBs need to be aware of the risks facing them in the physical world and how to secure themselves against these threats.”

Interestingly, protecting data centers from physical threats follows roughly the same path as the process for protecting data: Buy tool, deploy tool. However, like moving into a new home and getting bombarded with calls from security vendors looking to outfit the house with an overkill security system, SMEs can easily fall prey to vendors looking to make a quick—and big—buck. As such, they'll need to carefully consider their situations and subsequent options.

■ Secure On All Fronts

Determining what physical security is needed, along with how much, can be a tricky proposition for a company of any size. Randy Scott, vice president of the critical infrastructure and data center group at Skyline Construction (www.skylineconst.com), says that the technology should depend on the level of protection required. For example, some companies might require audit capabilities that track personnel entering and exiting a room. Other companies might need CCTV (closed-circuit television) cameras to create a visual record of personnel activities or movements, while others in multitenant environments might need to pay particular attention to the placement and shielding of their security cabling.

“As a minimum, I believe that small to midsized data centers should have controlled access via biometric readers, swipe or proximity readers, etc.,” Scott says. “[These will] control critical areas to authorized personnel, provide an audit trail to identify any personnel entering the critical environment, and allow for denial of entry should an employee be terminated or leave the company.”

Certain procedures, such as background checks, can also boost physical security. Scott notes that employees can access a business' internal policies and procedures, financial information, and other sensitive information that's not available to the public. Additionally, they have access to critical equipment in a data center, such as UPSes, power distribution units, CRAC (computer room air-conditioning) units, backup generators,

automatic transfer switches, and emergency power-off buttons—all of which can bring down a power center. But background checks can help companies avoid potential hires with shady pasts.

■ Device Determination

According to Kris Domich, principal consultant for data center and storage solutions with Dimension Data (www.dimensiondata.com/na), companies should adopt the general practice of restricting access to the data center to only those employees who have a legitimate need for it. He also notes that they should focus on preventing both intentional and unintentional human interference.

“For example, organizations should protect sensitive information such as customer data or trade secrets—mitigating the potential for internal sabotage—as well as implement measures to protect against downtime events due to human error or negligence,” Domich says.

Physical security options span a range of devices, and each has a particular function that works best within certain environments and situations. One of these options is the motion sensor, which Domich says makes a good fit in areas that aren't constantly monitored but where the presence of personnel must be detected immediately. However, due to the potential for false alarm, Domich adds that these areas should be otherwise physically secure and behind a locked entrance.

Cameras are also useful in areas not regularly patrolled or manned, such as a remote, lights-out facility, Domich explains. “This is common at many disaster recovery sites. Customers that co-locate assets at an outsourcing provider often install IP-based cameras to monitor their equipment, as employees are not often at those locations. Cameras also provide audit trails when there is a need to trace back events, and they are often deployed in conjunction with motion sensors for that purpose.”

Data centers can also benefit from the use of audible alarms, which can deliver both notification and deterrence. However, Domich warns that while alarms might stop a break-in by bringing attention to the event, motivated intruders will have a “sense of time delta” between the alarm triggering and an actual reaction. Therefore, companies should carefully determine the entire process before deploying alarms, including the reaction time.

■ Protect The Ins & Outs

Domich says that the amount of physical security deployed should be proportionate to the potential threat itself and the consequence of not having security measures in place. At the minimum, he recommends implementing controlled, auditable access to the data center using a proximity card, fob reader, swipeable card, or a biometric device that can scan palms or fingerprints. The ultimate goal here, he says, is to require unique credentials for each person entering and leaving the data center. ■

by Christian Perry

Go With A Guard?

Cameras, motion detectors, and other devices are inherently useful in the battle against physical intrusions, but they all generally have one downfall: The reaction time to an actual event could be far too late to prevent a theft. However, certain environments demand instant reactions to potential intrusions, and for these, a human guard could be the answer.

Noel Rojas, senior vice president for security at Terremark (www.terremark.com), says Terremark's new facility in Virginia is being constructed to the highest federal security standards, which is important for commercial customers. In this instance, the company uses a layered approach that blends electronic monitoring

with a highly trained security force.

“Any company that handles critical applications that must be operational on a 24/7/365 basis should employ physical security guards that can protect the physical space in which these applications are housed and managed,” Rojas says. “Guards are costly but the most effective measure if deployed correctly. Guards can respond to an incident quicker than police and also serve as a deterrent to would-be criminals and individuals with bad intentions.”

Copyright © 2008 Sandhills Publishing Company U.S.A. All rights reserved.