3625 Alleghany Drive
Salem, VA 24153
1-800-675-7558
www.medeco.com

Server Room Security, Data Control, and Sarbanes-Oxley Compliance
July 15, 2008

By Jennifer Riley
Medeco High Security Locks

Server Room Security, Data Theft and Sarbanes-Oxley Compliance

Abstract

The Sarbanes-Oxley Act of 2002 (SarbOx) was established specifically to address financial reporting for public companies. The accounting data that is the foundation for this financial reporting is invariably electronic-based, and as a result, needs to be adequately protected and controlled, both for the corporation's benefit as well as to comply with SarbOx.

Individuals responsible for their organization's electronic data need to understand the level of protection their current security system provides, or doesn't provide, particularly in the area of server room access.

This paper will examine SarbOx requirements for controlling data, discuss the risks inherent in traditional server room security, and outline specific solutions to protect electronic data and maintain SarbOx compliance by controlling and tracking access to the organization's server room, and consequently, its data.

Introduction

Security systems that do not both restrict server room access *and* track who is physically accessing or attempting to access company server rooms place public corporations in potential violation of the Sarbanes-Oxley Act of 2002 and expose all corporations – public and private – to unnecessary data security risks and liabilities.

A recurring and central theme in both SarbOx and The Public Company Accounting (PCAOB) Oversight Board it established is that of internal controls as they relate to financial data. Since financial data in today's organizations is primarily electronic based, any discussion of internal controls has to include controlling access to electronic data.

Security systems that purport to protect electronic data by controlling server room access through a traditional lock and key system or type of electronic access do not adequately protect access to electronic data – indisputably one of an organization's most valuable assets.

Fortunately, new security product innovations are available that specifically control and track server room access.

SarbOx and PCAOB – A Brief Explanation

The Sarbanes-Oxley Act of 2002 was adopted "To improve quality and transparency in financial reporting and independent audits and accounting services for public companies, …… to increase corporate responsibility and the usefulness of corporate financial disclosure….and for other purposes."[1]

Section 302 of SarbOx addresses internal controls "and specifically, outlines several responsibilities for the company's signing officers related to establishing, evaluating and maintaining internal controls."[1] while Section 404 addresses "Management Assessment of Internal Controls"[1]

The PCAOB is a private sector, non-profit corporation established by SarbOx "to oversee the auditors of public companies in order to protect the interests of investors and further protect the public interest in the preparation of informative, fair and independent audit reports."[2]

PCAOB's Accounting Standard No. 5 places requirements that center on control on external auditors, including:

- Assess both the design and operating effectiveness of selected internal controls related to significant accounts and relevant assertions, in the context of material misstatement risks;
- Evaluate company-level (entity-level) controls;
- Evaluate controls designed to prevent or detect fraud, including management override of controls;
- Evaluate controls over the period-end financial reporting process;
- Evaluate controls over the safeguarding of assets; and
- Conclude on the adequacy of internal control over financial reporting.

Both SarbOx and PCAOB place significant emphasis on controlling and safeguarding data, and place the responsibility for ensuring that effective internal controls exist squarely on the shoulders of an organization's leadership.

These controls apply to corporation's processes and procedures for ensuring the validity of its financial reporting and most certainly to the physical control of and access to the data that serves as the foundation for that financial reporting.

Data Theft – A Real and Recurring Problem

Data is valuable, both to its owner as well as to individuals and organizations seeking to gain unauthorized access to the data through theft and manipulation, and needs to be protected.

The primary focus of data protection is often an electronic solution – firewalls, passwords, encryption, etc. – but just as important and sometimes overlooked is the physical protection of data and the equipment on which it is maintained, both from theft and unauthorized access. The corporate landscape is littered with painful and costly instances of data that was inadequately controlled or protected in server rooms, and as a result, exploited.

At the Midwest office of American Insurance Group (AIG), a thief broke in and stole a camcorder, and a computer server.[3] The value of the stolen hardware pales in comparison to the data contained on the server – personal information on nearly one million Americans.

In Chicago, police reported that thieves assualted a company security guard and stole 20 data servers worth $15,000.[4]

Verizon's Business Data Center in London lost more than $4 million in computer hardware when thieves impersonating policemen entered the facility and removed the equipment.[5]

In Indiana, 700,000 residents have their personal data at risk after a server and eight PCs were stolen from a debt collection company.[6]

"We live in a time where the information contained on a server is often more valuable than the server itself," says Martin McKeay in his column Security Matters at ComputerWorld.com. "A server can be easily replaced, the information not so much."[7]

The Need to Control Access – What the Experts Say

One of the first steps in protecting data, and controlling it per SarbOx, is to control the access to where said data is stored – server rooms. Because once unauthorized individuals gain access to the server room, the theft of data usually isn't far behind and oftentimes is easier to access than was entry to the server room itself.

"My point is that any savvy system wizard who can gain physical access to a computer can take that machine over in less than half an hour under most circumstances," says Ed Tittel, an expert contributor at SearchSecurity.com. "This helps to explain why physical security -- or

managing control over the space where systems and other key aspects of IT infrastructure reside in the real world -- is such an important component of a well-designed and well-executed security policy. If you don't maintain physical security in the real world, any and all safeguards you erect in the virtual world may be meaningless."[8]

Pete Sacco, a contributor at DataCenterDesign, a blog dedicated to the open exchange of ideas relating to the design of data centers and computer rooms, echoes other experts' recommendations for server room security. "Server room security begins with controlling access to your facility,"[9] Sacco says.

Bernie Klinder, a consultant with SearchWinComputing.com, echoed other experts' opinions in his post. "The final piece of the puzzle is securing your Windows server room," Klinder writes. "At a minimum, you must control and log access to the room via security cards, biometrics or other auditable methods."[10]

Controlling physical access to data and identifying attempts to gain unauthorized physical access to data should be a primary focus on any security plan whose goal is to protect an organization's assets and maintain compliance with specific SarbOx mandates.

Traditional Security Systems and Why They Are Inadequate

Tittel adds that for most small to mid-sized companies, security means things "like locked server rooms, additional authentication or access controls to operate administrator consoles and, possibly, some kind of monitoring system to track access and use of sensitive systems."[8]

Mechanical locks are often the first line of defense for companies attempting to protect their data and control access to server rooms, and understandably so. They're quick, easy, and inexpensive to install. There's a certain comfort level associated with this familiar security system used countless times daily to protect homes, vehicles, offices and other valuables. They don't require users to memorize access codes or carry electronic access cards, and traditional locks are, cosmetically, unobtrusive. Unfortunately, most locks are also woefully inadequate when it comes to protecting one of a corporation's most valuable assets.

The traditional lock and key system is a good solution in situations where there is only one person using the key, where tracking access isn't important, and where the need to add or delete keys from a system isn't a concern. But even this "one user, one key" situation, while fairly uncommon in today's business environment, is fraught with risk. What happens if the key is lost or stolen, or worse yet, copied without the owner's knowledge?

This risk, however, can be mitigated to a degree by using a high-security mechanical system. Often employing patented or otherwise restricted keys and locks that are extremely difficult to bypass, these high-security mechanical systems do offer a significant level of protection and control as compared to standard systems, albeit without an audit and tracking feature.

A traditional mechanical masterkey system, particularly one that isn't defined as high-security, simply doesn't offer enough protection, flexibility and data needed to control access to data and to provide tracking features that enable management to "assess and evaluate internal controls," per SarbOx.

When compared with other security options, traditional, non-high security mechanical masterkey systems come with other inherent risks and weaknesses, including:

- No ability to track who is accessing or attempting to access a door, how often, and when.
- No ability to quickly add or delete keys from a system when a key is lost, stolen, or an employee is no longer part of the organization.

- Unpatened or otherwise restricted keys can be copied and locks easily bypassed without leaving physical evidence to serve as an indicator of a security breach.
- Users need multiple keys to access different locks.

Electronic security systems that employ security cards, alpha-numeric codes or biometrics, provide heightened levels of protection when compared to a traditional mechanical masterkey systems but also bring with them a set of drawbacks separate from mechanical keys and locks, inluding:

- Expense to install, both from a time and materials standpoint.
- Installation locations dependent on the availability of power and network lines.
- Installation requires significant modifications to the door or frame, or both.

"Security cards, biometrics and other auditable methods are commonly used to limit who is able to gain entry into the server room, but these methods can only do so much," Tittel adds. "Security cards, keys or passwords can fall into the wrong hands, while biometrics devices are expensive and may accidentally keep out people who should have access."[8]

In certain environments, either a mechanical- or an electronic-based security system can be the appropriate solution to asset protection. Neither system by itself, however, is the right solution for securing and controlling data assests in today's complex environment of complying with SarbOx requirements.

Solutions

A viable, cost-effective solution to protecting data and fullfilling the control requirements outlined in SarbOx Sections 302 and 404 and PCAOB's Accounting Standard No. 5 lies in combining the best attributes and features of mechanical and electronic door locking systems.

Medeco High Security Locks designed and introduced Logic – a new electromechanical product line that consists of digital lock cylinders and digital keys – as an answer to security and access tracking needs by using the most desirable characteristics that both mechanical and electronic sytems offer.

Logic offers functionality similar to that of sophisticated electronic security systems, including audit trails, scheduling and the ability to add and delete users easily, but installs without any wiring, door or frame modifications or additional hardware.

Logic's digital cylinder and digital key look much like a traditional lock and key. The key is virtually indistinguishable from most car keys, with the exception of a small display screen, as is the cylinder. The difference lies in the digital technology contained in both the self-powered key and the cylinder, which is powered by the key.

Logic's digital cylinder retrofits into existing hardware, enabling the replacement of an existing cylinder and mechanical key with the electro-mechanical Logic cylinder in less than five minutes. This upgrade results in a stronger mechanical system, and the ability to both electronically audit access and change accessibility features, such as times and authorized users, quickly.

With Logic, any key can be programmed to work or not work on any cylinder, without being limited by a mechanical hierarchy like on a mechanical masterkeying system.

Knowing who is accessing or attempting to access data is a key element is demonstrating data control and in protecting data from theft. Logic systems allow up to 1,000 audit trails to be pulled from both the key and the cylinder, showing who is entering the protected area, how often, and when, thanks to time and date stamps. This data enables administrators to regularly evaluate and assert that the internal controls are operating efficiently, and helps companies comply with key SarbOx requirements related to internal controls and effectiveness.

Lost keys can simply be electronically deleted from the system to maintain security. And, any time a new user key is needed, it can be quickly and easily added.

Additionally, unauthorized key copying is removed from the equation because replacement keys are cut and issued only by the Medeco factory and because of the patented electronic technology in Medeco keys – two features that, combined, offer superior protection against unauthorized key copying.

Instant rekeying is another Logic benefit as keys and cylinders can be instantly and easily deactivated or reprogrammed with different access permissions or schedules, either by Medeco dealers or by end-users who choose to self manage their systems with an optional programming device and software.

While Logic's auditing and tracking features that show who is accessing or attempting to access a server room and its technology that prevents unauthorized access are compelling by themselves, the installation benefits shouldn't be overlooked.

Traditional electronic security systems, including card readers, biometric systems, or keypads, usually require electricity in order to operate, and if the system is being installed as a retrofit, significant installation expense in both time and materials. Logic cylinders simply retrofit existing mechanical cylinders and leverage the use of existing door hardware without any door or hardware modifications. No electricity, hardwiring, phone, or Internet connection is necessary. And, unlike many stand-alone systems, Logic cylinders blend discretely into existing hardware and architectural designs and are available in most common architectural finishes.

Logic provides a straightforward, cost-effective security solution where a mechanical masterkey system simply doesn't offer enough flexibility to keep up with businesses' ever-increasing demands, and the ever-changing methods individuals are employing to gain unauthorized access to data.

Logic offers strong physical security with the flexibility of schedules, audit trails, the ability to easily add and delete user keys, and unlike electronic systems, a retrofit cylinder that blends unobtrusively into existing hardware.

Conclusion

In today's business environment, data security isn't a question of whether protection is needed but rather what type of protection is the best choice. The added complexities of ensuring compliance with SarbOx, specifically sections 302 and 404 addressing control, make that security decision even murkier.

Industry experts agree that any data protection plan has to begin with securing, controlling, and evaluating access to the data's home – the server room. Both mechanical and electronics-only locking systems have their limitations when it comes to securing server rooms and providing the data and control needed to comply with SarbOx.

A viable, cost-effect solution to server room protection and SarbOx data control requirments is a security system that combines the best attributes of both the mechanical and electronic systems.

- 0 -

For more information, please contact Joseph Kingma, Director of Business Development at Medeco High Security Locks: 1-800-675-7558 ext. 1683 or jkingma@medeco.com

References

[1.] Sarbanes-Oxley Act of 2002, November 2, 2002, www.sarbanes-oxley.com

[2.] Public Company Accounting Oversight Board. 2003-2008, www.pcaobus.com

[3.] MSNBC, "Stolen Computer Server Sparks ID Theft Fears," By Jim Pompkin and Tim Sandler, June 14, 2006, http://www.msnbc.msn.com/id/13327187/

[4.] Data Center Knowledge, "Armed Robbery at Chicago Data Center," November 4, 2007, http://www.datacenterknowledge.com/archives/2007/Nov/04/armed_robbery_at_chicago_data_center.html

[5.] Data Center Knowledge, "'Ocean's 11' Data Center Robbery in London," December 8, 2007, http://www.datacenterknowledge.com/archives/2007/Dec/08/oceans_11_data_center_robbery_in_london.html

[6.] Dark Reading, "Server Theft Exposes Data on 700,000 Consumers," By Tim Wilson, Site Editor, April 21,2008, http://www.darkreading.com/document.asp?doc_id=151557

[7.] Computerworld Magazine, "Targeting the Servers," By Martin McKeay, June 20, 2006, http://blogs.computerworld.com/node/2801

[8.] Searchsecurity.com, "Policy for the Real World: Physical Security," By Ed Tittel, April 1, 2003, http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci891293,00.html#

[9.] Data Center Design, "Server Room Security Measures," By Pete Sacco, January 26, 2007, http://datacenterdesign.blogspot.com/2007/01/server-room-security-measures.html

[10.] Searchwincomputing.com, "How to Secure Your Windows Server Room," By Bernie Klinder, February 8, 2005, http://searchwincomputing.techtarget.com/news/article/0,289142,sid68_gci1046221,00.html