Sarbanes-Oxley Act:

Remote Control Software for a Compliant IT Infrastructure

The Sarbanes Oxley Act (SOX) has put stringent regulations on the corporate governance of publicly traded companies to ensure the protection and validation of all financial data. As a result, corporate IT departments are turning to more secure products for network maintenance and end user support. The following white paper identifies potential security threats created by remote control software and provides a solution for compliant, secure remote access to end user machines.

Contents

CrossTec Corporation
500 NE Spanish River Blvd.
Boca Raton, FL 33431
800-675-0729
www.CrossTecCorp.com

Sarbanes-Oxley Act:
Remote Control Software for a Compliant IT Infrastructure

In November of 2001, Enron shocked the investment world with the announcement of the largest financial swindle in American history, a betrayal that created a considerable lack of trust and confidence in corporate governance. In response, the Federal Government signed the Sarbanes-Oxley Act (SOX) into law to protect corporations and valuable information used in every day business practices, ensuring the fiscal integrity of public organizations by holding them legally responsible for the accuracy of their financial reports. SOX requirements have forever changed the auditing practices and financial reporting procedures for thousands of corporations nationwide and quickly developed the need for properly secured IT infrastructures.

1. Information Security

Corporate IT departments have been forced to make considerable changes in their accounting practices to comply with SOX rules and regulations. If a problem arises, individual computers and servers on the network are frequently shut down until an IT specialist can address the problem. For instance, when an accountant requests technical support, an IT employee must go to their computer and resolve any technical issues.

Thousands of IT departments utilize remote control software to simplify this process. Remote control technology enables IT employees to access and fix problems anywhere on the network. This eliminates additional travel time, costly labor expenses, and downtime to the user or user group.

2. Corporate Responsibility

One intrusion from a hacker could result in the corruption or deletion of crucial financial records that are necessary for accurately submitting financial and operating reports, further costing the corporation time, energy, and severe penalties. SOX regulations and potential repercussions are compelling reasons for corporate executives to take all the necessary precautions to maintain a SOX compliant network infrastructure.

The SOX Act clearly describes the personal liability of corporate executives of publicly traded companies for the accuracy of financial reports. Under Section 302, it is required that every quarterly and annual financial report submitted to the SEC is personally reviewed and certified by the CEO and CFO. By holding the executive accountable for the actions of the entire organization, SOX demands an accurate account of the company's current and predicted financial status as well as the integrity of reporting true numbers.

Additionally, Section 302 mandates that internal audits of all financial procedures be conducted annually. Inaccurate financial reporting due to a network intrusion or internal mishap may result in fines to the CEO/CFO of as much as $5 million and/or jail sentences up to twenty years.

3. SOX Compliant Network Infrastructure

In 2004 the Conference Board Commission on Public Trust and Private Enterprise stated that the effective internal control systems should encompass all major areas of risk and vulnerability to operate a company. According to Section 404, all internal controls must be documented, reviewed, validated, and tested to ensure complete effectiveness.

The corporate network stores a warehouse of knowledge necessary to the business continuity of an organization. However, most immediate vulnerabilities are usually found on private networks, such as working from home or using a laptop while traveling. It is imperative that system administrators utilize secure technologies that protect virtually all electronic communication in the corporate structures of today.

4. Remote Control Compliancy

SOX regulations demand strong remote control solutions that protect the transmission of corporate financial data. However, if the remote control application lacks the proper security, points of entry can create holes in the company network, making the application vulnerable to hacker attacks and inconsistent with SOX regulations.

There are two modules that must be present in order to remote control the desktop of a remote computer: a Control and a Client. The Crosstec Control is the administrative computer and the Crosstec Client enables the Crosstec Control to establish the connection and control the Client desktop once a connection has been established. In order for a Crosstec Control to remotely access and control a Client computer, streams of information must be exchanged between the two machines. Therefore, an extremely secure remote control application is needed to protect network access and prevent hackers from intercepting data streams or confidential information.

5. SOX Compliant Security

Remote Control software can be an ideal utility for any organization, but it must conform to SOX regulations. CrossTec provides the security necessary because every connection is authenticated, encrypted, and logged.

Once the system administrator has assigned who can remote control the clients using Active Directory (AD) or basic NT authentication, every time a remote connection is attempted, the Control logging in can be identified by their AD account. Another useful feature of a Remote Control Client is event logging. Every Client should have the ability to log, to the Windows Event Log or a network location, any activity done to the Client machine during a remote session. In the event of an intrusion by a hacker, or just for general auditing purposes, it is important that these logs be accurate and easy to understand. If an unrecognized or outside Control attempts to make a connection to a Client machine, the Client will automatically prevent them from establishing a connection and log the event accordingly.

The CrossTec Client also enables an administrator to restrict Remote Control access to a client. By creating Profiles on the Client machines and associating these Profiles to AD Groups it becomes easy to create multiple sets of permissions depending on which Windows AD Group member is controlling the Client. This allows an administrator to assign remote control permissions for the Help Desk group that are lower than those of the Domain Admins group when connecting to the same Client for example. Also a supervisor that is only using the software to monitor employee actions may have a specific set of privileges that do not include inventory or actual remote control.

For additional authentication and connection restriction options, CrossTec customers may use connection password, which embeds a unique password into the purchased software license group. Therefore, any attempt to connect from an outside Control application that lacks the unique embedded password will be automatically rejected by the Client. This prevents terminated employees with the knowledge of administrative passwords from gaining entry to the network..

6. Encryption

Strong Encryption is needed when transferring data between two machines as it converts the data to an incomprehensible form, and CrossTec Remote Control provides the highest level of encryption. Every connection is protected with the government standard 256-bit AES encryption, the fastest and most secure means of transferring data available. System administrators can finally rest assured that all corporate data remains confidential and the company does not suffer Federal penalties. With CrossTec Remote Control, system operation and maintenance is dramatically simplified because it enables immediate response from a centralized location.

Top-of-the-line encryption from CrossTec ensures security from any location. Every remote session is authenticated and has the option of being encrypted with encryption standards ranging from 56bit DES to 256bit AES encryption. The software performs thorough logging of every remote control action.

7. Additional SOX Requirements

The majority of the regulations set forth by SOX protect the access and use of financial databases and information. However, there are a variety of procedural requirements that pertain to the validation of information. Under SOX, public organizations must meet additional requirements, including:

- System Operation and Maintenance
- Data Integrity
- Conduct Audits
- Record and Report Transactions

According to SOX, corporations should be able to provide 'real time' financial reports that are consistent with the company's current economic condition. CrossTec facilitates this need with its Recording feature, allowing an administrator to record the desktop of a Client machine. By simply viewing the recording, all financial information is clearly displayed on the desktop in a summarized format. Each connection is logged to the Windows Event Log in easy to understand messages. If aggregating these logs into Security Information Management tool administrators spend less time figuring out what the events mean and more time identifying events of interest on the network such as unnecessary connections, intrusions, or vulnerabilities on the network.

8. Summary

The Sarbanes Oxley Act of 2002 helps restore public faith in the U.S. stock market and public trust in corporate governance. However, SOX simply assigns fiscal responsibility to public organizations. Public organizations now face the challenge of constructing a secure network environment where information is internally shared without the fear of external threats. By providing adequate information security the company network is protected and data integrity is maintained. CrossTec Remote Control is the secure remote access solution that doesn't generate back doors for would-be attackers, protecting all information, whether financially related or not. CEOs, CFOs, and accountants whose corporations are using CrossTec can relax with the knowledge that their network is protected by industry-leading remote control security.

CrossTec Corporation
500 NE Spanish River Blvd.
Boca Raton, FL 33431
800-675-0729
www.CrossTecCorp.com