

www.securecomputing.com

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years. We help our customers create trusted environments both inside and outside their organizations.



Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters

East Wing, Piper House
Hatch Lane
Windsor SL4 3QP UK
Tel +44.1753.410900
Fax +44.1753.410901

Asia/Pac Headquarters

1604-5 MLC Tower
248 Queen's East Road
Wan Chai Hong Kong
Tel +852.2520.2422
Fax +852.2587.1333

Japan Headquarters

Level 15 JT Bldg.
2-2-1 Toranoman Minato-Ku
Tokyo 105-0001 Japan
Tel +81.3.5114.8224
Fax +81.3.5114.8226

© February 2005 Secure Computing Corporation. All Rights Reserved.
SW-SDX-TP-Ap0501v2. Secure Computing, SafeWord, SideWinder, SmartFilter, Type Enforcement, SafeToken, SecureSupport, SecureOS, MobilePass, G2 Firewall, Base, SideWinder G2, enterprise strong, PremierAccess, and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, Application Defender, RemoteAccess, On-Box Power-it-On!, Sentinel, and Securing connections between people, applications, and networks are trademarks of Secure Computing Corporation. All other trademarks used herein belong to their respective owners.

Sarbanes-Oxley compliance and strong authentication

SafeWord PremierAccess provides compliance assistance

Table of contents

Overview 2

Section 404 and Internal controls 2

Deadlines and spending 3

Financial data at risk of compromise 3

Strong authentication and Sarbanes-Oxley 3

Cost-effective strong authentication solutions 4

Recommendations: Access controls and how SafeWord can help 4

More ways SafeWord products provide Sarbanes-Oxley compliance assistance 5

 Giving the right authorization to the right people 5

 The inherent risks—and annoyances—of passwords 6

 Remote access is a way of corporate life 6

Overview of the different advantages of SafeWord PremierAccess and Safeword RemoteAccess 6

What are the penalties for not complying with Sarbanes-Oxley regulations? 7

Conclusion and our own Sarbanes-Oxley compliance efforts 7

Overview

The Sarbanes-Oxley Act of 2002 was passed by Congress as a response to corporate accounting scandals, as a way to restore America's confidence in the corporate world, and to make top-level executives accountable for what goes into the company's financial statements. It's a clear mandate: America will not tolerate corporate financial data being fudged. But beyond that, it means that CEOs are now personally accountable for their companies' financials. They have an obligation to ensure that financial statements are accurate and truthful before they sign off on them. Now more than ever, corporations must take precautions against tampering with the financials—tampering on the part of corporate executives, employees, outsiders, and attackers. C-level executives now bear responsibility for ensuring these occurrences do not happen on their watches and the prevention of even an unintentional inaccuracy must be ensured. Compliance also means operating with integrity, adhering to a set of standards and best practices, and implementing good security.

Smart corporations have already made it a policy to protect their financial data as policy, but Sarbanes-Oxley has raised the bar considerably by requiring proof of controls and security. For many, the process has been daunting—either because of the challenges of implementing new technology, or unplanned expenses, or both. By this time, many organizations have already had to comply with the regulations required for 2004 annual reporting. But that's not nearly the end of the story...compliance is an annual endeavor, and many companies now seek to improve their processes or at least reduce their expenses associated with the new processes.

Sarbanes-Oxley addresses many different areas, not all of which pertain to IT controls. For the purposes of this report, Sections 302 and 404 offer the most guidance in terms of implementing technological measures towards compliance. Section 302 outlines management requirements with regard to companies' 10Qs and 10Ks; and Section 404 takes it further by mandating internal controls designed to prevent accounting mismanagement in 10Ks.

Section 404 and Internal controls

Implementing the requirements of Sarbanes-Oxley's Section 404, the SEC now requires every company's annual report to contain "a statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting," and secondly, "management's assessment . . . of the effectiveness of the company's internal control structure and

procedures for financial reporting." If an organization has one or more material weaknesses relating to controls and their effectiveness, this must be disclosed in the organization's annual report. Section 404, and the internal controls to which it refers, is only a part of Sarbanes-Oxley, but it is a very important part, and one that requires attention to the IT security measures that underlie the organization's entire technological infrastructure.

Section 404, unlike some other federal regulations, does not specifically set out technological requirements. Nonetheless, strong authentication technology will necessarily play a major role in achieving compliance. The integrity of a company's financial data must be protected at all costs; this means above all, securing access to that data.

Sarbanes-Oxley of course, goes beyond basic "accounting internal controls." It is a far-reaching piece of legislation, calling for strict and verifiable adherence to generally acceptable accounting procedures at all levels; and much of that goes beyond the purview of the security manager. The "internal controls" referred to by Sarbanes-Oxley are not explicitly defined. However, the fact that financial data and reporting is dependent on electronic information and IT systems, means that technological controls must be used to ensure the security of that information.

Clearly, sensitive information needs to be safeguarded and access to it needs to be restricted to users who have clearance to view it and to modify it. Procedures must be in place that detail how certain process are to be executed, and these processes need to be approved by managers which ensures that they can be sure their staff is performing tasks in accordance with the proper procedures. This is also vital for the audit trail required by Sarbanes-Oxley so companies can keep a reliable and accurate log of activity (paper and/or electronic as applicable) in real time. Additionally, these controls over financial reporting need to be audited at least annually to verify the effectiveness of the controls, and for certification in companies' annual SEC filings. Moreover, the controls need to be monitored to identify any significant changes or deficiencies of the controls that need to be disclosed on a quarterly basis. Strong authentication is a highly effective network security control that prevents unauthorized access to financial data, which can assist with compliance of the one of many controls tested for SOX purposes. We will discuss this further below.

Deadlines and spending

For publicly held companies that have a market cap of \$75 million or more, the first deadline for compliance has already passed, based on fiscal years ending on or after November 15, 2004. Companies with calendar fiscal years will include Section 404 reporting in their annual reports filed in early 2005. Companies with market caps of under \$75 million have some additional time, having just received another extension in March of 2005 (at the time of this paper, the date has been extended from July 15, 2005 to July 15, 2006.).

But just because those larger companies have already passed the compliance deadline doesn't mean the war is over; they have merely passed the first hurdle. As noted above, Sarbanes-Oxley requires an *annual* certification of compliance. As a result, after the first year of initial implementation, companies will have to move their focus to ongoing compliance and maintenance of internal controls. During the first year of any new government regulation, there is the inevitable rush to comply, and some natural complexity and confusion. After the first year however, the focus can switch to refining the process of compliance, and reducing ongoing costs. In 2004, it is estimated that a total of \$5.5 billion was spent by corporations on Sarbanes-Oxley compliance; in 2005, that figure is expected to rise to \$5.8 billion, as smaller companies meet their first compliance deadline, and larger companies continue to refine their compliance procedures (Source: AMR Research, www.amrresearch.com). While it doesn't represent the majority of the Sarbanes-Oxley spending budget, technology spending is currently the fastest growing segment. Technology provides the necessary support for organizations in the areas of securing data, ensuring correctness, and managing applications, processes, and related information.

Financial data at risk of compromise

A corporation's financial data is often the "crown jewels" sought after by certain types of attackers or hackers, who, for whatever reason, may seek to gain inside information, steal or manipulate data, or influence the performance of a stock. They may seek to do so through trickery, electronic manipulation, and a variety of standard hacker tricks like keyboard logging, sniffing, and password attacks; they may try social engineering techniques to try to bluff

passwords out of unsuspecting employees; and they may even resort to outright thievery by rifling through an employee's desk when they're not looking. Should any of these breaches occur, officers may face strict penalties; even if they were unaware of a breach or false statement, not to mention the possibility of other negative ramifications all companies of course wish to avoid. Fortunately, there are steps that can be taken to prevent all of these types of attacks. The next sections describe some effective and reliable preventative measures.

Strong authentication and Sarbanes-Oxley

The internal controls called for by Sarbanes-Oxley cover many aspects of financial reporting, as well as security technology surrounding financial reporting. Part of the internal controls includes computer-related controls that implement information security that safeguards the integrity of financial data.

Although Sarbanes-Oxley itself does not have specific details on the technology of internal controls, the Public Company Accounting Oversight Board (PCAOB), part of the SEC that oversees implementation of, and compliance with Sarbanes-Oxley, has issued and approved the Auditing Standard No. 2, "An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements", which offers more detail on Sarbanes-Oxley's Section 404. Specifically, this document establishes a recommended framework for evaluating IT controls, called "Control Objectives for Information Technology" (COBIT).

Although there is no direct COBIT certification process, your technology solution, particularly with respect to security and strong authentication, should track closely with the controls outlined in COBIT. The PCAOB specifically calls for the auditor to examine IT procedures and controls, and the extent to which information technology is used in each financial reporting process. The document further lays out procedures with respect to IT controls which are commonly a function of IT security software, such as strong authentication systems. Specifically, the PCAOB document states that an entity can protect its data and program integrity by preventing unauthorized use of the system; and that there should be frequent reviews of user profiles that govern access. Some of the common elements specifically outlined that may pertain to strong authentication include role-based user management, real-time reporting, and validation.

Role-based user management, an integral part of SafeWord®, makes it possible to refine and maintain access controls within a large organization, granting individuals access to specific areas of the network based on the role or roles each individual may have. Each individual's access can be fine-tuned, as each person can have multiple roles that can easily be updated and changed by the administrator as needs arise.

Specific security protocols are not outlined in Sarbanes-Oxley, but the need for strong authentication as a means of compliance is evident. You can't run a tight ship without it.

Cost-effective strong authentication solutions

Using SafeWord® PremierAccess® or SafeWord® RemoteAccess™ for strong authentication as one piece of the Sarbanes-Oxley puzzle won't be something that costs an ongoing fortune. SafeWord products offer cost savings and a lower total cost of ownership in a variety of ways.

For instance, most authentication systems use an authentication device such as a token that generates secure, one-time passcodes to identify users. While competitive offerings require customers to repurchase tokens every few years (their tokens are programmed to expire in three years), SafeWord tokens do not expire. This means that with SafeWord, the cost of replacing tokens over the years is greatly reduced and in some cases, eliminated altogether (more details on this below). Additionally, SafeWord's user self-enrollment features keeps the initial deployment costs down to a minimum compared with other authentication solutions that have high administrative overhead. Manageability and integration with Active Directory also helps keep administrative overhead down. And yet another area of costs savings is SafeWord's ability to scale to unlimited numbers—meaning that you won't have to upgrade as your organization grows; you can simply add more tokens if and when the need arises. SafeWord solutions ensure that access to financial data is tightly controlled and that the user identification end of it is cost-effective.

Compliance with Sarbanes-Oxley involves not only up-front expenses, but ongoing expenses as compliance must be met annually. SafeWord PremierAccess and SafeWord RemoteAccess solutions, provide both the most cost-effective and the most secure authentication system on the market. (For some differences between these two solutions, see page 6.) SafeWord tokens offer significant savings over time within the help desk arena, because they

are *event-synchronized*. Competing authentication systems are time-synchronized; which means that they contain an internal clock, and the time is sent along with the user's secret key to the server. These competing devices are inevitably subject to clock drift over time, and eventually get out of sync with the server—which results in desperate help desk calls from users who cannot get onto their networks. In contrast, SafeWord's event-synchronized tokens have an event counter (with the *event* being the number of times the button on the token has been pushed). The server also keeps the same count. The counter number (which is *not* subject to drift) is sent with the user's secret key, and then SafeWord's algorithm creates and displays the one-time passcode.

Also, as noted above, while some competing tokens are pre-programmed to expire after three years (planned obsolescence that forces repurchasing), SafeWord PremierAccess tokens never expire, and batteries last an average of five years. SafeWord RemoteAccess tokens under maintenance contracts are *always* replaceable at no charge, regardless of the reason for replacement. This makes SafeWord a solution that is much less costly over time.

In addition, user acceptance is always high with SafeWord. Needless to say, no matter how good the solution, if it is too difficult for the average user, acceptance is a struggle. Companies switching from competing solutions to SafeWord have repeatedly reported great user satisfaction, widespread acceptance, and easy and seamless switch-overs.

Recommendations: Access controls and how SafeWord can help

It was never the intent of the SEC to outline a specific set of security requirements; that body wisely leaves the specific details up to each company, and to the security industry itself, to sort out. The end results are what matter. Do you know who is accessing your company's financial data? Are there security protocols in place to ensure that those who access that data are authorized to do so? Have you taken steps to ensure that unauthorized employees, attackers, and criminals cannot access that data? Sarbanes-Oxley calls for corporations to verify that these steps have occurred. In terms of implementing the necessary access controls, security experts recommend several technological steps be taken (again, with the caveat being understood that no single product can claim to be Sarbanes-Oxley "compliant," since there are no specific technological mandates).

1. The implications of Sarbanes-Oxley call for strict access controls. A technological solution that implements unbreakable security, such as two-factor authentication and single-use passcodes, accomplishes this need. SafeWord products from Secure Computing® overcome the limitations and eliminate the risks of memorized passwords, by providing a one-time-only passcode. Because the passcode is used only once, even if an attacker could sniff, steal, or shoulder-surf this passcode, it would be useless to them—and financial data remains protected.
2. Sarbanes-Oxley clearly intends for there to be an audit trail. In regards to access, this means providing an electronic record of who has access to what records; and further, providing a record of any attempts at unauthorized access. The SafeWord PremierAccess reporting system gives managers an easy view into the system's management, timely reports, and a simple way to make adds and changes as needed. Current reports can be generated periodically or on demand, reflecting any changes that have been made to access procedures. Roles often change within a corporation, individuals may require temporary access to financial records, and people come and go. Thorough documentation of these events helps to achieve compliance with Sarbanes-Oxley. With SafeWord RemoteAccess, auditing capabilities are available through Active Directory.
3. Role-based access plays a major part in Sarbanes-Oxley compliance. The principle of "least access" or "separation of duties" is a standard best practice for all companies, whether they are subject to Sarbanes-Oxley or not; and in the case of Sarbanes-Oxley compliance, part of the annual certification is to show that these sorts of checks and balances are in place. For example, it is necessary to show which individuals in which roles have access to financial data. The role-based authorization provided by PremierAccess can help to ensure that each individual has access to only that which is necessary for the completion of his or her job. With SafeWord RemoteAccess, authorization capabilities are available through Active Directory.
4. Managing multiple access points from a single location is a practical necessity when trying to comply with Sarbanes-Oxley. Larger enterprises often allow users to access the system through a variety of means, including remote dialup, Citrix® connections, VPNs, or a variety of other

connectivity methods. Connections may come from branch offices, traveling employees, partners, clients, or outsourcing centers. SafeWord PremierAccess provides a reliable way to meet compliance throughout the enterprise, and to ensure that proper authentication protocols are being followed regardless of access method. PremierAccess' ability to work with multiple access methods, as well as its single sign-on convenience, means that strong authentication is uniformly applied across the board—regardless of how, or from where, any individual connects to the system. PremierAccess also supports virtually every type of authentication device—from tokens to certificates to smart cards and biometrics. You have tremendous amount of flexibility in determining which methods to use to authenticate your users.

More ways SafeWord products provide Sarbanes-Oxley compliance assistance

Giving the right authorization to the right people

Even if every single one of the top-level executives is scrupulously honest, a company can still fall out of compliance due to third-party attack. While PremierAccess can't turn a crook into an honest person, it can keep those who would do harm away from vital financial information.

It should be noted that because Sarbanes-Oxley does not lay out specific security protocols, no security product can lay claim to being "Sarbanes-Oxley compliant." Rather, it's up to the security officer to determine best practices, and to implement proven technology to ensure that the corporation's financial data remains intact—and to ensure that a strong system of technological controls are in place to ensure that only authorized persons are able to access the financial data. As noted above, role-based authorization ensures that a policy of "least access" is applied uniformly—so each person has access to what they need, but *only* what they need and nothing more. The process of identity management involves managing multiple users in different roles, both within and outside of the organization; provisioning user privileges, and reporting on who has access to what, in compliance with internal policy. Part of establishing internal controls is determining who has access. SafeWord PremierAccess provides a solid solution.

The inherent risks—and annoyances —of passwords

A company typically allows access to many third-party individuals and companies, including partners, financial institutions, and clearing houses. This is necessary for carrying out day-to-day business. But simple memorized passwords are inadequate. Access to this important data must be protected with strong, two-factor authentication. It is not likely that an auditor is going to approve of a system that protects financial data with simple, memorized passwords, especially passwords that can be easily guessed.

But that is where companies using memorized passwords face a dilemma. When using passwords, experts recommend using at least eight characters with a combination of letters and numbers; which cannot be easily guessed. Passwords should not be tied to anybody's birthdate, personal information, spouse's name, or anything else that an attacker might be able to derive. But the problem then becomes that these types of passwords are not easy to remember. Employees are likely to circumvent the security by writing them down—opening up the possibility that an attacker could gain access to the system simply by rifling through a desk drawer to find slips of paper with strange series of letters and numbers on them. Alternately, employees may bypass the security completely by changing their complex passwords to simpler ones that they can more easily remember. And even if an employee is diligent, follows complexity procedures and doesn't write the password down, it's very likely they will forget it at some point. Calls to the help desk go up dramatically in organizations that use complex memorized password strategies; and the costs for maintaining this type of password environment is often high as a result.

SafeWord products, by providing one-time passcodes for users every time they log in, addresses the password problem—both the security risks and the nuisance of complicated passwords to remember. User identity is far more reliably ensured for security, and our own SafeWord customers have reported a significant reduction in help desk costs when users switch to tokens because there are no complicated passwords to be forgotten. For more information on the weaknesses of passwords, please see our Weak Passwords Weaken Networks paper at www.securecomputing.com/goto/weakpasswords.

Remote access is a way of corporate life

Remote access has become part of corporate business, and often, employees need to access data from a remote location. Gaining access to that vital data from a remote location must be a reliable, secure process. Making that access secure is what SafeWord products are all about. And because many larger organizations use a combination of remote access methods, centralized control and consistent security across all remote access systems is essential. The PremierAccess GUI-based console lets you manage all users, roles groups, policies, devices, and authenticators from a single point.

SafeWord PremierAccess is the most comprehensive and powerful strong authentication system available for securing remote access connections, offering protection for Web, VPN, wireless, Citrix®, Oracle, Windows, remote dial-up, and other network applications. For more information, please visit www.safeword.com.

Overview of the different advantages of SafeWord PremierAccess and SafeWord RemoteAccess

Both SafeWord products can provide strong authentication in support of Sarbanes-Oxley. SafeWord RemoteAccess, the simpler of the two SafeWord products, provides simple strong authentication. Under maintenance contracts, tokens are replaced *free of charge forever* regardless of the reason for replacement, including your dog ate your token. SafeWord RemoteAccess does not inherently provide authorization or auditing capabilities, but because of its seamless integration with Active Directory, these functions are available through Active Directory. We have some customers using these features as part of their Sarbanes-Oxley compliance measures.

SafeWord PremierAccess is the most complete, flexible, and robust strong authentication solution on the market, and in general, provides more comprehensive support for Sarbanes-Oxley authentication needs. PremierAccess protects many different applications and resources, supports virtually any and all types of authenticators, and can be customized with our software developer kits to fit the specific configuration you desire. In addition, while also integrated with Active Directory, SafeWord PremierAccess provides its own industry-leading role-based authorization capabilities. You can set and define roles for groups of users, allowing them access to exactly the information they need, no more, no less. And PremierAccess also provides its own auditing capabilities with its powerful reporting features.

Both of these SafeWord products provide cost-effective and secure measures for complying with Sarbanes-Oxley regulations as it pertains to strong authentication. Both products offer user self-enrollment to save time and costs. For more information on the differences between the two SafeWord products, please view our comparison table: <http://www.securecomputing.com/index.cfm?key=1391>. And for more information on SafeWord products overall, see www.safeword.com.

Complying with Sarbanes-Oxley is a complicated matter. Secure Computing's SafeWord products can help you to make at least one part of it easier to deal with.

What are the penalties for not complying with Sarbanes-Oxley regulations?

Section 906 of Sarbanes-Oxley outlines the penalties that may apply should compliance measures fail to provide the internal controls that are mandated. Sarbanes-Oxley holds both CEOs and CFOs personally responsible for their companies' financial statements. The logic of the law is that it's the responsibility of corporate governance to ensure that financial statements are accurate, not only by being honest themselves, but by keeping others honest by implementing a set of internal controls that make it impossible to tamper with the company's financial records.

Conclusions and our own Sarbanes-Oxley compliance efforts

By providing authentication, authorization, and effective audit trails, SafeWord products can provide help in several steps along the way toward Sarbanes-Oxley compliance. As a case in point, we can cite our own experience here at Secure Computing. We, of course, use our own SafeWord PremierAccess product during the course of every single business day. When taking measures to comply with Sarbanes-Oxley regulations, having a strong authentication system in place put us in a strong position in terms of authenticating users, authorizing access, and establishing audit records. SafeWord PremierAccess handles all remote access to our internal systems, as well as provides a consolidated log of all authentication events. This not only met the expectations of security, but also provided us with a very simple, single location from which to pull appropriate audit information. We were secure, and we could easily show this was the case. We would like to help you achieve the same confidence and security.