Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Corporate Governance and Information Security

Corporate governance has a long history of ups and downs within US corporations. With the recent streak of scandals affecting public companies, governance and related legislation has again been brought into focus. As an information security professional, it is important to understand corporate governance in general as well as what can be done to prepare for questions or audits of information technology and security resources. This discussion of corporate governance and some methods to prepare for participating in a fir...

Copyright SANS Institute
Author Retains Full Rights

AD

Corporate Governance and Information Security

An analysis of increased interest in Information Security within today's Boardroom.

Steve Loyd
GIAC Security Essentials Certification Practical (GSEC)
March 2004
Practical Assignment Version 1.4b Option

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

Corporate governance has a long history of ups and downs within US corporations. With the recent streak of scandals affecting public companies, governance and related legislation has again been brought into focus. As an information security professional, it is important to understand corporate governance in general as well as what can be done to prepare for questions or audits of information technology and security resources. This discussion of corporate governance and some methods to prepare for participating in a firm's governance efforts will assist any information security professional in being prepared.

Corporate Governance History and Definition

Corporate governance has long been an integral part of a corporation's ability to grow while providing assurances to investors and other stakeholders that the business is being run with diligence and without abuse.
The first US corporations began through needs of public good such as building infrastructure or providing services that benefited the base requirements of the populace[1]. These corporations were sanctioned into existence by the states in which they operated and were subject to oversight and control by smaller numbers of investors[2]. The nineteenth century brought incredible growth in industry that resulted in less individual oversight of corporations. However, a succession of situations gave rise to new legislation which reined in corporations. Legislation such as The National Banking Act, Tariff Act, Homestead Act, Sherman Antitrust Act all were enacted in response to corporate behavior[3]. During the twentieth century this activity continued, as if a cycle controlled by nature the ebb and flow of business activity to increases in oversight charged on. In the twentieth century the problems were mostly oversized mergers, corporate raiders and environmental abuses. The response to these included amendments to the Clayton Act, junk bond reform legislation and the creation of the Environmental Protection Agency[4].

Throughout this history, investors continued to be acutely interested in knowing measurable details of corporations in which they owned shares. Investors cannot endure the burden of detailed knowledge in multiple companies, so it is the governance practices and related legislation which provides the trust and the metrics by which investment decisions can be made. When these are compromised, firms, and investors, suffer from a lack of trust in the operations and financial performance of the business. Such a lack of trust can severely affect the value of a firm's equity in stock markets around the world.

While Corporate Governance is a term likely to appear in any given day's business periodicals, it is a term that remains undefined for most people. John C. Shaw defines Corporate Governance with an emphasis on risk management in his book Corporate Governance and Risk[5].

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

> *"….the system by which corporations are directed and controlled…*
> *…provides the structure through which company objectives are set…and monitored"*[6]

This explanation of the governance term draws attention to the outcome, or results, of oversight operations. What is the result of company operations? What happens if a strategic decision is made one way or another? In addition to inferring these questions, the definition addresses the issue at hand for information security professionals; how can the information within a corporation be maintained and trusted and how can wrongdoing be prevented or detected? A key goal for information security professionals involves the protection of corporate information from improper access or modification. This is similar to the goal of the financial reporting process and, in fact, a part of the financial reporting process includes a role played by the information security function.

Topics of governance are chiefly concerned with the operation of the board of directors of a corporation. The board is responsible for the following[7]:

- Fiduciary Oversight – ensures that the corporation has the appropriate processes and controls in place, selects and works with the external auditing firm, generally monitors the corporation as it attempts to meet financial goals.
- CEO Selection and Succession Planning – The board of directors hires the CEO, not the other way around. As such, the board must monitor the CEO and ensure that his/her actions and intentions are in the best interests of shareholders.
- Strategic Planning – Although a constant process, the official strategic plan for the corporation should be reviewed by the board at least annually. Throughout the year the board should revisit the plan to ensure that the corporation is headed in the right direction.
- Equity Policy – Plan for the distribution of stock equity among executives as well as to line employees, if applicable. Ensure that equity plans are in line and related to overall corporate financial performance.

The board of directors is led by the chairman, normally numbers from eight to twelve total members, and each member is assigned to one or more committees that are divided up among the entire board. The audit, compensation, and corporate governance committee must be made up of board members who are independent of the firm (non-employees)[8]. Understanding the makeup of a firm's board can help in dealing with requests that arise from board discussions.

Generally, governance deals with the core aspects of the business and how their context can be made *transparent* for stakeholders of the corporation. The term "transparent" is continually referred to within governance discussions and refers to the ability of the company board, investors and stakeholders to understand the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

key drivers, metrics and risks that exist for a corporation as well as how the corporation is fairing in meeting key metrics over time.

Current Events

The past two years have provided a long list of studies in governance failures through a host of industries. Huge oversight failures at Worldcom, Enron and Tyco have highlighted how wrong corporations can go, and how easy it can sometimes be to cover up wrongdoing. The failures were the result of a variety of problems, from initially small earnings "corrections" to completely dishonest financial management by executive teams. Regardless, the problems continued over a number of operating periods due to poor governance by corporate boards, and lackluster audit procedures from independent auditing firms. Of course, the problems would not have ever have occurred if it were not for the improper behavior of key executives and their teams. However, simply focusing on the selection and hiring of a trusted top executive is not enough to protect against fraud.

In response to many of these governance failures, government and fiduciary organizations have placed a number of new laws and regulations in place to protect investors. The ebb and flow of governance throughout history continues today. Numerous legislative and regulatory changes have taken place since the first of the recent scandals. Most famous are the Sarbanes-Oxley[9] and Graham-Leach-Bliley[10] acts, which have significant impacts on corporate information security professionals and their practices. Information security practices within corporations have been highlighted as a result of governance changes and the future holds additional interaction between today's CIOs/CISOs and the boards and investors of our corporations.

In a letter to the Securities & Futures Commission in Nov 2001, Andrew Sheng notes "Now more than ever, the world regards good corporate governance as a hallmark of quality. It is a competitive necessity." He further notes, "Dotcoms can expect more shareholder involvement in the manner in which the company is run[11]". Sheng's comments recognize that boardrooms are increasingly interested in the operations and control environments in a company in addition to the reported financial results.

The Issue

The financial information of all public corporations exist in a virtual world, spread across data centers, networks, servers, applications and databases. The journal is no longer a journal, the ledger not a ledger. Corporate financial data is a collection of electronic information, assembled into different views per the task at hand. Daily entry of expense information, automated recognition of revenue, and periodic financial rollup reporting routines are all a common part of any day for executives of any public company. Much of this data isn't entered by hand, and

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

not by a companies own workers. Data is just as likely to come via an electronic feed from a partner, supplier or the company bank.

Furthermore, most all companies have manual processes that play a key part in their financial accounting, and reporting activities. Excel spreadsheets, simple macros, and human processes are commonly used to tie data together from disparate systems.

Who is to say that the data regarding a given periods revenues hasn't been changed maliciously, or accidentally? What indication will there be of a zero erased from a value in a database, when it leaves no smudge? When access is not tightly controlled, or when key components of a process, such as financial reporting, are trusted to a small number, or maybe just a single individual, it's no small task to ensure that no errors or malicious modifications are made to the true state of financial information.

The applications that form the financial and management user's view into corporate data provide a structure for preventing, and in many cases detecting, misuse. Yet, at some level with a given set of access, knowledge, and intent there are still opportunities for fraud that would likely go unnoticed. Policies such as division of responsibility and mandatory vacations go a long way in preventing fraud, but more needs to be done.

Information Security and Assurance aren't Simple

Corporations must put safeguards in place through policies, procedures and technology so that the "proverbial zero" isn't erased. However, information security is not a simple topic and certainly doesn't make for interesting cocktail party discussion for most people. This partly explains the disinterest from boards of directors and corporate executives in the past. Explanation for the remainder of disinterest is grounded in a revenue-side focus and an ignorance of the costs associated with aggregated risk and actual loss. Financial scandals have changed the situation, whereby executives and boards are now very interested in the controls and procedures that are in place to prevent fraud, control loss and keep operations continuing. The focus is again on corporations to explain how they organize and implement internal controls for all systems related to financial reporting, and there are those that call for the controls to go much further than just financial reporting.

Trouble at the NYSE

In 2001 allegations of trader misconduct at the NYSE led to sweeping changes of the organization, ultimately leading to the resignation of Dick Grasso, the NYSE Chairman. The beginning of the allegations dealt with trading specialists placing their own trades ahead of market orders by "pausing" the trading system. The NYSE reported spending $142 million on regulation activities during 2000, but

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

former officials had reported “Grasso’s lieutenants turn down requests for additional funding while the marketing and communications departments’ budgets surged”[12].

The NYSE had systematically failed to report on recognized misconduct within the organization, and controls were not in place to enforce the transparency that would have brought such misconduct to light. An organization with the proper controls, policies and procedures in place will not require a whistleblower, nor will it require leadership with remarkable acuity for addressing existing problems. Such an organization, due to the transparency brought on through the governance program will provide the indicative metrics to the board and other stakeholders, without having it be a deliberate operation[13]. This would have meant that monitoring and metrics would likely have shown the trading behavior of the specialists, long before it became a widespread practice. A chart showing the number of system “pauses”, or an analysis of the type of activity by time throughout a normal trading day, may have indicated that there was suspicious behavior that required additional review.

Part of the solution to the NYSE problem took over two years to implement, involving a number of trading system application changes as well as a handful of new procedures or modifications to existing procedures. These included management and reporting changes, as well as the implementation of new technology and technology process to stay on top of the trading activity within the systems. Threaded throughout this solution was involvement by Information Technology and Information Security personnel, displaying the impact of a governance issue on the field.

Preparation for Participation in the Governance Process

A CIO, CISO or other professional involved with the management of information security must be prepared to play a part in the corporate governance process. The initial step in preparing for a part in the governance process is refreshing knowledge and understanding of corporate governance. Being able to provide a definition and participate in general discussions regarding governance will help to foster further inquisition into the related issues. In addition to the corporate governance definition, it helps to consider all the players involved in corporate governance scenarios. Everyone involved with the company plays a part, but in particular are auditors, the board of directors, investment banks, and the corporate executive management[14]. Once familiar with the general issues and practices of overall governance, the next task is to make sure that information security management and practices are in line with the expectations of good governance. Just as the overall corporation is to be transparent, with processes and checks to ensure good financial reporting, so should the information security organization exercise similar transparency.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Transparency in information security and information technology comes down to having good processes, knowing how and why they work, documenting them thoroughly, and reporting on the result. Backups for example, in many IT shops are working "great". In others, there are documented goals and procedures indicating what the backup philosophy is and exactly how and what to do to run them each day. The answer to how backups are running in such as shop is a clear set of data showing the number of failed backups, requested restores, avg restore time and other metrics, all tracked over time. Identifying what "status of the backup program is", and applying metrics to monitor it is key. That's transparency. It allows other groups, those who aren't systems administrators, to understand how the program is working. The audit committee, the CFO, the Board of Directors may someday ask to understand the status of backups, with the metrics in place you'll have the answers.

Document retention is also an area that is at the top of the list for audit committees and the corporate legal team. A recent CIO article notes "enforcing document destruction policies could be a different way of thinking to a CIO whose mantra is backup, backup, backup.[15]" However, just as backups are to be run with precision processes, so is document retention. This means having the process and technology in place to identify date by type, and properly determine it's content and age. Then, according to the corporate document retention plan, data no longer within the policy should be properly destroyed. A bit of a misnomer, to an IT worker, a retention policy has more to do with destruction than retention, since that's the part that is new. If there isn't an official document retention policy in place, it's time to get the corporate counsel together and create one. A good explanation of the factors involved and the process for creating such a policy is described in a paper by Jay G. Martin entitled "Developing an Effective Document Retention Policy[16]"
This document leads an information security professional through the process, including working with corporate legal and executive management in getting the policy approved, an absolutely critical step.

With the plan in place, just as with backups, the key metrics and the methods for monitoring them need to be established and implemented. Here again, when the day comes when you're asked for the status of the document retention plan, you'll have the necessary data, and maybe even some pretty graphs.

Backups and document retention are just two examples of keys areas that are within sights of the corporate audit committee, the board of directors, and definitely executive IT management. The same philosophy applies to all parts of information security and technology. Even if the day never comes when a board member tests the waters by asking for status on a specific information security or technology program, your overall performance in the areas will be all the better for the added process review and tracking.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Preparing for taking part in the governance process comes down to two key items. First, be familiar with governance, the people involved, the issues at hand, and the goals for all involved. Next, get your house in shape and apply the same "transparency" to information security and technology as is applied to the corporation as a whole. Finally, have the processes and metrics of the organization reviewed by an outside party. In many cases this means an outside security review by an independent auditor. However, don't just settle for the standard set of scripts and questions that an IT/IS auditor brings along, have them audit your specific set of processes and metrics that have been devised. Ask that they review and provide information about the format, content, and implementation of the processes that are already in place. Having a third party review the plans and their overall implementation is a perfect way to get new ideas as well as determine the efficacy of the changes.

Framework for Information Security & Technology Transparency

As noted above, one of the most significant outcomes of recent governance events was the introduction of the Sarbanes-Oxley legislation, and in particular, section 404 of the legislation which covers internal controls. The section on internal control requires that systems storing or processing corporate financial information have appropriate controls in place to safeguard such information. What is appropriate and what the controls should cover has been argued and debated for much of the past two years. Without arguing the points here, there is still much to be gained from the resources put in place as a result of the legislation. The requirement has been most recently defined as "appropriate controls for systems and processes used in the financial reporting process", a much tighter definition. Even so, a lot of the resources that were put together to fit a much broader requirement provide a very useful framework to be applied in a variety of situations. Most notably for IT environments is the Control Objectives for Information and related Technology from the IT Governance Institute, otherwise referred to as the "CobiT". These resources provide a starting point of control objectives in the COSO framework. The COSO framework was developed as a method for identifying risk and documenting controls for corporate processes, both manual and automated[17]. CobiT takes the COSO framework and begins to fill in control information that would be appropriate for most organizations. The framework is a useful resource as an implementation of full COSO is a rather intense undertaking. The CobiT guidelines run through a step-by-step process outlined as follows[18]:

1. Plan and Scope – Establish a team to coordinate and guide the process. Learn about the financial reporting processes, as well as other key business processes. Define which business processes are critical, and will be included, in at least the first run of the project.
2. Risk Assessment – Identify the areas that exhibit potential for problem. Assess and rate each with a "likelihood" and "impact" rating.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3. Accounts & Control Review – Inventory existing controls and accounts within systems and processes that are the target of the project.
4. Documentation Design – Although there is not specific guidance as part of most frameworks, the CobiT provides a base to work from.
5. Control Design – Critical to the success of a control program, this step evaluates the ability of the organization and its processes to enforce a particular control. Key issues are what other controls any given control will be dependent on, or what personnel or processes must be involved for the control to succeed.
6. Current Operations Audit – For each control, identify what state the control is currently in. Some will be "non-existent", others may be "Managed and Measurable".
7. Identify Weaknesses – Considerable professional judgement comes to play in this step where shortcomings should be defined as either "deficiencies" or "weaknesses", based on whether the issue is likely to subvert the control, or in a financial environment, result in the misstatement of an organization's financial records.
8. Document Results – It's just as important to document the test results as it is to document the tests. Having documentation of the outcome of tests will provide the records required for auditors, or to go into further detail with others.
9. Build Sustainability – Review the full program at this point and ensure that it is sustainable into the future. Controls are not a one time event, but a continuous process.

In addition to the process guidelines, the CobiT materials go into additional detail, making it much easier to create an effective program without having to re-invent the wheel. The CobiT materials are extremely informative, yet there are other materials available, and more are likely to become available in the future.

Summary

Corporate governance is again a key topic for legislators, investors, and executives. As a key topic, information security practitioners should ensure that they are responsibly dealing with the issue and ready to provide related information. Recent events have shown that there is much to be done to restore investor confidence in today's corporation, and that it must be done. The situation continues to change, even recently key regulations were further relaxed from their initial "knee-jerk" reaction[19]. However, as a manager responsible for information security it is important to be prepared by being familiar with corporate governance concepts, setting up transparency in operations, and adopting an structured framework for analysis and documentation, such as that offered by CobiT.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

[1] Macauley, Irene. "Corporate Governance: Crown Charters to Dotcoms" 2002 URL: http://www.financialhistory.org/fh/2003/77-1.htm (Jan 10, 2004)
[2] Hawley, James P., Williams, Andrew T. The Rise of Fiduciary Capitalism. University of Pennsylvania Press, Nov 2000, xii
[3] Macauley, Irene. "Corporate Governance: Crown Charters to Dotcoms" 2002 URL: http://www.financialhistory.org/fh/2003/77-1.htm (Jan 10, 2004)
[4] IBID
[5] Shaw, John C. Corporate Governance And Risk: A Systems Approach. 1st ed. Indianapolis: Wiley, 2003.
[6] Shaw, John C. Corporate Governance And Risk: A Systems Approach. 1st ed. Indianapolis: Wiley, 2003. p.23
[7] http://www.tiaa-cref.org/pubs/pdf/governance_policy.pdf
[8] ibid
[9] "Public Law 107-204." U.S. House of Representatives. 3 Mar 2004. <http://www.nabl.org/government/Public%20Laws/PDF/PL%20107-204.pdf>.
[10] Worthen, Ben. "How to Meet Tomorrow's Privacy Rules Today." 1 NOV 2002. CIO.com. 4 Mar 2004. <http://www.cio.com/archive/110102/rules.html?printversion=yes>.
[11] Sheng, Andrew. "Corporate Governance – How does it concern Dot.Coms?" 2001 URL: http://www.hksfc.org.hk/eng/press_releases/html/speech/01/as271101_icac.pdf Jan 20, 2004
[12] Ip, Greg. Kelly, Kate. Craig, Susanne. Dugan, Ianthe Jeanne. "How Grasso's Rule Kept NYSE On Top But Hid Deep Trouble" Dec 30, 2003 URL: http://online.wsj.com/article/0,,SB107273454992830200-search,00.html?collection=autowire%2F30day&vql_string=grasso%27s+rule+kept%3Cin%3E%28article%2Dbody%29 (Jan 4, 2004)
[13] Shaw, John C.. Corporate Governance and Risk. Wiley Press, 2003, p.76-91
[14] "bigger than enron: watchdogs." PBS.org. 4 Mar 2004. <http://www.pbs.org/wgbh/pages/frontline/shows/regulation/watchdogs>.
[15] http://www.cio.com/archive/011504/policy.html
[16] "Developing an Effective Document Retention Policy." 10 FEB 2003. Winstead Sechrest & Minick P.C.. 23 Feb 2004. <http://www.winstead.com/articles/articles/Developing%20an%20Effective%20Document%20Retention%20Policy.pdf>.
[17] "Report of the National Commission on Fradulent Financial Reporting." Oct 1987. COSO.org. 16 Mar 2004. <http://www.coso.org/NCFFR.pdf>.
[18] "IT Control Objectives for Sarbanes-Oxley." IT Governance Instutute. 16 Mar 2004. <http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=9757&TEMPLATE=/ContentManagement/ContentDisplay.cfm>.
[19] Worthen, Ben. "A Funny Thing Happened on the Way to Compliance." 1 Dec 2003. CIO.com. 6 Mar 2004. <http://www.cio.com/archive/120103/oxley.html>.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**