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.

Jekyll & Hyde in the Boardroom

Businesses rely on a balance of technological implementation and security implementation to create and maintain sound practices and trusted business relationships. Due diligence is an Executive requirement of traditional brick-and-mortar business that has greater implications for businesses with an on-line presence. Business success or failure can hinge on the business implementation of the Chief Technology Officer and the Chief Security Officer, two key IT management positions. Each stand on one side of a scale with t...

Copyright SANS Institute
Author Retains Full Rights

AD

Jekyll & Hyde in the Boardroom

David A. Nixon

August 8, 2001

Version 1.2e

Introduction

Businesses rely on a balance of technological implementation and security implementation to create and maintain sound practices and trusted business relationships. Due diligence is an Executive requirement of traditional brick-and-mortar business that has greater implications for businesses with an on-line presence. Business success or failure can hinge on the business implementation of the Chief Technology Officer and the Chief Security Officer, two key IT management positions. Each stand on one side of a scale with the Executive focus determining the balance. The balance directly equates to the extent of due diligence exercised. The Chief Technology Officer provides direction in translating business objectives to technology implementation. The Chief Security Officer provides direction in managing risk and leveraging security implementation as a requirement to both support and enable_an on-line presence. This trinity is a system of checks and balances that will ultimately lead to success in the New Economy.

Due Diligence

This term is used in many vocations yet the concept is always the same. Due diligence cognates responsibility for ensuring a requirement is met to the best of one's ability. The application for Corporate Officers is for the protection of corporate assets. Protection includes fiduciary protection of shareholder interests and protection from risks and liabilities against corporate assets. For shareholders a corporate asset represents an object of monetary value, much like a US twenty dollar bill represents a fraction of a gold bar that is held in a federal reserve. Due diligence also incorporates proper management of corporate debt. Security compromises, even minor incidents, incur a cost that increases debt. Failure to practice due diligence can be prosecuted as a criminal matter.

Due diligence is an important matter for businesses with an on-line presence. What is an asset? Is a several million dollar ERP system an asset or a liability? I guarantee that if a company were to liquidate, a several million dollar ERP solution would be listed as an asset. Good test to determine if an on-line resource is an asset is to unplug it for a day. If the company helpdesk is inundated with phone calls then it is an asset. NOTE: I do not recommend doing this without written approval from not only your supervisor but also your supervisor's supervisor. This is to demonstrate that IT systems that were traditionally regarded as overhead are actually company assets that require protection. This is not an obscure concept but an actual requirement that goes beyond theory to reality.

CareMark International Inc. had a computer intrusion that resulted in the loss of critical information. Publicity surrounding the event severely affected stock prices. "As a result, claiming that the officers should have employed better protections to safeguard company

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

assets, shareholders attempted to sue CareMark officers and directors individually for fraudulent theft from the company."[4] In other words, the officers were charged with not practicing due diligence by the shareholders. The CareMark officers were able to provide company policy and procedures demonstrating that a security team was in place along with policies and procedures to deal with the intrusion. This resulted in a ruling in favor of the CareMark officers. You are probably asking "why" because it is obvious that the security implementation was inadequate. The court ruled that the CareMark officers "had set up a due diligence framework for security—the officers should not face personal liability, even though they were unsuccessful in detecting the particular fraud scheme in question."[4] Lessons learned: security is a moving target and the courts realize this fact. Demonstrating an attempt to keep pace is enough to show due diligence is being exercised.

Current unresolved court cases, specifically distributed denial of service (DDOS) based tort claims, have added a new dimension to due diligence, third-party liability for online conduct and negligence managing on-line resources. A good example is the DDOS launched against eBay. eBay generates somewhere close to eight million dollars an hour through on-line presence. A DDOS attack spanning several hours not only takes away generated revenue but also affects stock price. eBay's stock price dropped twenty four percent right after their denial-of-service attack. eBay is rearing mad, and lawyers are chomping at the bit. Who do they go after in this litigious society? Common sense might say go after the individual who launched that attack. It is very unlikely that eBay will be able to recoup several million in loses this route. How about the individual owners of the PC's that launched the packets at eBay servers? Again the chances of recouping several million in loses are slim and the cost to go to trial against the multitude of individuals is not worth the cost expenditure. Evidence gathered showed that a majority of the DDOS traffic came from cable modem and DSL Internet service providers. Who has the deep pockets? The ISPs generally have deep pockets. Excite@home is the leader in broadband cable Internet connectivity (according to their website). A good chunk of the DDOS traffic targeting eBay came from @home users. eBay lawyers see @home as not being a good Internet neighbor because @home has failed to maintain adequate security to protect Internet neighbors. Did @home officers practice due diligence to protect @home from third-party liability? That is for the courts to decide. Incidentally, the choice of using Excite@home is to show the troubles that a potential legal battle can have. Excite@home is currently having a little financial trouble because of a drop in stock price along with several debts that are being called. Excite@home is having difficulties borrowing capital to cover those debts because of their drop in stock price. The stockholders could charge the Excite@home officers with failure to practice due diligence. Granted, much of the Excite scenario is speculation and speculation is what drives the Stock Market.

Chief Technology Officer

Depending on the company management structure, the Technology Officer position might be incorporated into another position or defined by another title. The application of titles is not the focus, application of the duties of the position is the focus. The

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

individual with the duty to advise the Corporate Officers through business decisions involving the implementation of technology to meet an organization's business strategy shall here after be referred as the Chief Technology Officer (CTO) within this paper.

This position is a simple evolution over the past 25 years of the accounting equipment (calculator) manager to computer services department head to Chief Technology Officer. As computers became more prevalent, accounting personnel shifted from manual computations on clunky calculators to automated computations with the assistance of spreadsheet software. VISICALC, a simple spreadsheet application started the (r)evolution. What took a week to compute manually took hours with the assistance of a computer and simple software. Computers have evolved as a viable business tool to the point of being an assumed fixture of at least one on every business desktop. There is no arguing that technology is now a driving factor in Strategic Business Plans for companies. The Chief Technology Officer is the focus for that direction, translating business strategy into technological implementation. The key role of the CTO is an advisory function to the Corporate Officers so that they may make informed decisions on what business resources should be allocated to which technology implementation projects. Also of importance is the management oversight of deployed technology such as file and print services, network infrastructure, telecoms and power plant.

Chief Security Officer

The Darwinistic view of the Chief Security Officer (CSO) does not have a long lineage compared to the CTO. The CSO is the Old Testament Genesis of Adam. The desire (need) arose, the position was created. Y2K did have one outcome, it helped push computer security into the perspectives of the common household and businesses. If any CSO lineage can be drawn it could be linked to Y2K remediation project managers.

The duties of a CSO comprise being aware of and notifying Corporate Officers of potential and current technology risks and liabilities to meet due diligence requirements of Corporate Officers for deployed technology and technology marked for future deployment. An important function of the CSO is management oversight of deployed systems to lower risk. A sampling of these systems include power backup, tape backup, fire suppression for computer rooms, intrusion detection systems, encryption, and firewalls.

Jekyll And Hyde

When compared side by side it is obvious that the CSO and CTO positions are fundamentally polar. The CTO strives to utilize technology to open avenues of communication, to make it easier for employees and external business partners to complete job tasks with a savings to time and finances expended. The CSO is constantly assessing risk and determining liability for open avenues of communication and striving to limit risk and liability by closing avenues of communication.

An example of the dichotomy is the debate of deployment of single sign-on products.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

These systems make it easier on the user by placing the password management for multiple systems off of the user and onto a computer system. The obvious positive gains will be increased productivity, lowered requirement for employee training, and ease of integrating user interface to multiple systems. The risks invoked are a single point of failure and a reimplementation of a remote host (rhost) system. One password is used to access multiple systems and there have been a multitude of papers on the subject of poor password creation by users.

The example shows the focus of each perspective. Which perspective is correct? Both! The proper solution will factor in the benefits verses the risks and conclude if the benefits outweigh the risks. Who decides on the proper solution? The correct deciding individual(s) are those who will be ultimately responsible for protecting company assets under the definition of due diligence. The CTO and CSO should serve in an advisory capacity to the deciding individual(s). Making both the CTO and CSO positions a vital managed resourses for business success. Due diligence exercised in the decision process is proportional to the Executive focus on risk management. With the decision made, the task falls back to the CTO and CSO for implementation. The CTO responsible for driving the deployment and the CSO responsible for conducting audits and risk assessments to confirm that the deployment falls within the decided risk parameters of the deciding individual(s). This structure does not separate CTO staff from CSO staff. Ideally specialized personnel are commingling so that expertise can be shared and utilized. For example, Intrusion detection specialists make excellent network managers. They are obviously the ones most familiar with the network traffic within the managed network. Coupled with a system administrator, the combination can better tune systems for network performance.

The New Economy

Robert X. Cringley fairly consistently comes out with little nuggets of wisdom that tend to grow on you as you peel the layers back like an onion. "All That Glitters" just happens to be one of those onions. Most of the article is prequel to the points made in the second to last paragraph.

> "[B]usiness intelligence allows businesses to fail more quickly, which is good. Quick failure is cheaper and easier than a long death. Quick failure makes companies more willing to take risks on new ideas, knowing that if those ideas fail, the failure will be detected early. Failing quicker is the essence of this new economy, creating nimble organizations that can do more with less and often require no debt at all to finance growth."[12]

Consider that many companies deploy security as an add-on feature to be included at the end of an implementation. The correct approach is to design and develop both side by side. Common business sense dictates that discovering that part of the implementation fails to meet a needed requirement early in the implementation rather than toward the end is more desirable. What happens if a security requirement is the short fall? Is it overlooked or does the company go back to redesign?

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

> "Businesses thus need to discard the outdated view of security as simply an "insurance" plan against fraud; they need to view is as a necessary element for the long-term viability of new markets and to ultimately enable the NEW Economy to achieve its full potential."[4]

Conclusion

It is paramount that the job duties of the CTO and CSO do not fall on the same person in order to stay viable in the New Economy. Business intelligence alone is greater with two sources providing input. Delegating responsibility for both CTO and CSO tasks to one individual leads to favoring one side and neglecting the other, breaking the scale of checks and balances. Executives then lack two dedicated opposing perspectives to base decisions. Typically the development side is favored over risk management. This leads to neglected security and neglected security is neglected due diligence.

© SANS Institute 2001, Author retains full rights.

References:

1.Holohan, Meghan "Administration problems often lead to security lapses" 19 July 2000
URL: http://www.computerworld.com/community/security/perspectives/0,,NAV65-663_STO47316,00.html

2.Wetmore, Pete "Covering Your Assets" 4 December 2000
URL: http://www.insurehitech.com/apps/usr.class/content/about/articles/interactive.jsp

3.Tobias, Zachery "The New Security Pro" 7 May 2001
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60207,00.html

4.Author Unknown "NVP: Information Security"
URL: http://www.ttivanguard.com/risk/netpresentvalue.pdf

5.Vijayan, Jaikumar "IT security destined for the courtroom" 21 Mat 2001
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60729,00.html.html?OpenDocument&~f

6.Kang, Shin Cheol "What is CIO?"
URL: http://oracle.hannam.ac.kr/~sckang/lecture/cio/cio.htm

7.Author Unknown "NCHICA-HIPAA Job Descriptions" 8 August 2001
URL: http://www.nchica.org/HIPAA/HIPAAjobs.html

8.Trickey, Fred "Secure Single Sign-On: Fantasy or Reality?"
URL: http://www.gocsi.com/sso_ft.htm

9.Korman, David P. & Rubin, Aviel D. "Risks of the Passport Single Signon Protocol"
URL: http://avirubin.com/passport.html

10.Thaddeus, Jude "Culture of Indifference Plagues Password Security" 5 February 2001
URL: http://www.computerworld.com/community/security/security_manager/0,,NAV65-663_STO57286,00.html

11.Author Unknown "Password Clues" 13 July 2001
URL: http://www.centralnic.com/page.php?cid=77

12.Robert X. Cringely "All That Glitters" 18 May 2000
URL: http://www.pbs.org/cringely/pulpit/pulpit20000518.html

© SANS Institute 2001, 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**