

Security and Compliance

Author, Timothy M. Ameredes

No two topics will keep a CIO or CSO up at night like Security and Compliance (S&C). Mostly because achieving both is like trying to grasp water. Both are moving targets since attack methods and the business environment are continually changing - especially if one is starting with nothing in place. For purposes of this paper, S&C initiatives are focused on safeguarding data. This paper will also attempt to lay out a high level road map to achieve both.

1. S&C requires change in the following five areas:

- A. Policy
- B. Infrastructure (and possibly architecture)
- C. Business Process
- D. Security (technical and non-technical)
- E. People

A. Policy- Policy is the easiest of the five areas to solve. It requires reviewing existing policies from perspectives of the other four areas (infrastructure, business process, security and people). If one is working in a larger organization, sometimes policies will need to be aligned with broader corporate or governmental “parent” policies. Where gaps exist, write/revise policies to address them. One example, laptops are a prime target for security policies because they make large amounts of data portable and easy to steal. So companies should draft new policies on the handling the equipment and encrypting the hard drives. Including aspects like requiring users to lock down laptops while “on-site”, not using corporate laptops for personal use, or requiring drive encryption software to be loaded and utilized. Encryption software comes with its own administrative caveats and user learning curve but it is worth the effort. In either case, personal laptop usage should be prohibited for business use.

B. Infrastructure- Does network equipment need upgraded to take advantage of security features that is included with the newer technology? Will your current infrastructure allow you to research a potential breach from an internal or external source? Probably not. It requires CIO’s to assess audit capabilities of every server, router, switch, firewall, database, application and disaster recovery site. It will require quite a bit of configuration of audit functions on prior mentioned equipment and software platforms. Your analysis will also require the organization to purchase an audit log file management solution. This will provide your company central storage (or distributed depending on company size, locations, etc) for log files that

have been collected via automated processes. Not to mention an audit trail that spans a company defined time frame. This solution will also provide a reporting structure that can be run on defined time intervals.

C. Business Process- Do your business processes expose sensitive or HIPAA protected data to unauthorized employees (“need to know” rule), the public or less secure business partners? Have you revised outsourcing contracts to include verbiage that make partners bear risk for not protecting data or require them to meet industry accepted security standards, like ISO 270001 or others? Have you evaluated the capabilities of outsourced vendors to meet expectations for protecting data? One example of a business process change is requiring phone calls to be screened for phishing attempts. Requiring call centers to ask an account related question that only the correct individual would know. Another more straight forward example is eliminating printed social security or bank account numbers from all correspondence, external billing processes or usage while logging in on-line (usernames). Other business process changes directly related to security include modifying Project Management and development processes (SDLC, CMM) to include security checks and balances. Business process changes are very tied to people and their acceptance/adherence to changed processes.

D. People- Most people are resistant to change. The toughest part of compliance is getting employees and managers to bear responsibility and support the compliance changes over the long run. In most instances, compliant processes adds steps or takes longer, or slows down a businesses ability to adapt, react or capitalize on changing business needs. Training, awareness, persistence and regular audits are keys to success. Persistence and auditing being the most important. Both show employees that these initiatives are here to stay. In State government there is a long standing mind set that all information is owned by the public and should be given when requested. The mind set primarily stems from the Freedom of Information Act and State Public Records laws that support it. It will take time to change. Policy also plays an active roll in getting employees up to speed.

E. Security- Security and compliance initiatives tend to overlap. It requires an organization to mesh the two strategies together into a cohesive approach. Organizations should have a formal, well defined incident review process, incident team identified and a qualified external forensic auditor to assist in verifying investigatory results. It is best to utilize a qualified external auditor since it is viewed legally as being a stronger verification. Using unqualified auditors weakens your audit results and can cause them to be challenged. It requires an organization to regularly monitor infrastructure reports for anomalies and if the reports do not exist, go to item B above and layer in the infrastructure to achieve them. Separation of duties is another approach to controlling internal/external exposures. Separating duties is much easier to achieve for larger organizations than it is for smaller ones. The obvious reason is a smaller organization may not have enough employees or

will become cost prohibitive to segment duties properly. However, if the small organization is in the Healthcare, Financial or Insurance sector, then they need to find a way to staff up and/or change business processes in order to limit liability of a breach (internally or externally). Physical security is another aspect to protecting data. Access to buildings, data centers, securing all servers (test, etc) are all included in physical security layer.

2. Potential obstacles when implementing S&C Initiatives

The more rocks one turns over, it seems the more items that need to be addressed. It may take years of due diligence and tenacity to truly achieve S&C initiatives. Things like implementing an audit log management solution, system upgrades and cost/time required to implement the initiatives will compete with business, revenue generating or political initiatives. In the government sector, new S&C legislation does not always work well with the long standing Freedom of Information Act or State sponsored public records laws. If Governments “do what they need to” to protect data (i.e. Citizens from phishing, scams, etc), then those efforts will directly work against the prior legislation. Legislators to take a hard look at making these laws work together as well as requiring state entities handling health information to be HIPAA compliant. Currently, States are not required to be HIPAA compliant.

3. The Compliance ROI Equation

Much has been written about the ROI of S&C initiatives. It is very difficult to measure. Some say it is measured by how much an organization needs to spend to “feel safe”. Below is another alternative for measuring ROI for S&C initiatives. It requires organizations to view ROI as preserving net income and market share against costs of not complying (or not implementing security) and their competitors who are viewed by customers as protecting their data.

$$\text{Compliance ROI} = \frac{\text{Cost to Comply}}{\text{Net Income Saved by Complying}}$$

Net Income Saved by Complying = Cost Of Not Complying (since implementing S&C initiatives or “complying” protects net income, the cost of not complying directly correlates to net income saved)

Cost Of Not Complying = Risk x (Liability Avoidance + Lost Net Income + Regulatory Fines)

Liability Avoidance = Costs to settle or pay lost law suits (ie industry average)

Lost Net Income = Short Term Loss + Longer Term Loss

Short Term Loss = Legal fees to defend a breach, cost of public notifications, forensic audit costs, customer fraud protection costs, etc.

Long Term Loss = Loss of Market Share (ie long term revenue)

Regulatory Fines = Industry average compliance related fines

Risk Scale = 0, .1, .2 .3, .4, .5, .6, .7, .8, .9, 1

Cost To Comply = Total cost to implement security and/or compliance solution(s)

Risk should be measured by the organization's standard risk identification process. Then crosswalk their internal measurement to the scale above for purposes of the calculation. The more close an organization is to the whole number 1, the more impact not complying will have on net income.

Most of the above data can be determined by studying costs, revenue impact and fines that businesses have occurred for breaches over the last 4 years.

Compliance ROI result will equal the length of time in years to recoup the initial investment.

4. Summary

Due to the adverse impacts of not complying has on corporate finances, branding or government image, who should be responsible for achieving compliance efforts? The CEO, CIO, COO, CSO, Board Members, Managers, Employees? The correct answer is "everyone". Securing customer data and infrastructure is an organizational effort, shared responsibility and should be funded accordingly.



Author Bio

Tim Ameredes has 17 years of experience in leading roles where he streamlined business operations and/or aligned IT in corporate, government, higher education industries.

COPYRIGHTS

Copyright © 2008 B2B Knowledge Source, Inc. The works of authorship contained in this document, including but not limited to all design, text and images, are owned by B2B Knowledge Source Corporation and all rights are reserved therein. They may not be copied, transmitted, displayed on Intranets or the Internet, mass distributed by email, US Mail, fax or any other means (for compensation or otherwise), licensed, altered or otherwise used in whole or in part in any manner without the B2B Knowledge Source's prior written consent, except to the extent permitted by the Copyright Act of 1976 (17 U.S.C. § 107), as amended, and then, only with notices of B2B Knowledge Source's proprietary rights.

TRADEMARK NOTICE

B2B Knowledge Source and "The B2B Symbol" are trademarks of The B2B Knowledge Source Corporation.