Compliance Motivation: The Info Security Diet

Rebecca Herold, CISSP, CISM, CISA, FLMI

December 2003

I'm writing this on New Year's Eve and thinking about resolutions. Possibly the most popular resolution is to lose weight. Possibly the most quickly broken resolution is to lose weight. People spend hundreds to thousands of dollars buying equipment, memberships, and food plans to help them with their resolution. People know they must eat less and exercise more to lose weight. However, just getting a $3000 piece of equipment will not result in weight loss if it sits in the corner gathering dust. Those who are successful in their goals have strong motivators to keep them going. An expensive piece of equipment does not, in and of itself, provide motivation to use it. The motivation comes from either strong inevitable punishments or strong inevitable rewards. Motivations can vary greatly from person to person.

If it is so hard for people to follow their own, self-imposed rules (resolutions), why do we think they will all happily follow our information security and privacy rules? Sure, they know they SHOULD follow the rules; that they will help protect organization assets by doing so. But, what consequences do they face if they don't?

Every organization struggles to have personnel follow good information security practices. Most personnel generally do not like to jump through the perceived hoops that good security often requires, and there is no motivation for them to perform security activities and no consequences for them to face when they do not comply with the organization's information security rules.

It is safe to say most personnel have difficulties performing all the tasks they are expected to accomplish each day. Most want make their work easier by finding shortcuts. One of the easiest shortcuts is simply to go around security; technology as implemented in most organizations makes this fairly simple and seemingly innocuous…who's going to find out if an individual "loaned" his password to a co-worker when he can't get to the office and needs to get an important message sent on his behalf? And, isn't it tempting to save time by not making a regular backup of laptop and PDA files and email? Or, think of the time saved by not applying those OS patches that seem to be released almost daily. These and other actions truly do save quite a bit of time…and most personnel are willing to gamble that something bad will not happen any way.

Information security professionals must effectively and frequently communicate the impact of information security and personnel activities. Executives must clearly and visibly support information security policies and practices. Organizations are almost completely dependent upon technology to secure information because they cannot confidently expect that personnel are going to follow information security rules just because it is the right thing for them to do. Personnel must be motivated, and management must actively enforce information security requirements.

Motivation Factors

Information security must become integrated with job performance and the appraisal process. Personnel become motivated to actively support information security initiatives when they know that their job advancement, compensation and benefits will be impacted. Studies about employee motivation in general have been demonstrating this since the 1920's

(Mayo's, Roethlisberger's and Dixon's, and Landsberger's to name a few). When they do not have this motivation, then an organization is destined to ultimately depend only upon technology for information security assurance. "But we can't do that! HR would never go along with making security a part of the appraisal process!" Of course they will, if you demonstrate the importance of doing will validate due diligence and to be in compliance with laws and regulations. Much research has been done job motivators, and many theories abound. Good managers want to know how to be more effective with their business efforts, and HR is usually willing to try a motivator if it is well presented and explained. Legal compliance, revenue support and due diligence will make their ears perk up. Establish an ongoing line of communication with your HR and Law areas. They may seem unreceptive at first, but your persistence will pay off.

Organizational motives for information security must support primary business objectives; they cannot be an afterthought or superfluous. For example, information security is necessary to:

1. Comply with applicable laws and regulations
2. Demonstrate due diligence
3. Help prevent loss and thus increase profit
4. Protect the organization from liabilities related to security negligence
5. Enhance and/or support customer and public reputation

So, what are personnel information security motivators? The details will vary from organization to organization. However, at a high-level personnel motivators include at least the following, in no particular order:

1. Complying with laws and regulations
2. Getting a good report following a regulator's compliance review
3. Meeting security requirements during internal compliance reviews
4. Getting the respect and admiration of coworkers
5. Having good relationships and interactions with coworkers
6. Doing work that is interesting and fulfilling
7. Following personal, ethical and social principles
8. Reducing information security risks
9. Personally experiencing a security incident or loss
10. Learning the loss experiences of others
11. Showing dedication and faithfulness to the employer
12. Making the boss happy
13. Protecting personal and employer reputation
14. Competing to succeed beyond peers
15. Doing something that is fun and interesting
16. Working conditions
17. Feeling achievement and satisfaction from a job well done
18. Obtaining power and affiliation with others in power
19. Getting good press for the employer for demonstrated effective security practices
20. Avoiding bad press for the employer because security was ineffective
21. Preventing a security incident from happening again after experiencing a security attack or incident

22. Implementing automated security mechanisms that are transparent to the end-user and do not degrade systems performance or slow business processing
23. Making security more convenient than alternative (non-secure) methods
24. Anticipation and receipt of rewards for security activities relative to corresponding job responsibilities
25. Fear and experience of penalties for inadequate security activities relative to corresponding job responsibilities

The last two items in this list are the most powerful motivators to individuals. They relate directly to the human need for safety and security as proven in such models as Maslow's Hierarchy of Needs. They are also the items that organizations can most effectively control. Rewards and penalties are not new ideas; they have been traditional job performance motivators in business since business began, and should be used for motivating personnel to be secure as well. Rewards for information security can include:

- Job promotion and advancement
- New privileges and benefits
- Additional vacation
- Gifts, prizes and awards
- Praise and recognition
- Financial rewards, such as bonuses or raises

Penalties, on the other hand, can include:

- Loss of employment
- Demotion
- Loss of benefits, privileges, or perks
- Salary reduction
- Unpaid leave
- Legal action
- Internal publication of noncompliant personnel

Some of the above may work very well in some environments, but be completely unacceptable, or possibly illegal, in other environments. Always discuss any of the motivators, prizes, penalties and sanctions with Human Resources (HR) and Law departments prior to implementation. It is important to ensure the plans are in compliance with existing laws, contracts and policies, and also ensure the information security department has the support of the legal and HR areas.

Implementing Information Security Motivation

Donn Parker has been extolling the importance of motivation to achieve security compliance for years. I heard him speak a while back about this topic, and he listed some effective steps for implementing an information security motivation program. I don't have his exact recipe for such, but from the notes I took from his presentation I created the following information security and privacy compliance motivation diet that I've used and refined. (Donn covers the previously described topics of motivation factors, in addition to creating his original recipe framework to integrate security into job responsibilities, within his book

Fighting Computer Crime: A New Framework for Protecting Information, John Wiley & Sons, NY, 1998.) Hopefully the following successfully captures the flavor of Donn's original gourmet security instructions.

1. **Make demonstrated due diligence the objective of security.** Yes, risk reduction is the ultimate desired outcome, but it really has little motivational value in and of itself. Personnel demonstrate due diligence by being in compliance with security standards (such as ISO 17799, NIST, etc.), laws and regulations (such as HIPAA, GLBA, etc.), organizational policies, and accepted industry best practices.

2. **Update organizational policies and standards to include documentation of rewards, motivation and penalties.** An organization's security policy must be current, be accepted and supported by stakeholders, and be practical to achieve. It should also document motivators for personnel compliance.

3. **Include security as a specific objective in job descriptions.** Work with management to develop the objectives. Do what applicable labor unions and laws allow. Job descriptions should include specific security assignments that will comply with regulations and policies, and provide accountability for the organization's assets.

4. **Require all personnel to regularly sign an information security and privacy agreement.** State in the contract that the individual will support organizational policies and standards. Require employees to sign the agreement upon initial employment and on an annual basis. This ensures personnel have reviewed the policies and provides accountability for compliance.

5. **Establish security as a specific objective in performance appraisals.** Ensure you have the support of management and unions. This motivator is particularly effective for employees whose job description includes security activities. As Parker notes, "Security must become a part of job performance rather than being in conflict with job performance."

6. **Engage top management to explicitly review the security performance of all managers.** I have witnessed the effects of executive modeling during dozens of office area security reviews. Managers with poor security practices also have direct reports with poor security practices. Managers who model good security practices have direct reports with good security practices. Top-down motivation of managers is necessary to achieve security support through all levels of an organization.

7. **Implement rewards and penalties that are supported and carried out by management.** Once you document penalties, you must consistently apply them to make them effective motivators. Once you document rewards you must consistently grant them to make them effective motivators as well. Keep in mind when establishing rewards and penalties that you should not try to require more security than is necessary for your business circumstances. If you try to "over do" security with no justification behind your requirements, you will not get support from management and your security and privacy efforts will fail.

Yes, motivators are effective when they are consistently applied. I still have vivid memories of the motivators my parents provided when I was a child; such as when I had to pick all the green beans in our very large garden on the Fourth of July in 104 degree heat. If I completed the task, I could shoot off my fireworks and watch the county fireworks display. If I did not complete the task, not only did I get no fireworks, but I would also have to wash the dishes, wash the clothes and clean the house. I picked the green beans. I knew the consequences would unerringly be applied.

Do a little research and observation. Determine the motivators that will work best for your organization and environment. These answers will not come neatly packaged from anywhere else other than from understanding your personnel and organization. Sometimes I think our titles should include "Information Security Psychologists"…understanding motivators and using them to succeed in information security compliance and due diligence is about more than just knowing how to install an IDS or firewall. If one of your resolutions is to have a more successful information security and privacy program in 2004, then you must go beyond technical safeguards and include motivators in your operational information security diet. Then you can ask your employees to pick the security green beans or face the consequences.

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.