Motivating the Workforce to Support Security Objectives:
A Long-Term View

Donn B. Parker, CISSP, RedSiren Technologies, Inc.
<donnlorna@aol.com>

October, 2002

[Based on Chapter 16, "Fighting Computer Crime, A New Framework for Protecting Information," By Donn Parker and published by John Wiley & Sons, 1998]

Introduction

The deadly serious game we play in information security is unfair. Attackers have a great advantage over the defenders. An attacker is intensely motivated to succeed in his one, selected, limited, and focused nefarious effort at a specific time and target and with no concern for collateral damage. The victim organization must require all of their workers, contractors, partners, customers, and suppliers while they are trying to do their many assigned tasks to be alert and defend all vulnerabilities, all assets, at all times, and in all the varied work places from unknown attackers. This is a contest even more lopsided than open warfare where at least the enemy is usually known, and motivation to win is high on both sides. We don't know who or where information attackers are in any specific situation, and we don't know when and how they will attack with what resources and for what purpose. We only know that they are highly motivated to succeed in their attacks on victims while the victims' greatest motivation is to succeed in their own organization objectives. Victims must defend everything of value in fixed, easily knowable locations while attackers only have to attack one thing of value. Motivation is the key to successful attacks and also for good security against such attacks. We must increase the security motivation in our organizations to approach the motivation of our enemies.

We all hate security because of the inconvenience and the constraints it puts on us in performing our jobs. Remembering and using passwords, limiting information we may use, locking doors and computers, and having to use cryptographic protection are bothersome and detract from our work for which we are compensated. A popular approach to improve our information security attitudes and performance is through security awareness programs, but they are relatively ineffective in my experience because we have ignored motivation that is fundamental to making security awareness effective. In fact, awareness programs may result in less security. This may occur as the result of creating security awareness to assist workers to discover ways to avoid security so that they can be more productive in the work for which they are compensated. Management participates by telling their workers to be secure in their jobs while emphasizing and rewarding job performance that supports the positive objectives of profitability, productivity, and growth of the organization.

Job performance motivation in the postmodern workforce is based on the benefits of salary, commission, contractual payments, bonuses, perks, recognition, and job advancement. Loyalty, pride, ethics, and satisfaction of a job well done are the more obscure motives. Workers and management alike know that when job performance and

compensation review time arrives each year, advancing the profitability, productivity, and growth of the enterprise to produce more and better widgets is what counts. The more closely involved an employee is to the objectives of the organization, the higher his or her compensation tends to be. When security gets in the way of achieving these goals, what is likely to happen under these circumstances? People are willing to take a chance, at least in the short run, and security is the loser. It has been this way with safety as well.

A. Padgett Peterson, P.E., CISSP, Senior Security Advisor at Lockheed Martin Information Technology recently made the following comments in the CISSP Web Forum:

> It became clear to me a year ago that part of the problem is that we are designing to the wrong paradigm. United States history (cannot speak for others) is rife with examples that safety does not sell; it is only accepted when a standard or otherwise is required.
>
> Look up the Janney Coupler and the Westinghouse Air Brake [legal cases] for notorious examples from the 1800's. Ever wonder why almost no commercial shipping is registered in the United States? Look at the maritime act of 1915 that came in the wake (or lack thereof) of the Titanic disaster. More recently Ford adopted safety in their 1956 car models. Buyers stayed away. It took laws (Federal Motor Vehicle Safety Standards) before seat belts became mandatory and then air bags were adopted because so few wore the belts.
>
> Computer security is even more arcane because it is designed to prevent/respond to things that are not supposed to happen and are not obvious when they do.

I see poor security in every organization no matter how good the information security staff, awareness program, and technical controls may be, because of the lackadaisical, unsustainable performance of the organization's staff and managers to make the bothersome safeguards and security practices effective. They give lip service to security; they have bursts of security efforts when they are being watched or have suffered a loss, but support ultimately deteriorates for lack of a natural, ongoing motivation in the face of the overpowering pressure of job performance and finding the convenient way to do things. In contrast, computers maintain security, because security is built into their performance (if users and administrators do not tamper with it).

We need to build security into the performance of people as well as into the performance of our computer systems. Some information security experts and human resource managers responsible for work performance review methods complain to me that it can not be done, because security performance can not be measured, yet they are eager to attempt to measure unmeasurable security risks. They complain that managers will not be able to sustain the explicit role of security performance in appraisals of their staffs year

after year because of the pressures of motivating the staffs' job performance that counts directly towards the managers' and organization's success.

Workers view security as being in conflict with their job performance. Employees know that they can increase their performance and receive position and income advancement in their jobs by avoiding the constraints of security. For example, an employee can work faster and better by not making backups, using pirated software, failing to securely store sensitive information, endangering information, and secretly sharing the organization's sensitive information with competitors over the Internet in return for favors. Organizations must remove this conflict between job performance and security constraints by making security a part of workers' job performance. Real progress in security will not be achieved until this is accomplished. The self-interests of job advancement and financial compensation are the primary motivators in employment, and security of information must be included to avoid conflict. Otherwise we will continue to have only cosmetic and superficial security.

Failure of Intangible Risk Reduction as a Motivator

Security awareness is based mostly on the objective of security risk reduction. Subjects of awareness programs are told that their security efforts and security constraints on their work are necessary to reduce the high risk of great losses. However, when awareness is great and effective, then losses don't occur, and awareness is seen as unnecessary. So awareness diminishes until losses start increasing and the cycle repeats.

Risk reduction is self-defeating or at least self-limited. Workers usually see little timely cause and effect. Risk is intangible, and its materialization is not observable except after the fact when it is too late. Workers rarely see that their changed security practices result in any change in unobservable risks. Workers see the effects of their security efforts against high-incidence loss events occurring now such as virus attacks, but virus attacks are certainties, not risks.

In my years of experience with many computer criminals I found that they often start with one attack, encounter different circumstances than they anticipate, and switch to new and different attacks. Workers responsible for supporting and carrying out security discover that the types, frequency, and size of loss described in awareness programs don't happen or are different than actual experience. A calculated risk of one expected event per year may be realized by 9 years of no events and ten events in the tenth year. Probability theory tells us this is the case. Workers also sometimes see that the security they support has no bearing on the kinds of losses that do occur, and they see inconsistencies of intense security in some circumstances and little or no security in others that erodes risk reduction efforts (Why lock the doors but leave the windows open?).

Not only is risk reduction a faulty objective of security because it cannot be measured, controlled, or managed in our imperfect security systems (risk is under the control of our unknown enemies), but it also fails to be effective motivation. Wouldn't it be easier to motivate people by emphasizing a positive and measurable objective of due diligence

with rewards rather than the negative approach of risk reduction? Due diligence encompasses using generally accepted good practices, meeting the requirements of laws and regulations, enablement of electronic business, achieving security effectiveness relative to others' efforts including competitors, and satisfying the demands of customers and shareholders. It is achieved by benchmarking, taking advantage of the multibillion-dollar security products and services industry, and using the current common body of safeguard knowledge and requirements. This is the more rational and tangible objective in contrast to invisible risk reduction [See my article, "Risk Reduction Out, Enablement and Due Diligence In," February 2002 from donnlorna@aol.com.]

Security Motivation Factors

Three important motives of organizations to support security are avoiding and mitigating loss, avoiding negligence, and enhancing strategic business values. We are amenable to being more secure after we have suffered a loss. With increasing use of fragile information technology, however, a single loss can be catastrophic and the accusations of negligence severe. Organization owners also gain peace of mind by having security comparable to the quality found in other similar organizations, and they are increasingly required to meet regulatory, contractual, legal, audit-imposed, and insurance requirements, thus more likely avoiding negligence. And finally, security enhances business, such as providing a strategic advantage over competitors. Support for this last motive has been illusive until recently when organizations started recognizing security as a basic means of enabling business in our postmodern electronic world. The challenge becomes how to impart these motivators to managers, contractors, partners, and workers.

Motivation efforts must take into account the culture of an organization. I have found that each organization, especially a business organization, has a unique culture that has a profound affect on how the organization deals with information security. The culture is determined by many factors including loss experience; interests and experience of top managers; acceptable ethics in the external and internal environments, the role that audit, industrial security, legal staff, and human resources play; the state of the economy, profitability, productivity, growth, and resources available; the scale of security efforts that are possible; and the many policies and practices that are or are not enforced.

Increasingly popular managed security services present an interesting trade off in effectiveness of security based on motivation. The service company's employees are compensated according to their security performance for clients. Therefore, security will likely be of the highest quality. However, the application of most safeguards is still in the hands of their clients' employees and quality of security is still determined for the most part by clients' employees' motivation.

Here are some kinds of circumstances that I have found among workers in any organizational culture that might increase security motivation that could achieve more than current cosmetic, superficial, inconsistent information security:

1) Having basic self-interest to preserve continued employment,
2) currently or recently suffering a known ongoing attack,
3) meeting security requirements during observation by officials,
4) having defenders free of need for security by having unmanned, invisible, automatic and effective safeguards continuously at work without deterioration,
5) finding that the most convenient way is the most secure way,
6) being sufficiently and effectively rewarded and punished in their security efforts relative to the rewards and penalties associated with their other duties.

I find that these security motivations are minimal or fleeting in today's business and government environments (except in the military and defense industries where the organizational objective is security). This is especially true with the threats of having 200 million other Internet users as close as the lock on your electronic front door and who are far less motivated in preserving your security. Employees are working at sites not controlled by their employer and often communicating through insecure networks and wireless facilities. There is a mix of employees and partner employees and contract or temporary workers side by side. Customers and suppliers are using the same computers and networks. Partnering with competitors and peers is more commonplace. Any of these people can secretly and instantly communicate sensitive information to anybody else in the world. Such is the eclectic postmodern world that works against common objectives and motives.

We have little control over the first three motivations described above. Choosing transparent safeguards that people accept or making them more convenient as suggested in the fourth and fifth items meets one of the principles of good safeguards and should be practiced, but this has little effect on security over all. An effective safeguard that is invisible or transparent to those that are protected by it or making a secure method among alternatives the most convenient require no security motivation for their effectiveness. One example is having well designed cryptographic capabilities with automatic key management where the users don't need to know it is in place and functioning. A safeguard that must have the cooperation of the people constrained by it for it to function effectively requires continued and persistent efforts to motivate them appropriately. Otherwise, these people are likely to neutralize its effectiveness, or even worse, neutralize it but make it appear effective. Necessary information security that can not otherwise be made transparent can be made easier to endure if we can find ways to minimize the constraints. However, there are severe limits on how far this can be carried out, and we are left with the need for security motivation.

An extreme example of creating motivation would be to require an employee or, more practically, a contractor to pay a deposit or bond to indemnify the employer against loss from the individual's acts. This may be acceptable in some contracting, but it is unacceptable in employer/employee relationships.

We are left with using rewards and penalties in the sixth item previously listed to go beyond convenient security. Military and criminal justice organizations that have the most experience with the highest levels of security seem to have learned that a rewards

and penalties approach is the best means of motivation, but they have the advantage of security as the primary organization objective that associates rewards and penalties directly with the goals of their organization. Governments explicitly pay defense contractors to implement security and audit and measure their compliance. When security is a secondary objective as it is in other organizations, security motivation efforts also will likely be secondary. I call efforts to stimulate this last motive based on rewards and penalties the mother of all security controls, and I address it in detail here.

Motivation Enhancement

An organization that is truly dedicated to security will recognize the need for motivation beyond mere security awareness and should develop an effective security motivation program along with or as a part of a continuing awareness effort. It should employ the following worker motivators:

- Anticipation and receipt of rewards
- Fear and experience of penalties
- Ethical, honest, social, and good business convictions
- Personal loss experience
- Others' loss experience
- Gratefulness and dedication to employer and profession for continued employment
- Protection of personal investment in effort, money, or other assets
- Protection or furtherance of personal and employer's reputations
- Competitive desire to excel beyond peers
- Expediency and convenience.

The first two motivators, rewards and penalties, are the only ones that are controllable and are the most powerful. These are the traditional job performance motivators in any employee/employer, contractual, or partnering relationship. Why not use them for motivating security as well?

Rewards usually involve job advancement, praise and recognition, financial remuneration (often in the form of specific bonuses for exemplary behavior). Rewards could also be prizes for exemplary security performance--for example, winning a competition among groups for the fewest guard-reported or auditor-reported security lapses or for the highest number of continuous days without a lost-time incident. Rewards could include recognition plaques to hang in offices, additional holiday time, TVs for rest break rooms, or special car parking privileges.

Penalties, or more generally, sanctions often involve loss of favor, perks, position, or remuneration, though organizations use other penalties as well. One group manager publicly posted the name of anybody who revealed his or her password and required everyone in the group to immediately change their passwords. This produced peer pressure to keep passwords secret because nobody liked having to learn a new one. Leave without pay, dismissal, and legal action would be the severest sanctions.

Implementation of a Motivation Program

The organization should do the following based on rewards and penalties to satisfy the fundamental need for security motivation to succeed in protecting assets.

- Change the objective of security from intangible and faulty reduction of risk (with little motivational value) to achieving due diligence by meeting standards (e.g., ISO17799 and BS7799), regulations, laws (GLBA, HIPPA, privacy), good practices (ISF Standard of Good Practice), business enablement, and the safeguards and practices used by other well-managed organizations under similar circumstances (unless there are prudent reasons that are agreed upon and documented for not doing so).

- Develop or update organizational policies and standards and offer guidance and resources to help members of the organization implement and maintain adequate security of the organization's assets. Organization security policy must be current, tolerable to stakeholders, and practical to achieve worker acceptance.

- Establish security as a specific objective in job descriptions, to the extent that management and labor unions allow. If management resists universal application of this practice, first implement it on a limited basis for some job descriptions. Job descriptions should include specific assignments to avoid endangerment of assets and to adhere to policy, and protect and be accountability for the employer's assets including information.

- Periodically require members of the organization and its contractors to sign a security agreement supporting the policies and standards. Some organizations require employees to sign a security agreement upon initial employment and on an annual basis. This is an excellent way to achieve accountability, because it recognizes that the members of the organization and contractors as well have reviewed the policies and will be held accountable for their execution. Agreements could also include nondisclosure of trade secrets, a code of ethics, or privacy issues. In banking security agreements are popular tools at the officer level. Lower level employees are usually not required to sign such agreements, although they should if their duties involve high trust stewardship over assets. The increasing use of small, powerful computers and distributed computing throughout the organization and among other stakeholders makes this increasingly important. Organizations may be more likely to require these security agreements with outside consultants and contractors, assuming that the employee agreement stipulating adherence to the organization's policies will cover their own employees. (For more on this subject, see Charles Cresson Wood's "Annual Compliance Agreement Signatures," in *Computer Security Alert Newsletter* of the Computer Security Institute, July 1994.)

- Establish security as a specific objective in periodic performance appraisals to the extent that management and unions support it. Implement this for members of the organization whose job description requirements include security elements.

Measurement can be accomplished using the factors listed below. Approach and attempt to gain support from the human resources or personnel department to add security accountability as an explicit work objective with rewards and sanctions. Alternatively, add security accountability as an explicit work objective with rewards and sanctions for a part of the organization as a pilot effort to be expanded later to other parts of the organization. Annual job appraisals should include specific evaluations and discussions of the employees' support for and practice of security including references to any exemplary efforts and violations and endangering information.

- Obtain support from top management for explicitly reviewing the security performance of all levels of managers. Top down motivation of managers in their job appraisals is crucial for achieving support for security and their sincere emphasis of it in the appraisals of their staffs. Employees will generally follow the lead of their managers who must be role models for good security.

- Specify a program of rewards for exemplary security performance and penalties for inadequate performance and implement it to the degree that management supports this program. Rewards could include plaques or desk ornaments, public recognition (photos and articles in organization newsletters), prizes, parking spaces, bonuses, job advancement, and remuneration increases. Penalties could include loss of computer privileges, penalty hearings conducted by appropriate members of management or an employee committee, change of password, loss of employment privileges, loss of remuneration, criminal arrest, and civil litigation. Explicit rewards and penalties must be consistently and fairly applied.

Managers should consider a number of factors in evaluating security performance in annual job or contract performance appraisals:

- Specific actions precluding and mitigating information-related losses,
- faithfulness and effectiveness in performing security assignments,
- rewards and awards for exemplary security performance,
- security violation citations received,
- commendations and criticisms received from others,
- reporting suspected vulnerabilities and loss incidents,
- effective safeguards being used such as anti-virus scanners,
- suggestions volunteered for improvements of security,
- attendance at training and awareness presentations,
- possession of and familiar with up-to-date security documents, and
- knowledge of the content of security policies and documents.

In many appraisal procedures, the process begins with managers stating their expectations, and employees stating their claimed performance relative to previously agreed upon goals. This is followed by the appraisal and establishing new goals. For security appraisal, there should be a general requirement on protection of organization assets, identification of specific assets to be protected, safeguards to be maintained and

new practices or modifications of practices to be made. This requires clear identity of owners, providers, custodians, and users of the assets and safeguards. Those who own or operate safeguards must be differentiated from those who are constrained by the safeguards for managers to know how to hold workers accountable.

The inclusion of security in job appraisals throughout the whole organization may be an excessive cultural change. In this case a useful tactic is to develop the job description and limited appraisal practices and apply them on a pilot or trial basis in only one or a few ideally suited organization units before rolling out complete practices to larger numbers of units. Management could start with IT and surely the security department to demonstrate the viability of the experiment (proving the value on a large scale could be far more difficult and would require expensive psychological studies). Security specialists in any organization should be the first to have security job performance incorporated into their reviews. They possess much of the sensitive information (information about the protection of sensitive information) and have sensitive duties. This security of security requires exceptional security motivation and awareness.

Do not try to advance security beyond the level of acceptance of stakeholders. Otherwise, they will defeat security efforts. I have experienced significant resistance in attempting to institute security in job descriptions and appraisals, and I do not know of any organizations, other than military and criminal justice organizations (where security is the goal), that successfully carry out this crucial motivational practice. However, I conjecture that there are a few.

In many cases the resistance comes from the human resources (HR) departments in organizations. HR usually strives to keep the appraisal process from being diluted with too many evaluation subjects and especially those that have less tangible means of performance measurement such as security. In one response to my plea, an HR manager said that security should be treated the same as non-smoking, using the Internet and telephones for personal purposes, and parking regulations. The rules are posted, and if you do not follow them, you suffer penalties up to the severest one of losing your job. The reward for obeying the rules is that you get to keep your job. He failed to see the significance of information security for the organization, its strategic value, and possible conflict with other job performance. We need top management support to convince HR and line managers to incorporate security in the ways that I recommend providing both rewards and penalties. These motivational efforts should be the objectives of security plans presented to top management through the chain of management until they are achieved.

Some Ideas for Security Promotional Efforts

First be sure that security promotional efforts are consistent with and ideally a part of other promotional, training, and human resources efforts and practices within the organization. You shouldn’t fight the battle on more than one front at a time.

Here are some additional security promotional efforts that some organizations have found effective. Some organizations have an annual information security promotion week. Others argue that this causes people to ignore security during the rest of the year. One HR manager believes strongly in a clean desk practice at the end of each workday. If the security monitors find any nonpublic company document exposed on an employee's desk or a computer that is still logged on, that employee must pay a visit to the HR Manager and explain how it happened.

There are some security promotional efforts that users deride and take as bad jokes. These have negative effects on security efforts. Videos are especially vulnerable to being trite and should be carefully selected to match the type of audience. Because of so much commercial TV viewing, people's standards of acceptable filmed training material are very high. Soap opera episodes in training videos loaded with unrealistic concentrations of obvious security violations and their solutions are the worst offenders. You must also approach sophisticated employees such as researchers and engineers differently than accounting clerks and factory workers. Less sophisticated workers desire and need detailed rules to follow, while more sophisticated professionals want general principles to apply as they see fit.

A security newsletter or a section of a general organization newsletter published by the information security unit and sent to people in the organization concerned with information security presents an image of a sustained and supported function. Receiving the newsletter could be considered a status symbol and has motivational value. For example, when a specialized newsletter is sent to security coordinators, it imparts special knowledge giving the recipients an inside track advantage over their peers and employees who are under their security care. It also provides the medium for announcing the results of employee award programs for exemplary security performance. For example, one company awards the outstanding security coordinator each year with a check for five hundred dollars or a TV set at the annual company information security conference.

The posters used in one company convey the security message in text, graphics, and cartoons in color and black and white form printed on 8.5"x11" size (A-size paper in Europe and Japan) poster board and heavy paper. This is an ideal size for gaining attention on bulletin boards and sending through the mail. They are often printed in wall-poster size as well for viewing at a distance. It is important that they not be displayed for too long and become commonplace and ignored or become too familiar and annoying. For example, Chris Aivaizian, when he was manager of information security at a large bank on Long Island, ran a poster design contest that drew added attention to his posters mounted in elevator waiting areas. A removal date printed at the bottom of posters may be useful. The equivalent of posters in electronic form through logon banners, screen savers, Web sites, and email message trailers may become the conveyance of choice especially with such diverse locations of workers in our postmodern age.

Use of a cartoon character, a logo, or distinctive design carried throughout all promotional materials is useful to maintain continuity of the subject matter. However, this can become excessive and have a negative impact as well. Publishers of this type of

material should survey their constituents periodically about their acceptance of and attitudes about the materials being used. The timing of publication is important relative to the timeliness of the subject matter covered, e.g., a new virus problem, or tying into other promotional efforts such as an annual information security week.

Referencing new technology in security motivation and awareness messages is important to increase interest in security. For example, the word "key" as used in "The Key to Security" is becoming important as cryptography with secret and public keys comes into use. The use of new terms such as software piracy, cybercrime, cyberterrorism, and firewalls are opportunities to use new jargon, themes, and plays on words to generate curiosity and attention. Always include security as a feature in every new information technology product or service introduced into the organization. The extension of the elements of security from the limited and incorrect CIA paradigm to confidentiality and possession, integrity and authenticity, and availability and utility provides another opportunity to advance more comprehensive awareness. Don't limit descriptions of types of losses to DDUM (disclosure, destruction, use, and modification). More different types of losses occur such as observation of confidential information, endangerment, and stealing. Use general terms such as abuse and misuse rather than violation of CIA. Don't use criminal terms such as fraud, theft, or burglary unless you are addressing law enforcement issues. I have previously recommended avoidance of references to faulty security risk reduction that cannot be proven. Workers will not respect providers of haphazard, incomplete, and incorrect lists and terminology.

In one of my client assignments I found that smart card authentication was introduced into a large bank in one division of 5000 workers as a pilot project. Management watched it closely. After about a year, the workers became disenchanted with having to present the cards to use computer resources. Contrary to the published risk assessments of annual loss expectancy, they complained that there had been no unauthorized computer usage events that they were aware of before the test and there were no attempts to cause harm after usage started. Nothing had changed except the additional burden of safekeeping and using the cards. There was significant worker pressure to eliminate use of the cards until the bank introduced other uses of the cards such as parking garage access and charging for food in the cafeteria. The addition of the conveniences quieted the complaints.

Side Bar
An Example of Poor Motivation
A good example of poor motivation in action is the enactment by the U.S. Congress of the Computer Security Act of 1987 (Public Law 100-235). This poorly constructed legislation requires each government agency to have a documented security plan for every computer that processes sensitive but unclassified information (Section 6), and every civil servant who handles sensitive but unclassified information to receive training in computer security. The stated objectives are "to enhance employees' awareness of the threats to and vulnerability of computer systems and to encourage the use of improved computer security practices." These requirements, however, carry no specific sanctions or rewards, and

consequently they have probably brought little or no advance in security, yet have wasted huge amounts of resources and money (according to the General Accounting Office's many agency security reviews).

During the hearings on the Computer Security Act bill, I wrote letters and visited the House of Representatives committee, urging them to introduce the additional motivational provisions that would make the requirements work. Committee staff members reassured me, saying that the Office of Personnel Management would add the motivational aspects. Those provisions that would include security in job performance criteria were never included in the bill. Therefore, they were never implemented, except possibly in the Department of the Treasury where security was added to job performance reviews. The Act is still in effect and its congressman author continues to praise it, in spite of its sad record. Business in general shares this failing of applying security only cosmetically because job performance appraisals do not include it.
End Side Bar

No matter how good the promotional materials and training are for awareness of the need for security, it is not enough without the motivation of every person in a position of trust to protect the assets of the organization. (See Dr. Mich E. Kabay's paper "Social Psychology and Infosec: Psycho-Social Factors in the Implementation of Information Security Policy." He provides an excellent guide and includes thirty-five recommended actions, and he recommends limiting organization cultural changes to small incremental steps. This paper won the best paper award at the 16th U.S. National Computer Security Conference, sponsored by NIST and NCSC in 1993.)

Conclusion

Unfortunately, positive security performance is seldom rewarded, whereas security failures are more often punished. This results in a negative, one-sided reinforcement. To be effective, motivational tools, rewards, and penalties must be consistently, fairly, and evenly applied for a significant period of time. If nobody is ever sanctioned or rewarded, or if this occurs only sporadically, the motivational value is lost. Rumors of failure to take management action may travel faster than the news of effective actions. In addition policies and standards that are not carried out represent severe security vulnerabilities themselves and should be periodically reviewed, and un-enforced or unused policies should be eliminated. Security must be motivated with both real rewards and real sanctions liberally applied. This can be done effectively through periodic job performance appraisals.

Workers and contractors know that observing security measures likely will inhibit their ability to achieve work objectives specified by management. Without security constraints, they believe they could devote more of their energies and be freer to advance the work that furthers the organization's objectives and rewards them with increased income, position, credit, and satisfaction. Many losses that would motivate the need for security

are so rare and unpredicted that they fail to motivate, at least not for long. How motivated will workers be to carry out security measures especially in postmodern times of workers in so many different roles, locations, and relationships? The only hope for security is to make it and its enforcement a part of each organization's and employee's work objectives, encouraged in a fundamental way with rewards and sanctions. Security will not advance and security awareness efforts will continue to be ineffective without an integrated and complete solution to the motivation challenge.

Appendix

I sent the following message to the Human Firewall Council:

To Info@humanfirewall.org (www.humanfirewall.org)
From Donn Parker, Feb 26, 2002

[Objectives of the Human Firewall International Council: This site is part of an international education campaign to improve information security awareness by focusing on the human issues involved. The Human Firewall Web site strives to help managers and employees in all kinds of organizations increase their information security awareness, and promote behavior that will improve protection of critical information against internal and external threats. (members include Charles Wood, Oivind Hoxiem of Statoil, and Darrin Shepherd of Fidelity, and many others in the U.S., Great Britain, Canada, and other countries)]

I commend you for your Human Firewall Manifesto efforts to emphasize the human element that I have emphasized for 35 years in this field. However, I take exception to your emphasis on awareness and total disregard for motivation. Awareness simply teaches people what they need to know to avoid the security and its constraints that we all hate so much and that interferes with our job performance.

You mentioned motivation only once in an obscure way in an example in your Manifesto: "a developer may be working furiously to meet a deadline for deploying a specific application---with a bonus attached for making the deadline---but have no incentive or motivation to ensure the application is secure before going live." Motivation to support security is necessary for awareness to become effective.

Employees don’t like security. How do you motivate employees to do things they don't like? Through financial rewards and penalties, recognition, perks, and job advancement just like other unnatural employment requirements such as being punctual and recordkeeping. Security must become a part of job performance, not be in conflict with job performance to achieve more than cosmetic and superficial security.

Security risk reduction is the common objective for most security programs in organizations. Unfortunately, this negative objective often works against developing a positive motivation for good security among security stakeholders. Motivation based on risk reduction comes from negative consequences of a loss event: “If you don’t support

good security practices, the organization will suffer the consequences." When negative consequences are frequent and a certainty such as computer virus and worm attacks, the constant reminder produces the desired motivation to use antivirus software and be cautious. When negative consequences are infrequent, such as with espionage, people relax security to concentrate on other more productive practices: "Who would want to steal information from us?" In many cases it is not even prudent to inform all stakeholders of loss events. The objective of reducing risk requires them to take actions and be continually alert to prevent bad things from happening that don't happen very often. You must frequently scare people enough to make them practice security in a risk situation. When loss events don't happen for awhile, complacency sets it.

Most people don't understand the probability theory behind risk. They often don't realize that the probability of a loss event of once every year is the same on the first day of the year as it is on the last, and when it doesn't happen in a year or even several years, doesn't mean it won't happen today. "The risk reduction approach to good security means that losses don't occur, and when losses don't occur, who needs security?" Reducing risk of loss is materialized only by changing predictive numbers in reports when no loss experience changes occur or when loss experience is different than predicted. Loss experience of other organizations often is not relevant because the circumstances are different and because of the natural attitude that, "it won't happen here."

The alternative security objective of due diligence and business enablement has far more, positive potential for good motivation. Rewarding due diligence, not just unpredictable risk awareness, is the secret kept far too long.

See my book, "Fighting Computer Crime," for details on how to do this.
END