Enforcing Compliance with Information Security Policies: Incentive Structure and a Penal Code Mechanism

1. Problem Scope and Motivation

Development and proliferation of new networking technologies and interdependent ways of conducting business with business partners is making it more difficult to secure the information systems that companies possess. Traditional well-defined security perimeters are becoming more spotty and porous as companies are forced to open their networks to business partners. This issue is further complicated by the growth of collaborative technologies, virtual teams and outsourcing. In collaborative environments, due to their distributed and heterogeneous nature, compliance with security policies becomes a huge challenge (Smith et al, 2006). Gartner Research argues that threats to extended enterprise are expected to increase, as outsourcing to offshore companies in countries with often weak or unenforced intellectual property and privacy laws becomes more common (Wheatman et al., 2005). In these conditions, compliance with information security policies becomes hard to enforce by legal or administrative means. Therefore, technical or economic tools must be developed and used.

However, the effectiveness of technical tools in enforcing security compliance is not clear. On one hand, an average of 11.9% (and up to 25%) of IT budgets is spent on compliance initiatives (Ponemon Institute 2011), and many companies are providing automated compliance solutions (e.g., Symantec, Open Text, etc.). Still, even these solutions do not provide complete security from security events that occur on daily basis. Majority of spending in the technical solution remains in the tools that help in “keeping the bad guys out” – firewalls, antivirus, anti-spam, etc. (Browning 2006). However, the demands of business operations in the world of fuzzy security perimeters are more along the lines of “letting good guys in” paradigm, allowing customers and partners to connect as needed to corporate networks. The question of who to allow such connection privileges and how to make sure that the "good guys" do not turn "bad" goes beyond technical solution into the area of social, economic and behavioral mechanisms. In other words, a shared belief is developing that information security is not solely a technology issue but should involve economic and behavioral considerations (Vijayan 2005). Note that access to sensitive data and computing infrastructure is an issue even when a firm does not extend its operational business environment beyond its traditional boundaries. A recent survey shows that 12% of IT users admitted to knowingly violating security policies to get their work done (Fiberlink 2010), while various reports attribute between 4% and 40% of all security incidents to the acts of insiders – ignorant or malicious (Verizon 2012, PriceWaterhouseCoopers 2010).

When it comes to social interactions involving information technology, it is important to understand that different entities have different and often conflicting goals and interests. While these issues are not new[1], they are becoming even more emphasized in the context of information security. Higher levels of information security generally restrict the ability of users to follow flexible operation routines, and may be perceived as counter-productive. For example, Perry (1991) identifies multiple trade-offs in systems reliability, including integrity vs. efficiency, usability and portability of systems. Such trade-offs play important role in forming perception about the true value of information security systems and resulting behavior of people and organization entities, potentially leading to non-compliance with security policies. Overall, the incentives of agents in information security interactions often leads to deterioration of security; for example, software manufacturers often have incentives to introduce new products as early as

[1] For example, Gurbaxani and Kemerer (1989) consider different goals and conflict between MIS and other functional departments

possible, while there are still many bugs that have to be patched later (Arora et al. 2006). Since incentives of agents are often misaligned, designing such incentive mechanism for information security becomes a challenge.

In this paper, we show that compliance with security policies may be enforced even for myopic, self-interested, agents by providing them proper economic incentives for compliance. We consider a game between an *organization* and a representative internal *user* of its security system, and show how compliance may be achieved with the help of two different approaches – namely, providing bonuses for compliance with security policies and imposing fines for lack of compliance.

Issues of providing incentives such as bonus and fines fall under a general umbrella of principal-agent problem and have been looked at in several fields, but the results remain inconclusive. For example, Sandmo (2002) argues that provision of bonuses in public sector is not always a right incentive. Conrad and Wang (1993) consider a subsidy\tax combination to regulate environmental emissions, but find that in many cases behavior of such schemes is ad hoc. Strand (1994) proposes a bonus and fine scheme to prevent environmental accidents and finds that the optimal configuration of such a scheme depends on the weights of individual and social welfare as perceived by society. A similar result is shown by Nault (1996) in terms of equivalence of taxes and subsidies as the policy tools that help control negative production externalities.

Comparison between bonus and fine incentive approaches has also received recent attention in the field of experimental economics. Several reports indicate potential conflict between controlling and controlled parties. While fines are favored by the principals, they have largely a detrimental effect on the agents (Gatcher et al 2006). On the other hand, use of certain performance-based incentives (such as fines) tends to lessen the individuals' desire to cooperate in the long run, as it signals distrust (Ellingsen and Johannesson 2005).

We explore the relative benefits and dynamics of incentive schemes involving bonus, fine or their combination in a variety of setting – from a one-shot simultaneous move game to repeated games to sequential games with uncertainty. The remainder of this paper is organized as follows. In Section 2, we develop a game-theoretic model in which a bonus and\or a fine is offered for compliance with security policies and illustrate that compliance is hard to sustain. In section 3, we develop an extension of the model – a penal code model. We show that a repeated game perspective is one way to enforce compliance with organizational security policies and derive conditions necessary to insure compliance using bonus, fine and combination of both. We conclude in section 4 with a discussion of our main results, their applications and directions for future research.

2. Role of Trust (Assurance of Future Interaction) as a Consideration of Incentive Design

Security-related interactions rarely take place just once. Real-world organizations periodically monitor their partners' behavior and change its own security policies to adapt to new threats and solutions. In order to develop a formal analysis of repeated interactions between the user and the organization, we consider an infinitely repeated game. At every stage of this game, the user and the organization play a one-shot compliance game. In the following paragraphs, we will provide a detailed analysis of the bonus-only game, and then show how it extends to encompass the cases of fine-only and bonus-fine incentive schemes.

First, let us develop a game theoretic model for a situation where an *organization* wants to ensure that its users comply with its security policies. Lack of compliance by the users increases the organization's exposure to security breaches, resulting in expected losses of z

dollars. This amount can be envisioned as the amount that the organization has to reserve to implement additional security measures or to be prepared to use this money in clean-up and repair activities after a security breach. We assume that non compliance with security policies always leads to organization suffering a monetary loss (*-z*). On the contrary, in case of the user compliance with security policies security risks are countered and the organization can re-deploy previously reserved resources. Therefore, in this case the organization experiences a gain of *z* dollars.

For a given user[2], however, compliance with security policies is costly because it requires commitment of additional monetary and human resources which ultimately may reduce its own productivity. We represent the cost associated with compliance to security policies as *c* dollars. The users may not see immediate ways to redistribute increased protection to everyone, i.e., they anticipate no direct gain from improved security. However, when users do not comply with security policies, from a myopic perspective, there is no cost of non-compliance with the organization's security policies.

Because of the conflicting interests and different perceptions of value for security, the organization may need to offer additional incentives to the user to ensure compliance with security policies. We can now formally define the compliance game between a user and an organization. In this section we assume that the organization and the user are in a single-period simultaneous move game. The user may choose to comply with security policy at cost *c* or not to comply at zero cost; its strategy set can be represented by S_u*=(Compliance, No Compliance)*. The organization, on the other hand, may choose to provide bonus of *b* to the user for expected compliance or no bonus if it expects non-compliance; therefore, its strategy set can be

[2] This may be an individual employee, structural unit of a company or its business partner. We focus on the relationship between formal entities (departments, firms).

represented by S_o=*(Bonus, No Bonus)*. To ensure individual rationality, we require that double inequality $c<b<z$ holds, i.e., bonus received by the user must exceed its cost of compliance; however, the bonus cannot exceed the benefits retained by the organization. We can then represent the *payoff vector*, $S_o \times S_u \rightarrow \mathbb{R}$ in the Normal form game between the user and the organization as follows (payoffs of the user; payoff of the organization):

Org. The user	Bonus	No Bonus
No Compliance	$+b-d; -z-b$	$-d; -z$
Compliance	$+b-c; z-b$	$-c; z$

Players' payoffs in a repeated bonus-only game are accumulated over time depending on the outcome of every single-stage game. Once the cumulative payoffs are considered, we can show that there are possibilities for players to achieve mutually beneficial outcome (*Compliance, Bonus*). To account for future payoffs, we introduce a "time value of money" factor g ($0 < g < 1$). From the perspective of period t, one dollar received in received now is worth \$1, one dollar received in period $t+1$ is worth $\$g$, one dollar received in period $t+2$ is worth $\$g^2$, and so on. Thus, the payoff from the game becomes a sum of the geometric progression depending on g. The question of interest is whether there are some values of the factor g that can help to achieve the desired outcome (*Compliance, Bonus*) as an equilibrium of a repeated compliance game.

One way to analyze infinitely repeated games is to consider so called Nash reversion or trigger strategies (e.g., Friedman 1971, Furusawa 1999). Let t be the current period of the game (i.e., it has already been played $t-1$ times). In Nash reversion strategy, both players will choose mutually beneficial outcome (*Compliance, Bonus*) in current period t, if both of them played this strategy in previous period $t-1$. If one of the players deviates from this choice in the current period, in period *t+1* the opponent will start “punishing” this player by forcing the mutually inefficient outcome (*No Compliance, No Bonus*) thereafter.

To see if a particular strategy combination is an equilibrium, we need to check if any player has an incentive to deviate from the equilibrium path. For a rational, value-maximizing, player this incentive is a higher payoff from deviation strategy. In our game, incentive to deviate from (*Compliance, Bonus*) outcome is potentially present to both players. For example, the user may choose to play the *No Compliance* strategy in hope that the organization will still provide the *Bonus*; in this case, the user will receive the bonus, *b*, without taking any effort at all. Similarly, the organization can choose *No Bonus* strategy hoping that the user will still choose *Compliance*; in this case, the organization keeps all the benefits of increased security *z* without having to pay the bonus to the user. However, it is plausible to think that the opponent will be unhappy about such actions and will play only the Nash equilibrium strategy in the future (since it is the best response to opponent’s equilibrium strategy).

Since both players move simultaneously and do not know the opponent’s strategy in advance, deviations from the established path of the game are possible for both players. In making decisions about which strategy to pursue in the current period, players will compare two streams of payments after period *t*: one with stable payments associated with (*Compliance, Bonus*) outcome; another with a higher “deviation” payment in period *t*, but lower, inefficient payments from (*No Compliance, No Bonus*) outcome thereafter.

First, consider the strategies and payoff for the user. If she does not deviate from the *Compliance* strategy, then the (*Compliance, Bonus*) outcome occurs infinitely, and her payment stream is:

$$(b-c) \cdot (1+g+g^2+g^3+\ldots) = (b-c)/(1-g) \qquad (1)$$

If she deviates and chooses the *No Compliance* strategy, then (*No Compliance, Bonus*) outcome occurs once, giving the user a single-period payoff of *b-d* instead of *b-c.* In the next period, the organization does not believe in good will of the user any longer, and plays *No Bonus* strategy infinitely. The user's best response to the organization's anticipated strategy is *No Compliance*, and her payment stream is:

$$b-d + (-d) \cdot (g+g^2+g^3+\ldots) = b-d/(1-g) \tag{2}$$

Therefore, the user has no incentive to deviate from *Compliance* strategy if her payoff from deviation is too low:

$$(b-c)/(1-g) > b-d/(1-g), \text{ or } g > (c-d)/b. \tag{3}$$

Thus, as the user's cost of implementing high security is close to the amount of the bonus, she will prefer the *Compliance* strategy if sustainability of future payments is high.

On the other hand, from the organization's perspective, payoff from non-deviation and infinitely repeated (*Compliance, Bonus*) outcome is:

$$(z-b) \cdot (1+g+g^2+g^3+\ldots) = (z-b)/(1-g) \tag{4}$$

If the organization chooses to deviate from the *Bonus* strategy, then the outcome (*Compliance, No Bonus*) occurs once, giving the organization a single-period payoff of *z* instead of *z-b.* In the following periods, the user reverts to playing the *No Compliance* strategy, thus forcing the organization to play the *No Bonus* strategy. Therefore, the organization's payoff from a single-period deviation is:

$$z + (-z) \cdot (g+g^2+g^3+\ldots) = z\cdot (1-2g)/(1-g) \tag{5}$$

Therefore, the organization will not deviate from the *Bonus* strategy if the payoff from deviation is too low[3]:

[3] Technically, from previous inequality, deviation brings negative profit if g > ½. However, since b < z, this inequality also includes the case g > ½.

$$(z-b)/(1-g) > z\cdot (1-2g)/(1-g);\ or\ g > b/2z \qquad (6)$$

Therefore, as the amount of bonus increases compared to the organization's value of additional security, it will not deviate if sustainability of future payments is high.

The analysis presented above indicates that higher level of security can be achieved if both players are sure that future payments can be sustained. This is an interesting implication that is not apparent in the initial problem formulation: *for security to be provided at higher level, the parties need to be assured that their relationship will be continued in the future.* Therefore, building trust is very important. One example of how trust building may occur in reality is building a sense of job security in employees, so that they have a lesser incentive to expose a company's confidential data.

It is also worth noting that in our setting, deviation from the *Bonus* strategy for the organization has negative payoffs for any $g>½$. However, deviation might still be a better option for the user if the amount of the bonus payment is close to the cost of opting for higher security. Thus, subjectively, the user's incentives for deviation from the *Compliance* strategy seem to be stronger, and we expect to see more attempts to breach a contract of compliance on the side of the user rather than the organization. However, it is possible to find a range of bonus values that makes the outcome (*Compliance, Bonus*) optimal for the user as well as the organization. This result is presented in Theorem 1.

Theorem 1. **(Characterization of feasible bonus amount for the bonus-only game)** *Suppose that providing a bonus in the amount of b is feasible. Then, if the choice of reward b is inducing incentive compatibility (voluntary adherence with security policy), it may be characterized as follows:*

$(c-d)/g < b < 2zg$

Proof.

The assumption of incentive compatibility implies that there is no need to deviate from equilibrium outcome for either the user or the organization. Thus, conditions (3) and (6) hold. Rearranging those inequalities and combining them, we obtain

$$(c-d)/g < b < 2zg. \tag{7}$$

Since reaching an exact value at any end of this interval creates an indifference condition for one of the parties involved (and, thus a non-zero probability of deviation), we need to use the upper/lower bound notation for the feasible set of values of *b*. Still, actual values of *b* may be infinitely close to the ends of intervals without violating feasibility.

Q.E.D.

The incentive compatibility for a player occurs when this player has no incentives to deviate from the (*Compliance, Bonus*) outcome of an infinitely repeated compliance game. Corollary 1 shows that there is a value of time value of money factor *g* that guarantees incentive compatibility for both players.

Corollary 1. **(Existence of guaranteed discount rate that induces incentive compatibility).** *Suppose that providing a bonus is feasible. Then, there exist a lower bound on time value of money factor g that induces mutual incentive compatibility. This critical value of g is* $1/\sqrt{2}$.

Proof.

If provision of bonus is feasible, then double inequality (7) holds. From it, we can write that

$$(c-d)/g < 2zg, \text{ or } g^2 > (c-d)/(2z). \tag{8}$$

However, by construction, *c* is smaller than *z* to induce feasibility and *d* is smaller than *c*. Thus, *c/(2z)* < ½ . Substituting this result into (8), we conclude that *all* time value of money factors that satisfy the inequality $g^2 \geq$ ½ (or, equivalently, $g \geq 1/\sqrt{2}$ *)*, automatically induce incentive compatibility. *Q.E.D.*

It is possible that *some* values of g^2 below ½ (i.e., $g < 0.707$) still induce incentive compatibility, however, a value of $g \geq 0.707$ guarantees users' compliance with security policies. Note that these values of *g* suggest a reasonably large range of practically useful values[4]. since it is common in net present value analysis to use the discount rates in the range of 0.01-0.20 (corresponding to g values of 0.80-0.99) which is contained in our interval. A natural question is whether use of a fine instead of a bonus or in combination with a bonus influences the outcome of compliance game in a repeated game setting. Surprisingly, the structure of equilibrium results is very similar in both of these cases.

First, let us consider fine-only incentive mechanism. The payoffs of this game are the following:

Org. The user	Fine	No Fine
No Compliance	*-f-d; -z+f*	*-d; -z*
Compliance	*-f-c; z+f*	*-c; z*

In this case, our goal is to achieve an outcome (*Compliance, No Fine*) as a sustainable equilibrium of a multiple-period game. As before, there is potential incentive for the user to play a *No Compliance* strategy in the hope that the organization will not impose a fine in a given game period. Similarly, the organization may want to impose a fine on the user in a hope to increase its payoff. However, both of these actions will be punished in subsequent game periods as the outcome (*No Compliance, Fine)* will be chosen by rational players.

If the user chooses the strategy of *Compliance,* her payment stream is:

[4] Note, again, that the organization has no incentive to deviate for any g > 0.5. Thus, operating in the range of g > 0.707 assures that both The user and the organization have no incentive to deviate.

$$(-c) \cdot (1+g+g^2+g^3+\ldots) = (-c)/(1-g) \qquad (9)$$

If she chooses *No Compliance* instead, she will not have to pay the cost *c* once, but will be punished by the fine *f* at every game stage afterwards, generating a payment stream of

$$-d + (-f-d) \cdot (g+g^2+g^3+\ldots) = (-d-fg)/(1-g) \qquad (10)$$

Therefore, the user will have no incentive to deviate from *Compliance* strategy if her payoff from deviation is too low:

$$(-d-fg)/(1-g) < (-c)/(1-g), \text{ or } g > (c-d)/f \qquad (11)$$

Similarly, the organization's payoff from non-deviation from an infinitely repeated (*Compliance, Bonus*) outcome is

$$z \cdot (1+g+g^2+g^3+\ldots) = z/(1-g) \qquad (12)$$

while the payoff from a deviation – imposing a fine on the user – will be

$$z + f + (-z+f) \cdot (g+g^2+g^3+\ldots) = z+f + (-z+f)g/(1-g) \qquad (13)$$

Therefore, the organization will not deviate from the *No Fine* strategy if the payoff from deviation is too low:

$$z+f + (-z+f)g/(1-g) < z/(1-g), \text{ or } g > (2f-z)/(f+z) \qquad (14)$$

To compare the results of a fine-only game with those of a bonus-only game in a repeated setting, we should assume that the bonus and the fine are equal in magnitude, so that *b=f*. This way, we will be able to focus on the impact of the direction of incentive (positive bonus vs. negative fine) which will not be distorted by possible disproportions in the size of incentive. Then, if the bonus and the fine are equal in magnitude, the critical value of time value of money factor *g* that is sufficient for compliance with security policies by the user is the same in both cases (compare inequalities (3) and (11)):

$$g > (c-d)/b = (c-d)/f \qquad (15)$$

We may also show that critical value of *g* that is necessary to prevent deviation from equilibrium by the organization is also the same. To see this, recall that the amount of fine *f* is equal to that of bonus *b* and is smaller than *z* – the organization's value of increased security. Since $f < z$, we can rewrite (14) as:

$$g > (2f-z)/(f+z) > (2f-f)/(z+z) = f/2z \tag{16}$$

Thus, the condition for non-deviation of the organization from equilibrium strategy is the same in the case of bonus-only and fine-only mechanism (compare inequalities (6) and (16)):

$$g > b/2z = f/2z \tag{17}$$

We conclude that when the magnitudes of the bonus and the fine are the same, both bonus-only and fine-only mechanism will be effective under the same conditions. Theorem 2 formally describes the conditions when fine-only mechanism is applicable. It can be proven in the same way as Theorem 1 and produces the same corollary. We will omit proof steps.

Theorem.2. **(Characterization of feasible fine amount for the fine-only game)** *Suppose that assessing a fine f is feasible. Then, if the choice of penalty f is inducing incentive compatibility (voluntary adherence with security policy), it may be characterized as follows:*

$(c-d)/g < f < 2zg$

Proof. Follows from (11) and (16) *Q.E.D.*

Corollary 2. **(Existence of guaranteed discount rate that induces incentive compatibility).** *Suppose that imposing a fine is feasible. Then, there exist a lower bound on time value of money factor g that induces mutual incentive compatibility. This critical value of g is* $1/\sqrt{2}$.

We have seen that bonuses and fines produce similar outcomes when used separately. Now we should see what effect they will have if they are used simultaneously. Let us revisit the bonus-fine compliance game from a repeated game perspective. In a single period, players payoffs are as follows:

Org. The user	Bonus	Fine
No Compliance	$+b-d; -z-b$	$-f-d; -z+f$
Compliance	$b-c; z-b$	$-c-f; z+f$

The outcome (*Compliance, Bonus*) is beneficial simultaneously to both players. If it is to be sustained as an equilibrium of an infinitely repeated game, neither player should have an incentive to deviate from playing it. Using the same logical steps as before, we obtain that the non-deviation condition for the user is

$$(b-c)/(1-g) > b - (fg+d)/(1-g), \tag{18}$$

while for the organization the non-deviation condition is

$$(z-b)/(1-g) > z + f + (-z+f)g/(1-g) \tag{19}$$

As before, we would like to identify the effect of the direction of the incentive (bonus vs. fine) and avoid the effects of the relative magnitude of bonus and fine. Thus, we assume that the bonus and the fine are equal, $b=f$. Then we obtain the following non-deviation conditions for the user and organization:

$$g > (c-d)/2b \tag{20}$$

$$g > b/z \tag{21}$$

The equilibrium which enforces the compliance with information security policies is possible when both of these conditions are met, and the required bonus and fine amounts then satisfies conditions of Theorem 3.

Theorem 3. **(Characterization of feasible fine amount for the bonus-fine game)** *Suppose that providing bonus and fine is feasible and both bonus and fine amounts are equal, $b=f$. Then, if the* *choice of incentive b=f is inducing incentive compatibility (voluntary adherence with security policy), it may be characterized as follows:*

(c-d)/2g < b=f < zg

Proof. Follows from (20) and (21) *Q.E.D.*

Corollary 3.3. **(Existence of guaranteed discount rate that induces incentive compatibility).** *Suppose that providing a bonus and a fine is feasible, and their amounts are equal. Then, there exist a lower bound on the time value of money factor g that induces mutual incentive compatibility. This critical value of g is* $1/\sqrt{2}$.

We summarize the result of our analysis in Table 1.

Incentive mechanism	Incentive range	Compliance – inducing value of ***g***
Bonus only	*(c-d)/g < b < 2zg*	$1/\sqrt{2}$
Fine only	*(c-d)/g < f < 2zg*	$1/\sqrt{2}$
Bonus and fine	*(c-d)/2g < b=f < zg*	$1/\sqrt{2}$

Table 1. Comparison of different incentive mechanisms

There are three important observations that arise from this analysis. First and foremost, regardless of the particular choice of incentive scheme, it is possible to ensure compliance with information security policies if the time value of money is sufficiently high. Results of Theorems 1-3 and their corollaries suggest that despite all uncertainty and threat of opportunistic behavior, there is a practically significant range of potential values of discount factors for which it is possible to build trust relationships between the user and the organization and insure the provision of appropriate level of security. Moreover, such a cutoff level is independent of any particular configuration of agents' payoffs or choice of incentive scheme (e.g., bonus only, fine only, or both).

Second, a bonus and a fine will produce the same range of effective incentive levels when they are used independently. Therefore, they may be used interchangeably as the tools of enforcing compliance with information security policies, as long as their magnitudes are identical, or at least perceived as being so by the users.

Third, simultaneous use of a bonus and a fine will produce a narrower range of incentive magnitude as compared to use of bonus or fine alone. On one hand, this leaves the organization with fewer choices for policy configurations and may be perceived as a negative issue. On the other hand, it also restricts the space of potential negotiations between the user and the organization over the amount of bonus and fine and may lead to more concise and faster outcomes of such negotiations in practice.

To further extend our analysis, we consider another deterrent mechanism that may be used to prevent the user's opportunistic behavior and provide compliance with security policies.

3. Penal code

An important mechanism for achieving desirable outcomes in repeated games is known as a penal code. Abreu (1988) discusses the concept of optimal penal codes that can be used as an alternative to Nash reversion strategies to support favorable equlibria in infinitely repeated games with discounting. The logic behind penal codes is described below:

- Suppose the game has developed along some initial path through the current time period, for example, in the compliance game between the user and the organization, and both players were consistently choosing the strategies of *(Compliance, Bonus).* Then, if no player changes her strategy in the current time period, the same path continues.

- However, if a player deviates from the established path, the punishment takes place in the form of an outcome that is unfavorable for the deviating player. For example, in the compliance game, the user chooses the strategy of *No Compliance* if the organization did not play the *Bonus* strategy in previous period. If the resulting outcome is also the worst possible for the punished player, it is called an optimal penal code.
- Penal codes are player-specific and the same penal code is used to punish any deviation. Generally, penal code includes a sequence of actions (a path of the game), not just single-period punishments.

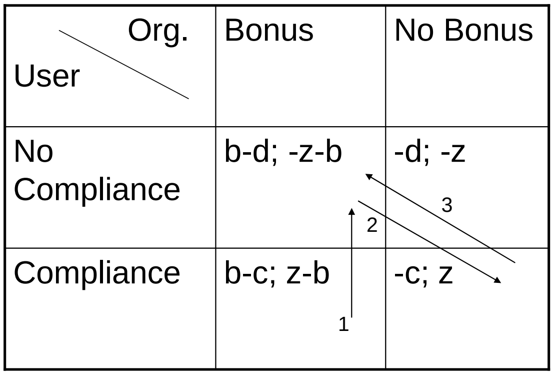
We modify the compliance game to implement a penal code that enforces compliance with information security policies using the following mechanism[5]. The user and the organization play an infinitely repeated game, moving simultaneously in each stage. The user may choose between strategies of *Compliance* and *No Compliance,* while the organization chooses between strategies of *Bonus* and *No Bonus.* While the user chooses her action at each stage, the organization strictly adheres to the following rule: after offering a *Bonus* in the first period, it monitors the action of the user. If the user chooses *Compliance* in any given period*,* the organization is committed to offer a *Bonus* again in the next period. However, if the user chooses *No Compliance,* the organization offers *No Bonus* in the subsequent stage of the game. The sequence of game decisions is presented below.

1. Start with the (*Compliance, Bonus)* game in previous period. The user chooses her strategy for the next period. If the user plays *Compliance* again, the organization plays *Bonus* and return to step 1. Else, go to step 2.

[5] We consider the modification of the "bonus-only" game. It is easy to show that similar results hold in case of penal codes applied to "fine-only" and "bonus and fine" games.

2. The organization punishes the user by playing the *No Bonus* strategy in the current period. The user chooses her action in response to this pre-announced strategy. If she chooses *No Compliance,* return to step 2. If she chooses C*ompliance*, go to to step 3.
3. The organization plays *Bonus* in the current period. If the user chooses to play *Compliance,* return to step 3. Else, go to step 2.

This decision sequence represents a contingent contract, as the user knows what actions the organization will take in response to her moves. The payoffs of players for a single stage are presented in Figure 1. Payoffs of future periods are discounted in the same manner as before, using a time value of money factor *g.*



Org. User	Bonus	No Bonus
No Compliance	b-d; -z-b	-d; -z
Compliance	b-c; z-b	-c; z

Figure 1. Compliance game with penal code

This figure also represents the potential paths of deviation that should be considered. Arrow 1 represents the original deviation by the user. Once it takes place, the organization imposes a penalty in the form of the *No Bonus* strategy, represented by arrow 2. As long as the user chooses a strategy of *No Compliance* in response to that, the game ends up along the Nash reversion strategies path, which was analyzed before. However, if the user accepts the one-period punishment and chooses the strategy of compliance, then she knows that in the next period the organization will offer a *Bonus.* Thus, there is a possibility of returning to the outcome of *(No*

Compliance, Bonus), represented by arrow 3 (since *b-d* is higher single-period payoff than *b-c*), thus invoking punishment by organization again. Such "oscillation" may repeat forever depending on the value of time value of money factor *g*. However, in the Theorem 3.4 we describe conditions under which the proposed penal code ensures compliance with security policies.

Theorem 4. **(Penal code that ensures compliance with security policies).**

Suppose that the penal code of the compliance game is defined as follows: in any time period t the organization plays Bonus if t=0 or the user played Compliance in time period t-1; and it plays No Bonus otherwise. Then, this penal code will enforce voluntary compliance by the user if b > (c-d)/g

Proof. We need to show that a) proposed penal code is incentive compatible for the user and b) under this code persistent compliance is preferred to alternating between compliance and non-compliance strategies.

To show that this penal code is incentive-compatible for the user, we need to consider her alternatives once the code is imposed. As mentioned before, the only other alternative available to the user once the penalty is imposed is to play Nash reversion strategies. Her payoff from the continued game in this case will be

$$(b-d) + (-d)\ (g+g^2+g^3 \ldots) = b - d/(1-g) \qquad (22)$$

If the user chooses to comply with the penal code path instead, she will return to the deviation path in alternating time periods, with corresponding payoff of

$$(b-d)\ (1+g^2+g^4 \ldots)+(-c)\ (g+g^3+g^5 \ldots) = (b-d-cg)/(1-g^2) \qquad (23)$$

Comparing the R.H.S of (23) and (24) we see that the penal code path is preferred to simple Nash reversion if *b > (c-d)/g*

Now, we need to show that consistent compliance is preferred by the user. This will be the case when its payoff exceeds that of “flipping” between compliance and non-compliance. Consider two consequent time periods, t and $t+1$. If the user chooses *Compliance* in both of them, her payoff is $(b-c) + (b-c)g = (b-c)(1+g)$ (24)

Alternatively, if the user flips between compliance and non-compliance, her payoff is $(b-d) + (-c)\, g = b-d - cg$ (25)

Consistent compliance generates higher payoff if the R.H.S. of (24) exceeds that of (25), or when $b > (c-d)/g$ *Q.E.D.*

Theorem 4 has important implications. First of all, it shows that it is possible to enforce compliance with security policies by the means of a simple penal code, which is a more realistic strategy than Nash reversion. Second, the critical condition when such penal code will work is the same as before: the bonus offered to the user for compliance in current period should exceed the difference of user’s cost of compliance and opportunism in the next period. Also, since the conditions for user compliance are the same as in Nash reversion strategies (Theorem 1), the organization has a choice between at least to mechanisms that lead to desired results, if time value of money factor is sufficiently high.

As we have seen so far, it is important to build trust in repeated future interactions between parties to ensure that no one is inclined to make one brutal move and cut ties with its counterpart. Also, such trust building is possible for a practically reasonable range of values of “time value of money” factor. However, it is not clear if decision makers in the real world indeed consider “time value of money” factors when making security decisions, and what particular values they use. Also, organizations and users usually know rules of engagement in advance, with performance bonuses and fines provided in contracts and policies before the engagement begins. Therefore, it is necessary to consider alternative approaches to providing incentives for compliance with information security policies. In the next section, we study the dynamics of user-organization interaction in cases when the organization announces in advance which incentive scheme it will use.

4. Discussion

The main goal of this work was to identify conditions under which fines and bonuses may be used as incentives for voluntary compliance with information security polices in organizations. We have found that such compliance may potentially be enforced if the interactions between the user and the organization are repeated over time. We found that fines and bonuses are, in theory, equally effective in this setting. A combination of bonus and fine may also be used.

An alternative perspective is that of sequential games, when the user observes organization's choice of incentive. While these results provide prescriptive recommendations on the use of bonuses and fines to design security compliance contracts, it is necessary to highlight some practically important issues that are not directly addressed by this set of models. First of all, though we found fines to be monetary equivalents or even sometimes preferred to bonuses, they may also be perceived by the users as unfair. In this case, a fine is usually preferred to a bonus by the organization; further, even a threat of fine is sometimes sufficient to ensure compliance.

REFERENCES

Abreu, D. “On The Theory Of Infinitely Repeated Games With Discounting”, *Econometrica,* 1988, 56(2), 383-396

Arora, A., J. Caulkins, R. Telang, “Research Note: Sell First, Fix Later: Impact of Patching on Software Quality”, *Management Science,* 52:3, 465-471, 2006.

Browning, J., “Midsize Business Security Spending Plans, 2006”, *Gartner Research,* report G00137654, 2006

Conrad, K., J. Wang, “On the Design of Incentive Mechanisms in Environmental Policy”, *Environmental and Resource Economics,* 1993, 3, 245-262

Ellingsen, T., M. Johannesson, “Trust as Incentive”, working paper, *Stockholm School of Economics,* 2005, http://www1.fee.uva.nl/creed/seminarpdffiles/EllingsenPaper.pdf

Fiberlink. “New Poll: One in ten Employees Knowingly Violates IT Policy”. 15 March 2010. Available online at http://www.maas360.com/fiberlink/en-US/presscenter/releases/2010/ITPolicyViolations.html

Friedman, J.W. “A Non-Cooperative Equilibrium for Supergames”, *Review of Economic Studies,* 1971, 38, 1-12

Furusawa, T. “The Optimal Penal Code vs. Infinite Nash Reversion in Trade Liberalization”, *Review of International Economics,* 1999, 7(4), 673-681

Gachter, S., E. Kessler, M. Konigstein, “Performance Incentives and the Dynamics of Voluntary Cooperation”, working paper, 2006, http://www.kent.ac.uk/ economics/seminars/sempapers/Spring0506/GaechterKesslerKoenigstein_v0.9.pdf

Nault., B. “Equivalence of Taxes and Subsidies in the Control of Production Externalities”, *Management Science,* 42(3), March 2006, pp. 307-320.

Perry, W. "Quality Assurance for Information Systems", QED, Boston, MA, 1991

Ponemon Institute. "The True Cost of Compliance". January 2011, http://www.tripwire.com/tripwire/assets/File/ponemon/True_Cost_of_Compliance_Report.pdf

PriceWaterhouseCoopers. "Information Security Breaches Survey Report 2010". 2010. Available online at http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf

Sandmo, A. "Public Provisioning and Private Incentives", *Norvegian School of Economics and Business Administration,* discussion paper 18/02, 2002

Smith, D., T. Austin, F. Caldwell, "Think of Compliance When You Manage Collaboration Systems", *Gartner Research,* report G00136737, 2006

Strand, J. "Environmental Accidents under Moral Hazard and Limited Firm Liability", *Environmental and Resource Economics,* 1994, 4, 495-509

Verizon. "2012 Data Breach Investigation Report". 2012. Available online at http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Vijayan, J. "Security Imperative", *Computerworld,* December 12, 2005

Wheatman, V., B. Smith, N. Shroder, J. Pescatore, M. Nicollet, A. Allan, R. Mogull, "What Your Organization Should Be Spending for Information Security", *Gartner Research,* report ID G00126733, 9 March 2005.