A Novel Model for Monitoring Security Policy Compliance

Mutlaq Alotaibi[1], Steven Furnell[1, 2, 3] and Nathan Clarke[1, 2]
Plymouth University, Plymouth UK[1],
Edith Cowan University, Perth, Western Australia[2],
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa[3]

Abstract

Organizations repeatedly suffer harm from employees who are not obeying or complying with their information security policies. Non-compliance behaviour of an employee, either unintentionally or intentionally, pose a real threat to an organization's information security. As such, more thought is needed on how to encourage employees to be security compliant and more in line with a security policy of their organization. As an initial approach to achieve this goal, we propose a model that is intended to provide a comprehensive framework for raising the level of compliance amongst end-users, with the aim of monitoring, measuring and responding to users' behaviour with an information security policy. The proposed approach is based on two main concepts: a taxonomy of the response strategy to noncompliance behaviour, and a compliance points system. The response taxonomy is comprised of two categories: awareness raising and enforcement of the security policy. The compliance points system is used to reward compliant behaviour, and penalise noncompliant behaviour.

1. Introduction

A security policy is defined in a formal document that specifies what constitutes acceptable and unacceptable behaviour of users in relation to dealing with information assets in a secure manner. It is part of the formal information security control and a baseline statement on the information security tasks which should be carried out by employees. According to SANS [1], a security policy is typically "a document that outlines specific requirements or rules that must be met, in the information/network security realm, policies are usually point-specific, covering a single area". Organizations ought to view having information security policies and procedures in place as being just as important as having technical solutions to hand [2]. The implementation of such technical measures alone does not guarantee a safe computing environment. As part of their implementation guidance, organizations should establish a set of information security policies, which are approved by top management and then distributed amongst and communicated to all employees.

Nowadays, the majority of organizations are aware of the importance of information security policy. According to PricewaterhouseCooper (PwC) [3], 98% of large organizations and 60% of small organizations have a documented information security policy. However, employees' compliance with information security policy is still of great concern to many organizations. According to the E&Y Global Information Security Survey [4], 57% of organizations consider their employees to be the most likely source of an attack, with 38% viewing careless or unaware employees as the most likely threat. Moreover, the UK Information Security Breaches survey [5] found that 70% of organizations with a poorly understood security policy had staff-related breaches, whereas only 41% of organizations where the policy was well understood had any of these. Therefore, when employees have a good understanding of the security policy, this positively affects the overall security of an organization. Arguably, the human factor is still the weakest link in the information security chain, causing an increase in the number of security threats. As such, many end users are still unaware of the importance of information security and the relevant organizational requirements. Chan and Mubarak [6] found that more than fifty per cent of the employees in their study were unaware of the existence of the information security policy in their organizations.

This study is considered part of an on-going research that is intended to provide a comprehensive framework for raising the level of compliance amongst end users, it aims at proposing a model that monitoring, measuring and responding to the users' behaviour with an information security policy. In addition to that, a scoring points system (compliance points system) will be used to play supplementary rule within the proposed model. The goal of utilizing the compliance points system is to motivate users to be compliant with the policy, as well as, measuring their compliance rate with the security policy or any element of it.

This paper begins by presenting the challenges facing the effective adaption of an information security policy. It then discusses the factors that affect human behaviour. The proposed model will be presented in the form of two main components: response taxonomy and the compliance points

system. Finally, the paper will draw a conclusion and suggest future work in this domain.

2. Key information security policies related challenges

A number of researchers have addressed the challenges associated with information security policy. Based on their assessments, Table 1 classifies those challenges into four major groups:

Table 1. An information security policy challenges

Group #	Main challenge	Sub-challenges	Sources
1	Security policy Promotion	• Dissemination • Awareness Raising • Training • Enforcement and Monitoring	[7] [5] [8] [9] [10] [2]
2	Non-Compliance with Security Policy	• Malicious behaviour • Negligent behaviour • Unawareness	[11] [12] [13] [14] [15]
3	Security Policy Management and Updating	• Regular review and update • Policy management • Technology advances • Designing good policy	[16] [17] [18]
4	Shadow Security	• Unclear security policies • Unusable security mechanisms • High compliance cost	[19] [20] [21]

2.1. Security policy promotion

Organizations encounter challenges associated with the promotion and dissemination of their information security policies. In research conducted by the Economist Intelligence Unit [7], most of the IT managers claimed that their organizations had developed information security policies to overcome many concerns, but only a few of these organizations had seriously instilled this culture into their employees. This is supported by PwC [5], who state that "Although there are more written policies in place to guide employees' behaviours towards security, we haven't yet seen this translate into better understanding of these policies". A survey carried out by Prince [8] revealed that more than half of the members of staff in organizations did not participate in any kind of security awareness training. This study confirms that the absence of training results in violations of policy and the occurrence of behaviour that poses a risk to the organization. Despite the presence of the best information security awareness programs, obstacles exist that make the successful implementation of awareness activities more challenging. These common obstacles are:

1) Implementation of new technology
2) One size fits all
3) Too much information
4) Lack of organization
5) Failure to follow up
6) No explanation of why [9][10].

Depending on the enforcement and monitoring of a security policy, implementing security monitoring tools can help to identify any security policy breaches that may occur. However, these monitoring tools are not widely implemented in organizations [2].

2.2. Non-compliance with security policy

Non-compliance with information security policy is considered to be primarily a human problem rather than a technical issue. Researchers have mentioned three types of non-compliance behaviour: malicious behaviour, negligent behaviour and unawareness. The main motivation for malicious behaviour is malicious intent to bring harm to an organization's information assets [11] [12], whereas negligent behaviour is intent to violate an organization's security policy but not to harm that organization [13]. The third type of non-complaint behaviour is due to unawareness, whereby end users are unaware of the importance of information security and the relevant organizational requirements. Khan et al.'s [14] research indicated that more than fifty percent of employees are unaware of the existence of an information security policy in their organisation. Moreover, Greitzer et al. [13] state that users tend to dislike the active controls that are imposed on their PCs, and this can be seen in many organisations. The reason for users having an aversion to these controls is that they impose a group of no commands (e.g. no Google apps, no Facebook, no Skype, etc.).

There is a direct relationship between the problems faced by many organisations and lack of attention paid to information security awareness and training [15]. Security awareness and training can play a supplementary role alongside a information security policy in order to reduce the number of potential insider threats. If there is a comprehensive and effective information security culture in an organisation and the users are applying it, this will make a difference.

2.3. Security policy management and updating

Many organisations do not continuously review and update their information security policy. Colwill [16] states that "security policy, controls, guidelines and training are lagging behind changes". Moreover, designing and managing a security policy that meets

all the important criteria can be a challenge for many organisations [17]. Furthermore, many organisations do not update their policy to be more in line with rapidly and constantly developing technology. A study conducted by Protiviti [18] found that only 24% of the respondents had a cloud acceptable usage policy in place. Evidently, this indicates that many organisations ignore the importance of updating their policies. Organisations should consistently review and update their policies to ensure that those policies are still meeting all their needs and ensure that updates are disseminated to all employees.

2.4. Shadow security

Two types of user behaviour associated with information security policy have been identified in the literature: compliance and non-compliance. However, Kirlappos et al. [19] have suggested a third type of user behaviour, which is shadow security. Shadow security is defined as "employees going around IT to get the IT services they want on their own''[20]. Such employees implement their own security solutions when they believe that compliance is beyond their capacity or will affect their productivity. For example, if a password security policy requires employees to choose a strong password (12-character length, upper letters and symbols), some employees may find it difficult to memorise the password, and therefore, they may write the password on a sticky notes and put it on the computer screen. In the aforementioned example, an employee is considered to be complaint with password policy; however, they are also implementing a shadow security policy, and this may threaten an organisation's security. Hence, shadow security may create a false sense of security. The risk that the organisation may be at due to their shadow security policy are not usually perceived by employees who play around with the main security policy. Thus, the employee does not understand the risk that the organization may be at due to this behaviour.

Shadow security may affect the success of policy implementation, for instance, ineffective communication of a policy to the management and security policies not being reviewed and evaluated in a timely manner; however, shadow security can make this task more difficult. Moreover, the presence of shadow security behaviour may lead to the emergence of a non-compliance culture within an organisation as a whole [21]. Furthermore, if employees play around with official security policy, they may not provide feedback on the shortcomings of that policy and suggest alternative solutions.

According to Kirlappos et al. [19], organisations should pay attention to reducing the cost of compliance with unusable security mechanisms and unclear information security policies, which may not provide efficient protection for an organisation because employees will attempt to find ways to play around with them as they are undesirable or impractical in their opinion.

3. Factors influencing user's behaviour

Multiple studies have attempted to identify the different reasons for the various levels of compliance with IT policies. According to [22], authors categorize the factors that affect the security of information into human and organizational factors. Several of the human factors have been studied in the literature in order to investigate their influence on a user behaviour, such as perception, personality, culture, gender, satisfaction, and habits. However, in this paper, the human factors will be out of the scope, therefore, we are going to focus on the organizational factors, which will have a relation to the proposed model. However, for further information about the human factors, our earlier paper is covering this aspect [23].

Although compliance with security policy is first and foremost a human issue, organizational factors found to be influencing users' compliance have been explored in several studies. Table 2 summarises the important factors that influence user compliance with information security policy, and these are also discussed in the paragraphs that follow.

3.1. Information quality

In the literature, the information quality of a security policy (date flow) is generally seen as a factor that is strongly related to employees' compliance with information security policy. Inadequate policies can contribute negatively towards non-compliance. Hence, inadequate organisational procedures may lead to a lack of skills, knowledge and ability to deal with security requirements [14]. A study conducted by Pahnila et al. [24] found that information quality has a significant effect on actual information security policy compliance. Furthermore, Bulguru et al. [25] investigated the impact of three quality dimensions, clarity, adaptability and consistency, on employees' compliance with security rules and regulations and highlighted their significance.

3.2 Motivation

Motivators can be used to encourage users to comply with information security policy [26]. A good example of a motivator is a reward, which is defined as a tangible or intangible gift that is granted to an employee who complies with the requirements of security policy. Several studies have revealed that rewards have a significant impact on an employee's perception of the benefits of compliance.

Table 2. Major organizational factors

Factor	Description	Research Method	Source
Information Quality (Data flow)	The facilitating conditions and information quality have a significant impact on user compliance behaviour.	Questionnaire (Participant:245)	[24]
		Theoretical	[13]
		Questionnaire (Participant:464)	[25]
Motivation	Motivation, such as rewards, has a significant impact on users' perception of the benefits of compliance.	Questionnaire (Participant:464)	[25]
		Theoretical	[26]
Sanction (Deterrence)	Sanctions (deterrence) are one of the important factors that affect employees' actual compliance with established information security policy.	Questionnaire (Participant:464)	[25]
		Questionnaire (Participant:113)	[27]
		Questionnaire (Participant:917)	[28]
Awareness & Training	Information security awareness has a direct effect on user compliance behaviour.	Questionnaire (Participant:464)	[25]
		Action research (Participant:16)	[29]
		Questionnaire (Participant:308)	[6]
Computer Monitoring	Computer monitoring tools are negatively associated with information security policy non-compliance intention.	Questionnaire (Participant:232)	[30]
		Questionnaire (Participant: 304)	[31]
Persuasion	Persuasion technology can raise security awareness and then increase level of compliance.	Experiment (Participant:30)	[32]
		Theoretical	[10]

For instance, Bulgurcu et al. [25] empirically investigated the role of rewards in driving employees to comply with the requirements of security policy and found that rewards have a significant impact on employees, making them more compliant.

3.3 Sanction (Deterrence)

The existing literature has highlighted the importance of sanctions (deterrents) in relation to changing users' behaviour towards information security policy, making them more compliant, and a number of studies have offered empirical support for this claim. According to Bulgurcu et al. and Cheng et al. [25][28], sanctions are one of the most important factors affecting the actual compliance of employees with established security policies. Similarly, a study conducted by Harris and Furnell [27] investigated the impact of sanctions on employees' compliance with information security policy, particularly on the use of shaming punishment as a deterrent, 71% of the participants indicated that they would be more likely to follow security policy if their employers were willing to shame those who did not comply.

3.4. Awareness raising and training

Previous studies on information security have highlighted the impact of security awareness on employees' behaviour. According to Bulgurcu et al. [25], awareness has a significant influence on an employee's intention to comply. Puhankinen et al. [29] carried out action research to validate a training programme on information security policy compliance. The results of the study suggested that increased awareness and training programmes have an impact on users' compliance with information security policy. Chan and Mubarak [6] concluded that a "lack of awareness and knowledge of policies may have allowed for staff to violate such policies".

3.5. Computer monitoring

Security monitoring and auditing tools can be utilised to change unwanted behaviour in order to enforce information security policy. Once users are fully aware of these tools, they are encouraged to change their behaviour and be more compliant. A

number of studies have provided empirical evidence of the relationship between computer monitoring and complaint behaviour. These studies [30][31] found that an individual's information security compliance is influenced by computer monitoring and auditing tools. As such, monitoring tools assist in mitigating non-compliance behaviour.

3.6 Persuasion

Persuasion is an integral part of our lives and of human interaction. Fogg [33] described persuasive technology (PT) as "interactive computing systems designed to change people's attitudes and behaviours". Persuasive computing technology can affect people's attitudes and bring about some constructive changes in many domains, for example, marketing, health, safety and the environment. Marketing is perhaps the most significant domain in which persuasive technologies are used to encourage customers to buy products and services. With regard to information security, the results of an empirical study by Yeo et al. [32] suggest the significance of persuasive technology in changing end-users' behaviour. Furthermore, Qudaih et al. [10] indicate that using persuasive technology to disseminate policies and procedures can lead to effective information security awareness programmes.

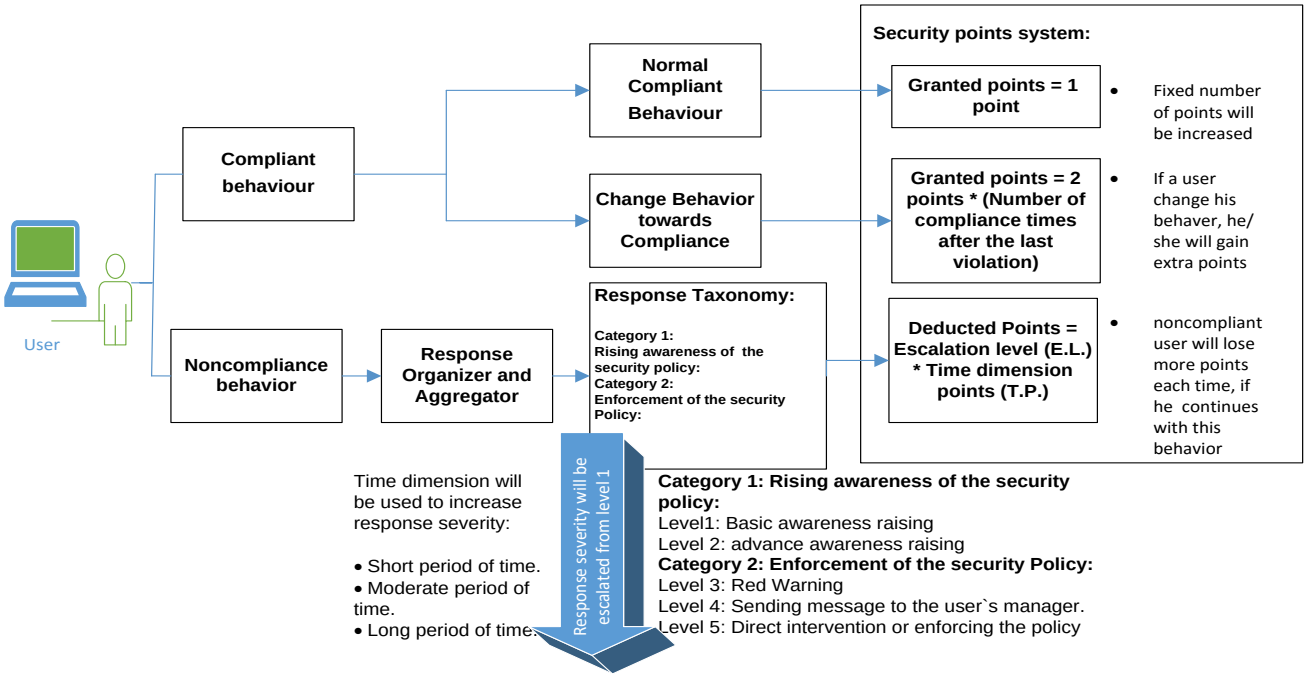

Figure 1. A Model for Monitoring Security Policy Compliance

4. A Model for monitoring security policy compliance

With the aforementioned challenges and the influencing factors of a successful implementation of an information security policy, the necessity for dynamic response to a user behaviour is becoming more apparent. Thus, a novel model is proposed which aims at increasing the compliance level of a user by monitoring and measuring the actual behaviour. Essentially, in order to get information relating to the actual behaviour, there will be local agents on each source of this information, for example:

• Local agent on the active directory or on an applications level, to gather data about a user behaviour with the password policy.

• Local agent on network traffic or proxy, to gather data about a user behaviour with an internet usage policy.

• Local agent on exchange server, to gather data about a user behaviour with an email usage policy.

Having monitoring an actual behaviour, the proposed model will rely on two main concepts: a taxonomy of a response to the noncompliance behaviour, and

utilizing a compliance points system (see Figure 1). The response taxonomy is composed of two categories:

1) Awareness raising, and
2) Enforcement of the security policy.

Whereas, the compliance points system will be used to grant points to the compliant behaviour, or to deduct points from the noncompliant behaviour.

4.1. Compliance behaviour

A user is considered to be compliant when he/she shows the desired behaviour of complying with information security policies and rules. In this regards, therefore, two methods for evaluating users' behaviour have been suggested: 1) based on explicit action, or 2) based on elapsed period of time. In the former category, based on explicit action, when a user performs a certain action of compliance, e.g. the user has changed his password after 6 months. In the latter category, based on the elapsed period of time (compliance period), a user will consider as a complaint once he or she did not violate the security policy during certain period of time, e.g. if a user has not browsed nonwork related websites for a period of 3 months.

Therefore, a user who adheres to the information security policy will get compliance points for that behaviour in relation to each element of the policy. And thus, each element of the information security policy will have a separate tracker of points for each user. There will be two mechanisms of granting points: points for normal compliance behaviour, and points for changing behaviour towards compliance (see Figure1).

4.1.1. Normal compliance behaviour. It is a desired behaviour; a user adheres to the information security policy as a part of his culture. This behaviour will be granted 1 point as a reward for each commitment with the security policy elements separately (Granted points = 1 point). To demonstrate this concept, in the following scenario (as shown in Table 3), we assume that a user called A has performed the below complying actions in relation to two different elements of a security policy, which are changing password security policy and non-browsing of non-work related websites policy:

Table 3. User A actions

#	Action & Date	Policy description
First action	User A has changed his password on 01-01-2016	Passwords must be changed every 6 months.
Second action	User A has changed his password on 01-06-2016	
Third action	User A has not browsing any non-work related websites from 01-01-2016 till 01-03-2016	Not allowed to browse any non-work related websites.
Fourth action	User A has not browsing any non-work related websites from 01-03-2016 till 01-06-2016	

According to the above actions, the User A will gain four points for his security complaint behaviour with each element of the policy. As a response for the first action, when he changed his password in compliance to changing password security policy, he will gain one point and the total points of changing password security policy will be one point. In the second action, which the evaluation is based on the elapsed time, User A was compliant for 3 months so he will get one point for that behaviour and as a result the total points for non-browsing non-work related websites security policy will be one point. In the third action, the user changed his password for the second time, therefore the user will gain another point for that behaviour and as a total the password changing policy will be two points. Likewise, in the fourth and last action, the user will gain another one point for being complying with the non-browsing of non-work relate websites security policy and as a result the total points of this particular security policy element will be two points.

4.1.2. Changing behaviour towards compliance. Correspondingly, the second mechanism has been proposed for those users who changed their behaviour from noncompliance towards compliance. The main aim of this mechanism is to encourage users to continue complying with the security policy in order to gain extra points that would gradually recover the lost points from previous noncompliance behaviour. The proposed equation of this mechanism would be as follows:

*Granted points = 2 * (Number of compliance times after the last violation of the same security policy element)*

The following scenario illustrates this mechanism; we assume that a user called B has not changed his password for three times (24 months). Therefore, due to his noncompliance behaviour, he had lost points for four times. After that he changed his behaviour to be in line with the changing password policy. In this case, User B will be given more points each time he/she complies with the changing password policy till recovering the lost points for that element of the policy, as shown in the three below actions.

Action 1: User B changed his password on 01-01-2016:

*Granted points = 2 * (Number of compliance times after the last violation) = 2 * 1 = 2 points.*

Action 2: User B changed his password on 01-06-2016:

Granted points = 2 * (Number of compliance times after the last violation) = 2 * 2 = 4 points.

Action 3: User B changed his password on 01-12-2016:

Granted points = 2 * (Number of compliance Times after the last violation) = 2 * 3 = 6 points.

Thus, in Action 1, the User B has earned 2 points for being compliant with this element of the policy,

and because this action was the first compliance after the last noncompliance behaviour. In Action 2, the given points to the User B has been increased to 4 points because it was the second compliance therefore the points total for this policy element would be 6 points. In Action 3, it was the third compliance on which the user has changed the password therefore the user earned 6 points and the total points for the changing password policy was 12 points. Thus, User B has gradually gained points because of changing behaviour towards compliance, however, this mechanism will be stopped when the user recovers the lost points and the user will be switched to the normal compliance mechanism, which was explained previously.

4.2. Non-compliance behaviour

Non-compliance behaviour of users is evaluated on an explicit action that leads to the violation of the security policy, such as downloading unauthorised software. Non-compliance behaviour is subjected to various levels of response, in conjunction with the points system (see Figure 1).

4.2.1. Response organiser and aggregator. The aim of this component is to organise the process of responding to non-compliant behaviour. The level of response is determined by this component, as is the number of points to be deducted. The aggregation concept is used to determine the method of the response. For example, if the response is an email to the user's manager, then the response aggregator considers other violations from other users, to be aggregated in one email.

4.2.2. Response taxonomy. There will be a response strategy for non-compliance behaviour to raise awareness or enforce the information security policy. Thus, the framework has two potential categories of response to the non-compliance behaviour: (1) Raising awareness of the security policy, (2) Enforcement of the security policy. Moreover, each category is composed of a variety of sub- responses, which have been designed for increasing the severity levels in a gradual manner.

• Category 1: Raising awareness of the security policy (Two levels of escalation) Level 1: Yellow Warning &Written security policy reminder (Basic awareness raising) Level 2: Orange Warning &Web-based awareness training program or video-based awareness reminder (Advance awareness raising).

• Category 2: Enforcement of the security Policy (Three levels of escalation)

Level 3: Red Warning

Level 4: Sending message to the user's manager

Level 5: Direct intervention or enforcing the security policy e.g. reducing privileges of accessing resources or blocking access to some IT resources

Time dimension is used as an indicator for increasing response severity up to the next level. Time dimension refers to the period of time between violations of the same security policy element. In other words, over what period of time the noncompliance behaviour has happened since the last violation in relation to a particular element of the policy. There are three types of time dimension:

(1) Short period of time

(2) Moderate period of time

(3) Long period of time

Table 4 clarifies the three types of time dimensions.

Table 4. Time dimension types

Time dimension	Expected behaviour	Escalation to the next level
Short time	Users may be unaware of the information security policy.	The sequence of events occurring in a very short period of time. All repeated events in this time duration will be considered as a single event, and there will be no escalation in this type of time duration.
Moderate time	Users may be aware of the information security policy and frequent violations occur in a moderate period of time,	Intervention is required, escalating the response severity to the next level.
Long time	Users may forget details of the information security policy, due to long period of time.	In this instance, users will require an awareness reminder from Category 1: raising awareness of the information security policy.

The three types of time dimensions (short time, moderate time and long-time) would be configurable by the organisation itself, but we have set the recommended defaults values of the three types as shown below.

• Short time dimension = less than 24 hours as a default value. Because, there will be not enough time for any significant intervention, so the time should be short.

• Moderate time dimension = from 24 hours up to 6 months as a default value. Because, there will be enough time since the last violation and the user should be received a response for the last violation.
• Long-time dimension = more than 6 months as a default value. Because, the period between the new violation and the last violation should be long period of time because the user is considered as a forgotten user.

To demonstrate the time dimension effect on the response strategy for non-compliance behaviour, Table 7 describes the following scenario: User C has violated a particular information security policy, policy 1, many times over a two-year time period.

Table 5. User C violations

Violation No.#	Description & Date
Violation 1	User C violated policy 1 for the first time on 01-01-2015
Violation 2	User C violated policy 1 for the second time on05-01-2015
Violation 3	User C violated policy 1 for the third time on 07-02-2015
Violation 4	User C violated policy 1 for the fourth time on 07-02-2015
Violation 5	User C violated policy 1 for the sixth time on 01-05-2016

User C has violated this policy six times over two years. The first violation was on 01-01-2015, and the response level was set to Level 1, basic raising of awareness. As such, because it was the first violation, there is no time dimension between the current violation and the past violation, therefore in this case the response level is considered as level 1.

The second violation occurred on 05-01-2015, four days after the first, so the time duration was considered as moderate. User C was considered to be intentionally violating the security policy for the second time, therefore the response level was escalated from Level 1 to Level 2, advanced raising of awareness.

The third violation on 07-02-2015, came nearly a month after the second violation. The time dimension was considered as moderate time dimension and the response escalated to Level 3, Red warning.

The fourth violation occurred the same day as the third, so the time duration was considered a short time dimension. There was no escalation of response because both violations occurred in a short period of time, so response severity remained at Level 3.

The fifth violation happened on 01-05-2016, 1 year after the previous violation, which was now considered as long-term dimension. As a result, there is no response escalation to the next level, and the required response is only Level 1, basic raising of awareness.

As described in this scenario with User C, the escalation of response for non-compliance behaviour is determined by the time dimension type. The response strategy consists of five levels, in which the escalation process is based on the time dimension type. The next step is to integrate the compliance points system with the response strategy.

4.2.3. Compliance points system for non-compliance behaviour. For any non-compliance behaviour, the user loses points from their compliance rate, with different procedures applied each time the level of response severity is increased against that behaviour. The amount of points deducted increases gradually after each escalation of response severity for the same violation. The number of deducted points relies on two factors:

1) Escalation level
2) Time dimension points

The escalation process of response from one level to the next is based on the time dimension type, short time, moderate time or long time, and is used in the points' deduction equation. Each type of time dimension has a points value: short time = 1, moderate time = 2 and long-time = 1.

A user loses points for continually violating the same security policy element and ignoring each escalation level of response. The escalation level of a user and the time dimension type affects how many points the framework deducts. An equation of the proposed technique is as follows:

*Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.).*

The E.L. value is based on the escalation level the user already has, and is used together with the time dimension points The second variable in the equation would be the time dimension. There are three types of time dimension, which are short period of time, moderate period of time and long period of time, and each type is assigned a particular point: short period of time =1, moderate period of time = 2 and long period of time =1

To clarify the concept of the compliance points system in conjunction with the response strategy to non-compliance behaviour, User C's violations will be used. It is assumed that User C has frequently ignored the escalation levels, which were in response to their non-compliant behaviour with this policy. Consequently, the compliance points of User C for this particular policy will be decreased after each violation.

Violation 1: User C violated policy 1 on 01-01-2015.
User C violated the policy for the first time, so E.L. is Level 1 and the time dimension type is considered as short because it is the first violation:
Deducted Points = E.L. x T.P.
Deducted Points = 1 x 1 = 1 point, with – 1 total for policy 1

Violation 2: User C violated policy 1 on 05-01-2015

User C violated the policy for the second time, the E.L. will be Level 2 and the time dimension is moderate period. (moderate period points T.P. =2). So, Deducted Points = E.L. x T.P. Deducted Points = 2 x 2 = 4 points, with -5 points total for policy 1

Violation 3: User C violated policy 1 on 05-02-2015
User C violated the policy for the third time and in the same day of the second violation, so the E.L. is Level 2 and the time duration is short. Because this violation occurred quickly after the previous one, there was no escalation to the next level. Deducted Points = E.L. x T.P. Deducted Points = 2 x 1 = 2 points, with – 6 points total for policy 1.

Violation 4: User C violated policy 1 on 01-02-2016
User C violated the policy for the fourth time, one year after the previous violation, the E.L. will remain at Level 2 and the time duration is long. (long period points = 1). Because this violation occurred a long time after the previous one, the deducted points are: Deducted Points = E.L. x T.P. Deducted Points = 2 x 1 = 2 points, with -8 points total for policy 1

5. Discussion

It is important to investigate the ability to encourage users to comply with their information security policy by implementing some important factors, such as monitoring, persuasion, awareness and enforcement, together in one framework [34] . As such, dynamic response to users' behaviour may be an effective solution towards raising compliance levels. The main objectives of the proposed framework are the individualisation and personalisation of raising awareness. There are targeted responses for each employee when non-compliance behaviour has occurred. Each user is given a targeted response, such as raising security awareness, based on their behaviour events and the response type focuses on the element of the policy that they have violated.

The use of persuasive technology in motivating behavioural change has recently gained the attention of many researchers as a useful approach to promoting change. It is now being applied in many domains, such as marketing, health and psychology. Motivation and deterrents are examples of persuasive techniques, such as rewards and sanctions as motivation and deterrence, respectively. As such, a scoring points system (or compliance points system) is used to reward or punish users to motivate or deter them.

There are two main reasons why the proposed work is deemed necessary and worthwhile. Firstly, no studies have been known to address targeted and on-going compliance raising with regard to security policy. Secondly, while theoretical research has investigated factors affecting employee behaviour in relation to compliance with information security, none has employed these factors in an integrated framework.

From the perspective of the authors, the proposed framework can assist an organisation to gain insight into two different aspects regarding the security policy itself and user behaviour.

6. Conclusions and future work

It is important for any organisation to know the extent of success of the implementation of its security policy. In many organisations, the information security policy is only ink on paper and there is no dynamic way to measure user's behaviour with each element of the policy separately. However, decision makers in an organisation need to have a clear vision about their information security policy and this is difficult without measuring each element of the policy. As such, the proposed framework attempts to fulfil this aim. continuously subjecting users to targeted awareness raising and dynamically monitoring their adherence to information security policy should increase their compliance level.

In our future work, a simulation-based approach will be carried out to evaluate the proposed model and gain insight into its functionalities. A prototype system is being developed to support this objective.

7. References

[1] SANS, "Information Security Policy Templates," 2014. [Online]. Available: http://www.sans.org/security-resources/policies/general. (Access Date: 15 May, 2015).

[2] K. J. Knapp, R. Franklin Morris, T. E. Marshall, and T. A. Byrd, "Information security policy: An organizational-level process model," in Computers & Security, 2009, vol. 28, no. 7, pp. 493–508.

[3]Price Waterhouse Coopers PwC, "2015 INFORMATION SECURITY," 2015.

[4] 2014 EY Global information, "Get ahead of cybercrime EY's Global Information," 2014.

[5] PriceWaterhouseCoopers PwC, "INFORMATION SECURITY BREACHES SURVEY 2014," 2014.

[6] H. Chan and S. Mubarak, "Significance of Information Security Awareness in the Higher Education Sector," Int. J. Comput. Appl., vol. 60, no. 10, pp. 23–31, 2012.

[7] Economist Intelligence Unit EIU, "Power to the people? Managing technology democracy in the workplace," 2009.

[8] P. Prince, “More Than Half of Enterprise Employees Receive No Security Training: Survey Finds,” security week, 2014. [Online]. Available:http://www.securityweek.com/more-half-enterprise-employees-receive-no-security-training-survey-finds. [Access Date: 01 May, 2015].

[9] The European Network and Information Security Agency (ENISA), “The new users ’ guide :How to raise information security awareness,” 2010.

[10] H. a Qudaih, M. a Bawazir, S. H. Usman, and J. Ibrahim, “Security Awareness in an Organization,” Persuas. Technol. Contrib. Towar. Enhanc. Inf. Secur. Aware. an Organ., vol. 10, no. 4, pp. 180–186, 2014.

[11] S. Furnell and K.-L. Thomson, “From culture to disobedience: Recognising the varying user acceptance of IT security,” Comput. Fraud Secur., vol. 2009, no. 2, pp. 5–10, Feb. 2009.

[12] S. Alfawaz, K. Nelson, and K. Mohannak, “Information security culture: A behaviour compliance conceptual framework,” in Conferences in Research and Practice in Information Technology Series, 2010, vol. 105, pp. 47–55.

[13] F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, and D. Mundie, “Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies,” in 2014 47th Hawaii International Conference on System Sciences, 2014, pp. 2025–2034.

[14] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, “Effectiveness of information security awareness methods based on psychological theories,” in African Journal of Business Management, 2011, vol. 5, no. 26, pp. 10862–10868.

[15] S. Furnell, “Malicious or misinformed? Exploring a contributor to the insider threat,” in Computer Fraud and Security, 2006, vol. 2006, pp. 8–12.

[16] C. Colwill, “Human factors in information security: The insider threat - Who can you trust these days?,” Inf. Secur. Tech. Rep., vol. 14, no. 4, pp. 186–196, 2009.

[17] G. Silowash, D. Cappelli, and A. Moore, “Common Sense Guide to Mitigating Insider Threats 4th Edition,” 2012.

[18] Global consulting firm Protiviti, “Bridging the Data Security Chasm,” 2014.

[19] I. Kirlappos, S. Parkin, and M. A. Sasse, “‘ Shadow Security ’ as a tool for the learning organization,” 2015, vol. 45, no. 1, pp. 29–37.

[20] I. Kirlappos, S. Parkin, and M. A. Sasse, “Learning from ‘Shadow Security’ : Why understanding non-compliant behaviors provides the basis for effective security,” 2014, no. February.

[21] A Da Veiga and J. Eloff, “A framework and assessment instrument for information security culture,” in Computers & Security, 2009.

[22] N. Badie and A. H. Lashkari, “A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP,” 2012, vol. 2, pp. 9331–9347.

[23] M. Alotaibi, S. Furnell, and N. Clarke, “Information Security Policies : A review of Challenges and Influencing Factors,” 2016.

[24] S. Pahnila, M. Siponen, A. Mahmood, P. O. Box, F.-Oulun, and E. M. Siponen, “Employees ’ Behavior towar ds IS Secur ity Policy Compliance University of Oulu , Department of Information Processing,” October, pp. 1–10, 2007.

[25] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information Security Policy Compliance: An Empiracal Study of Rationality-Based Beliefs and Information Security Awareness,” MIS Q., vol. 34, no. 3, pp. 523–548, 2010.

[26] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, “Human Factors and Information Security : Individual , Culture and Security Environment,” in Science And Technology, 2010, p. 45.

[27] M. Harris and S. Furnell, “Routes to security compliance: Be good or be shamed?,” Comput. Fraud Secur., vol. 2012, no. 12, pp. 12–20, 2012.

[28] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, “Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,” Comput. Secur., vol. 39, no. PART B, pp. 447–459, 2013.

[29] P. Puhakainen and M. Siponen, “Research Article Improving Employees’ Compliance Through Information Systems Security Training :,” 2010, vol. 34, no. 4, pp. 757–778.

[30] G. Greene and J. D Arcy, “Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance,” in 5th Annual Symposium on Information Assurance, 2010, pp. 1–8.

[31] J. D’Arcy, A. Hovav, and D. Galletta, “User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach,” Inf. Syst. Res., vol. 20, no. 1, pp. 79–98, 2009.

[32] A. Yeo, M. Rahim, and Y. Ren, “Use of Persuasive technology to change end user’s IT security aware behavior: a pilot study,” in World Academy of Science, Engineering and Technology, 2008, vol. 2, no. 10, pp. 193–199.

[33] B. Fogg, “Persuasive computers: perspectives and research directions,” in … the SIGCHI conference on Human factors in computing …, 1998, vol. 98, no. April, pp. 225–232.

[34] M. Alotaibi, S. Furnell, and N. Clarke, “Towards dynamic adaption of user’s organisational information security behaviour,” in Australian Information Security Management Conference, 2015, vol. 2015, pp. 28–36