

2019-03-11

A Framework for Reporting and Dealing with End-User Security Policy Compliance

Alotaibi, M

<http://hdl.handle.net/10026.1/12765>

10.1108/ICS-12-2017-0097

Information and Computer Security

Emerald

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.



A Framework for Reporting and Dealing with End-User Security Policy Compliance

Journal:	<i>Information and Computer Security</i>
Manuscript ID	ICS-12-2017-0097.R3
Manuscript Type:	Original Article
Keywords:	Human factors, Information security policy, User behaviour, Information security management, Compliance management

SCHOLARONE™
Manuscripts

A Framework for Reporting and Dealing with End-User Security Policy Compliance

Mutlaq Alotaibi^{1,4}, Steven Furnell^{1,2,3} and Nathan Clarke^{1,2}

¹ *Centre for Security, Communications and*

Network Research, Plymouth University, Plymouth, UK

² *Security Research Institute, Edith Cowan University, Perth, Western Australia*

³ *Centre for Research in Information and Cyber Security, Nelson Mandela University, Port Elizabeth, South Africa*

⁴ *National Information Center (NIC), Riyadh, Saudi Arabia*
cscan@plymouth.ac.uk

Abstract

Purpose – It is widely acknowledged that non-compliance of employees with information security policies is one of the major challenges facing organisations. This research has proposed 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.

Design/methodology/approach – The proposed model is based on two main concepts: a taxonomy of the response strategy to non-compliant 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 non-compliant behaviour.

Findings – A prototype system has been developed to simulate the proposed model and work as a real system that responds to the behaviour of users (reflecting both violations and compliance behaviour). In addition, the model has been evaluated by interviewing experts from academic and industry. They considered the proposed model to offers a novel approach for managing end users’ behaviour with the information security policies.

Research limitations/implications- Psychological factors were out of the research scope at this stage. The proposed model may have some psychological impacts upon users therefore this issue need to be considered by studying the potential impacts and the best solutions.

Originality/value- Users being compliant with the information security policies of their organisation is the key to strengthen information security. Therefore, when employees have a good level of compliance with security policies, this positively affects the overall security of an organization.

Keywords Human factors; Information security policy; User behaviour; Information security management; Compliance management.

1- Introduction

An Information Security policy is defined as a set of rules and regulations that describe how to make information technology safe and protect it from potential threats (Cosic & Boban 2010), or in others

words, it informs users what their responsibilities are, what they must do and what they must not do. There is a wide belief that compliance of users with information security policies is the foundation of securing an organization's information assets (Al-Omari et al. 2011) (Cosic & Boban 2010) (Kirlappos et al. 2015). Traditionally, information security policies have been used by organizations as a basis to manage their information security in which that users are expected to comply with. However, organisations are now having some issues regarding the extent of employee adherence to the information security policies. A significant proportion of researchers and security professionals consider end users or the human factor as a weakest link in the information security chain[5](Cushing 2012)(Bashorun et al. 2013)(Da Veiga & Eloff 2010). An information security survey conducted by (HM Government 2015) implied that most large organizations have now implemented their own documented information security policy, 98%. Therefore, this is a good indication that the majority of organizations are aware of the significance of having an information security policy. However, having such a policy in place is not a guarantee that users will adopt the desired behaviour, they may not behave as they are expected, whether due to an intentional behaviour to violate the policy, or even a lack of understanding of its contents. Non-compliant employees or those who are unaware of information security policy have become major concern to organizations since they pose a threat to a computing environment security. In Ernst and Young (EY's) Global Information Security Survey (EY'S Global information Security Survey 2013 2013), 57% of the surveyed organizations considered their employees to be the biggest threat to an information security, whilst 38% indicated that unaware or careless employees pose the greatest threat. This claim is strongly supported by (HM Government 2015), which indicates that 75% of large organizations suffered a staff related breach and nearly 31% of small organizations had a similar occurrence. As a result, the problem of employees being unaware or ignorant of their responsibilities in relation to information security is still an open issue (Alotaibi et al. 2016).

This study proposes 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 non-compliance 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. 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. A prototype system has been developed to simulate the proposed model in order to provide a clear image of its functionalities and how it is meant to work. Therefore, it was developed to work as a system that responds to the behaviour of users (whether violation or compliance behaviour) in relation to the information security policies of their organisations. After designing the proposed model and simulating it using the prototype system, the model has been evaluated by interviewing different experts with different backgrounds from academic and industry sectors. Thus, the interviewed experts agreed that the identified research problem is a real problem that needs to be researched and solutions need to be devised. It also can be stated that the overall feedback of the interviewed experts about the proposed model was very encouraging and positive. The expert participants thought that the proposed model addresses the research gap, and offers a novel approach for managing the information security policies.

In this paper, the theoretical background of the research model is illustrated in section two. It then presents a novel model for monitoring security policy compliance in section three. Section four shows a prototype system that simulates the proposed model in order to provide a clear image of its functionalities and how it is meant to work. In section five the experts' evaluation process of the research is discussed. Finally, Section six draws conclusions and suggests future work in this domain.

2- Theoretical background

An information security policy is considered to be the cornerstone of information security management and an organizational approach that mitigates potential threats from employees in relation to dealing with information assets in a secure manner (Peltier 2016). In the workplace, all employees should be made aware of acceptable and unacceptable user behaviour and the first step to achieving this is to implement a formal information security policy.

2.1 An Overview of Information Security Policy

According to (SANS 2014) , 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”. There are three major sources of the necessary information on security requirements (ISO 2013)(Alotaibi et al. 2015):

- Risk assessments or evaluations of potential risks to the organization and overall business objectives and strategies should be taken into account in this process.
- The legal, regulatory and contractual requirements that an organization and its partners, such as contractors and service providers, need to adhere to and their socio-cultural environment.
- An organization’s vision regarding dealing with information assets and the business requirements for information handling, such as storing, processing and communicating, that has been developed by the organization.

Information security policies should be organised into various meaningful categories (Stahl & Pease 2011), for example, physical security policy, password security and internet usage security, which helps employees to better understand it.

2.2 User’s behaviour with information security policy

In the information security field, the human factor is the vulnerability considered to be the most unpredictable one. In addition, the human factor is characterized by being the most variable and thus the hardest to control. When organizations deal with the human factor, the procedure for placing staff with the right level of commitment to the policies of Information technology should contain an assessment of the security behaviour of individual members of staff. According to (Colwill 2009), organizations may believe that implementing more advanced technical controls will minimize the risk associated with the human factor. However, they should understand that this factor still poses the greatest threat and increases their vulnerability and thus consider a balance between technical and non-technical controls, maintaining a holistic perspective (Jones & Colwill 2008).

A number of studies have suggested that when the level of compliance with and acceptance of the established security polices and controls amongst the members of staff in an organization is measured, the success of those policies can be anticipated. Members of staff can show different levels of compliance. There are four models to categorize user security behaviour with an information security policy, as follows (Alfawaz et al. 2010):

- Not knowing-not doing: In this model, the user has no idea about the information security of an organization and does not understand the security requirements. As a result, the user will violate the security rules or not perform the right behaviour.
- Not knowing-doing: In this model, the user does not have an understanding of the security policy and is not provided with the IS requirements of an organization; nevertheless, the user performs the right behaviour by following the rules.
- Knowing-not doing: In this model, the user knows the necessary information about the security policy of his or her organization and has the required skills and knowledge; however, the user neglects to perform the right behaviour or violates the security policy

- **Knowing-doing:** In this model, the security policy is in place and well delivered to the user; as a result, the user is carrying out the right behaviour. Therefore, the user's intention is not to violate the information security policy by following the required security rules.

Non-compliance with an information security policy can be divided into two main types: intentional and unintentional. An Intentional non-compliance behaviour involves an intentional misuse of an organization's information assets and the main motivation for this sort of threat is malicious intent to bring harm to an organization. However, Unintentional non-compliance behaviour can be the result of non-malicious users making errors or due to a lack of awareness or even carelessness (CERT® Division 2013). The following diagram (Fig. 1) explains the different types of non-compliance types.

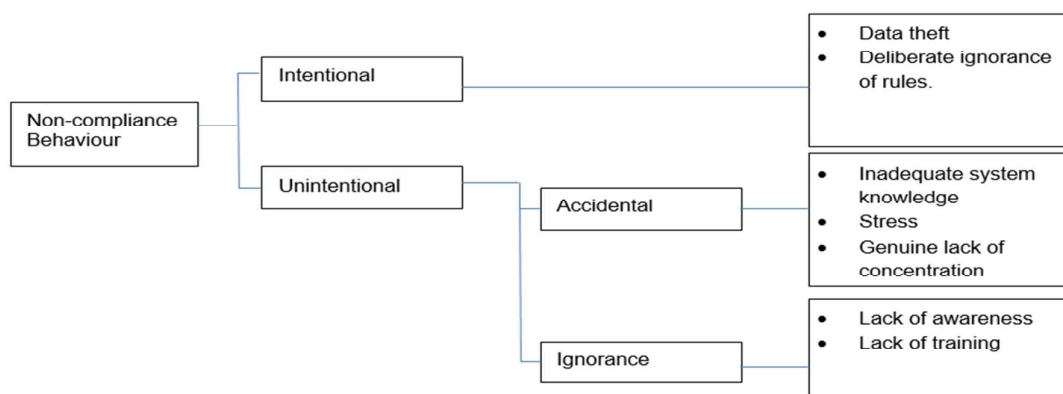


Fig1 - Non-compliance behaviour types

Non-compliance behaviour can be mitigated but it is not an easy problem to solve. It can be countered via multiple stages of defence that may consist of policies, procedures and technical controls (Silowash et al. 2012). Further to this, management needs to have an obvious vision regarding some significant aspects that can impact upon the organization, including its users, organisational culture, security policy and procedures, and technical environment.

3- A Framework for Reporting and Dealing with End-User Security Policy Compliance

In this study, we have designed a novel model that provides a comprehensive framework for raising the level of compliance amongst end-users, by monitoring, measuring and responding to users' behaviour with an information security policy (see Fig. 2). In addition, a scoring system (compliance points) is used to apply supplementary rules within the proposed model. The goal of utilising 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. By using this model, each element of the security policy is measured, which provides organisations with a clear vision about their security policies. For example, an organisation can determine which element of its policy is operating most or least effectively (e.g. based upon then minimum or maximum number of violations during a certain period of time).

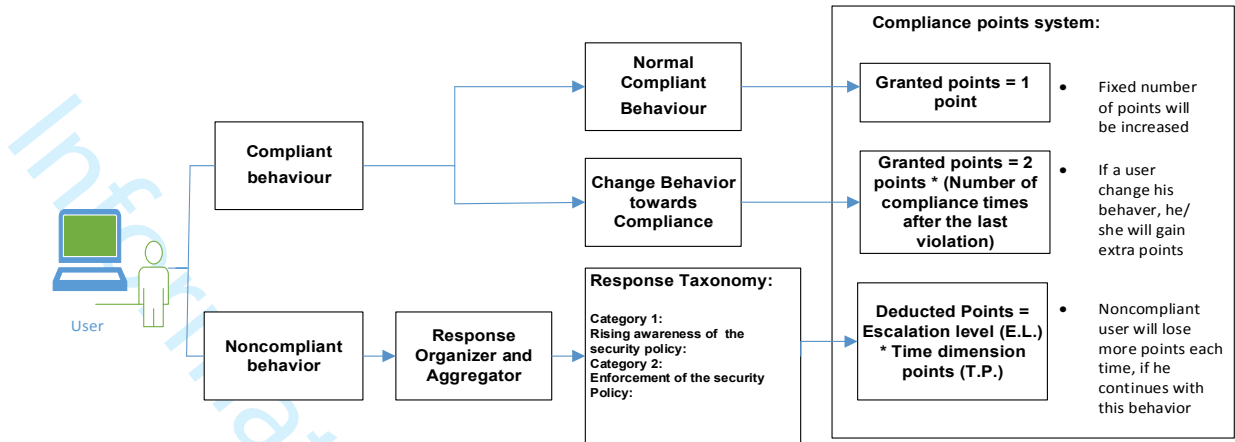


Fig 2- A Framework for Reporting and Dealing with End-User Security Policy Compliance

3.1 Compliance behaviour

A user is considered to be compliant when they show the desired behaviour regarding the information security policies and rules. To measure compliance, two methods of evaluating users’ behaviour are suggested:

- 1- **Based on the explicit action**, for when a user performs certain actions of compliance, for example, they have changed their password after six months in response to the policy requiring this specific action (the changing password policy);
- 2- **Based on the elapsed period of time** (the compliance period), considers a user as compliant if they do not violate a security policy during a set period of time, for example, if a user has not browsed non-work related websites for a period of three months.

A user that adheres to the information security policies earns compliance points for behaviour in relation to each element, and each element of the information security policy has a separate tracker of points for each user. There are two mechanisms for granting points: points awarded for normal compliance behaviour, and points awarded for changing behaviour towards compliance (see Fig. 3).

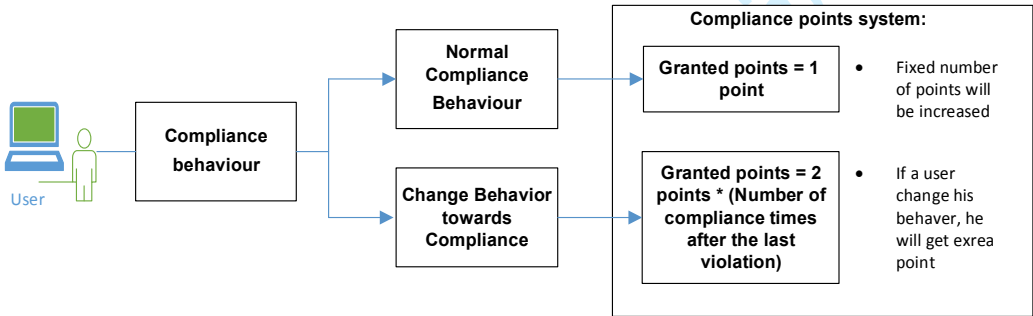


Fig 3- Dealing with compliance behaviour

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.

3.1.1 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 User 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. In short, the user is rewarded for normal good behaviour that is in line with policy.

Table 1. User A actions

#	Actions and date	Policy description
Action 1	User A changed his password - 01-01-2016	Passwords must be changed every six months.
Action 2	User A changed his password - 01-06-2016	
Action 3	User A did not browse non-work-related websites - 01-01-2016 to 01-03-2016	Browsing non-work-related websites is prohibited.
Action 4	User A did not browse any non-work-related websites - 01-03-2016 to 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.

3.1.2 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. This mechanism has been proposed because if a user loses a high number of compliance points, that will take the user long time to get back to the normal level of compliance. Moreover, a behaviour history of the user is kept with details in the system records, therefore, it can easily be traced back.

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 User B has not changed his password for three times (24 months). Therefore, due to his noncompliance behaviour, he had lost points for three 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. In this way, there is no incentive for users to change to non-compliance in order to seek the additional reward for becoming compliant again, as the penalties applied for non-compliance must be recovered before they can make any gains.

3.2 Non-compliant 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 Fig. 4).

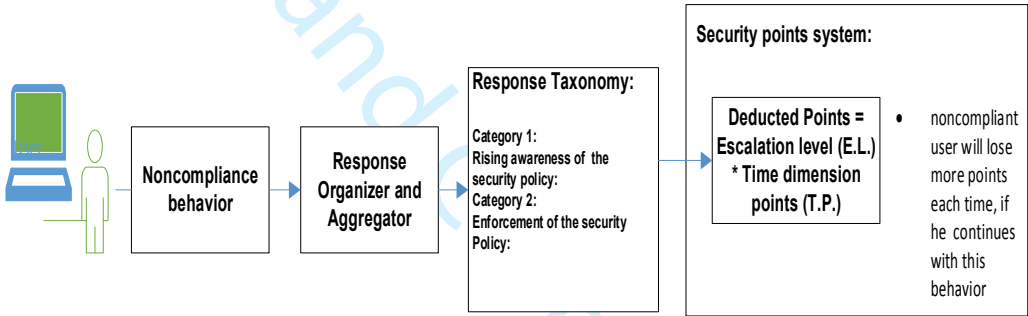


Fig 4- Dealing with non-compliance behaviour

3.2.1 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.

3.2.3 Response taxonomy

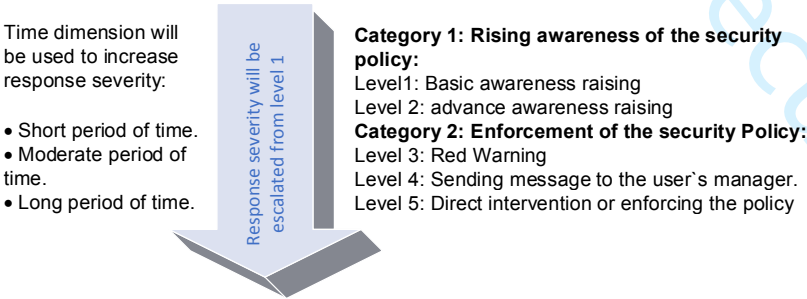


Fig 5- Response taxonomy with the time dimensions

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 (As seen in figure 5). 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: Short, Moderate, and Long. The three types of time dimensions (short time, moderate time and long-time) would be configurable by the organisation itself, but we have set illustrative defaults values of the three types in the table in order to show the principle.

Table 2. Time dimension types

Time dimension	Expected behaviour	Escalation to the next level
Short time (e.g. less than 24 hours)	Users may be unaware of the information security policy.	The sequence of events is 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. There will be not enough time for any significant intervention, so the time should be short.
Moderate time (e.g. 24 hours up to 6 months)	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. There was enough time since the last violation, and the user had received a response for the last violation.
Long time (e.g. more than 6 months)	Users may forget details of the information security policy, due to a period of elapsed time.	In this instance, users will require an awareness reminder from Category 1: raising awareness of the information security policy. The period between the new violation and the last violation should be a 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 3 describes the following scenario: User C has violated a particular information security policy, policy 1, many times over a two-year time period.

Table 3. 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 on 05-01-2015
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 five 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, here because the user committed the same violation. 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.

3.2.4 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 point. The second variable in the equation would be the time dimension. The three types of time dimensions (Short time, moderate time and long-time) would be configurable by the organisation itself, but the authors have set the recommended defaults values of the three types as shown below.

- Short period of time =1
- Moderate period = 2
- 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.

Table 3. User D violations

Violation#	Description & Date	Response & compliance points
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 long because it is the first violation: Deducted Points = E.L. x T.P. Deducted Points = $1 \times 1 = 1$ points, with -1 as a 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 = $2 \times 2 = 4$ points, with -5 points as a total for policy 1.
Violation 3	User C violated policy 1 on 07-02-2015	User C violated the policy for the third time, the E.L. will be Level 3 and the time duration is moderate period. (moderate period points T.P. = 2). So, Deducted Points = E.L. x T.P. Deducted Points = $2 \times 3 = 6$ points, with -11 points as a total for policy 1
Violation 4	User C violated policy 1 on 07-02-2015	User C violated the policy for the fourth time and in the same day of the second violation, so the E.L. is Level 3 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 = $3 \times 1 = 3$ points, with -14 points as a total for policy 1.
Violation 5	User C violated policy 1 on 07-05-2015	User C violated the policy for the fifth time, the E.L. will be Level 4 and the time duration is moderate. Deducted Points = E.L. x T.P. Deducted Points = $4 \times 2 = 8$ points, with -22 points as a total for policy 1.

4. Prototype implementation of the proposed model

Having offered a theoretical explanation of the model used for monitoring users' security policy compliance in the previous section, the next phase of the research concentrates upon developing a prototype system that simulates the proposed model and describe how to score security policy compliance and violations along with a taxonomy for the response strategy. The MATLAB environment was selected to develop the prototype system. With the purpose of operating the prototype system, some scenarios of the potential behaviour of users in relation to the information security policies of their organisations need to be assumed and simulated. Therefore, several scenarios were created and used during the simulation process, thus helping to explain the prototype system and how it works. As such, the scenarios of the potential behaviour of the users in relation to security policies were used to feed the prototype system (as an input for the prototype) in order to obtain a result and understand how it would work in a real environment.

4.1 Information security policies used

A variety of information security policies were selected from different types of policies, such as password security policy, Internet usage policy, clean desk policy and email usage policy, to be used during the simulation process. Thus, twenty elements of the information security policies were selected for use within the simulation process.

- Computer workstations must be locked when workspace is unoccupied
- Employees are not allowed to remove or disable anti-virus software.
- Electronic storage devices, such as USBs and DVDs that contain restricted information, should be kept secure
- Computer workstations must be shut down completely at the end of the working day.
- User level passwords, such as those used for application, web, email and desktop accounts, must be changed every four months.
- Passwords must not be added to or written in an email message, transmitted in any electronic form or revealed to anyone over the phone, via a questionnaire or in a security form.
- All passwords should meet or exceed the following guidelines: contains at least 12 alphanumeric characters, contains both upper and lower-case letters, at least one number and at least one special character
- Users are not allowed to utilise password memorisation, which is available in some applications as an additional feature, such as the web browser ‘remember password’ feature.
- Employees must not download, visit or view any illegal materials on the internet
- Employees must not undertake deliberate activities that wastes staff effort or networked resources.
- Personal use of the internet must not cause a significant increase in resource demand
- Employees must not download unauthorised software or files for use without prior authorisation from the IT department and their manager.
- Employees must not play any games on the internet.
- Employees must not download copyrighted material, such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval
- The organisation’s email account should be fundamentally utilised for business that is related to the organization.
- The organisation’s email system must not be utilised to create or distribute any offensive or disruptive messages.
- Sending chain letters or joke emails from an organisation email account is strictly prohibited.
- Employees must not send unprotected, sensitive or confidential information externally.
- Forwarding of the organisations confidential messages to external locations is not allowed.

Security events (violations) are recorded and captured using two methods: electronically from security monitoring and control devices (e.g. in cases where a user spends a lot of time on social networks or has not changed his password for a long time) or manually from security reports or line managers (e.g. in cases where a user leaves their computer unlocked). The event sources may include, but are not limited to: line managers, internet usage, email usage, application level and user’s machine. According to false positive (violations) that the system may trigger there will be an administrator in order to check users appeal about violations.

Each of the above policy is then defined in terms of the following characteristics:

- **Policy number:** A unique number to be used within the prototype.
- **Policy description:** A clear explanation of each policy element.
- **Weighted average:** This is based on the policy’s importance from an organisation’s perspective. A scale of the policy elements indicating their importance incorporates 0.1, 0.2, 0.3,.....1, with policies ranked 1 being very important (100%), 0.2 less important (20%) and

0.1 less important (10%). The main aim of identifying the weighted average of each policy element is that it can be used later in calculating the overall compliance points for each user for all the policies.

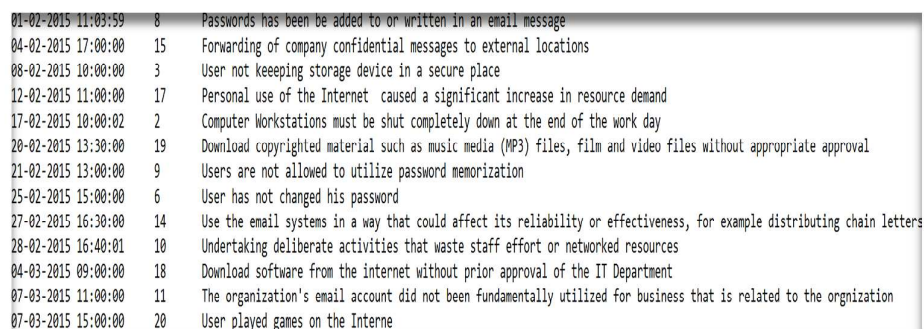
- **Elapsed time:** This is used to determine the users' period of compliance with each policy element in order to grant points to the compliant users

4.2 Scenarios of some potential behaviours of users

With the purpose of operating the prototype system, some scenarios of the potential behaviour of users in relation to the information security policies of their organisations need to be assumed and simulated. Therefore, several scenarios were created and used during the simulation process, thus helping to explain the prototype system and how it works. Five different types of user behaviour were chosen in order to create the following scenarios:

- **Scenario 1: User A Compliant behaviour (Optimal behaviour).** User A is very compliant with all the security policies. No violations during the simulation period with each policy element.
- **Scenario 2: User B Unaware behaviour.** User B is not compliant with all the elements of the security policies (20 policies) during the first six months of the simulation period. Only one violation during the simulation period with each policy element.
- **Scenario 3: User C Changeful behaviour.** In this scenario, User C is non-compliant, then becomes compliant, and then becomes noncompliant again. 5 or 6 violations during the simulation period with each policy element.
- **Scenario 4: User D Forgetful behaviour.** User D is forgetful in regard to complying with the information security policies of his/her organisation. 2 violations during the simulation period.
- **Scenario 5: User E Very noncompliant behaviour.** User E is very noncompliant with all the elements of the security policies. User E has not gained any compliance points on any of the elements of the policies because User E never passed the elapsed time of each element without a violation. 13 or more violations during the simulation period.

Each scenario represents a specific type of user behaviour, which were all assumed to apply to each of the twenty security policy elements. Each scenario was codified by creating a series of security events in the form of a log file, as illustrated in Figure 6.



01-02-2015 11:03:59	8	Passwords has been added to or written in an email message
04-02-2015 17:00:00	15	Forwarding of company confidential messages to external locations
08-02-2015 10:00:00	3	User not keeping storage device in a secure place
12-02-2015 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
17-02-2015 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day
20-02-2015 13:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
21-02-2015 13:00:00	9	Users are not allowed to utilize password memorization
25-02-2015 15:00:00	6	User has not changed his password
27-02-2015 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters
28-02-2015 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
04-03-2015 09:00:00	18	Download software from the internet without prior approval of the IT Department
07-03-2015 11:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the organization
07-03-2015 15:00:00	20	User played games on the Internet

Fig. 6- Illustrative extract of a user log file of violations

4.3 The output of the simulation

An input interface within the prototype facilitated input of the settings as well as the output of the simulation, as shown below in Figure 7.

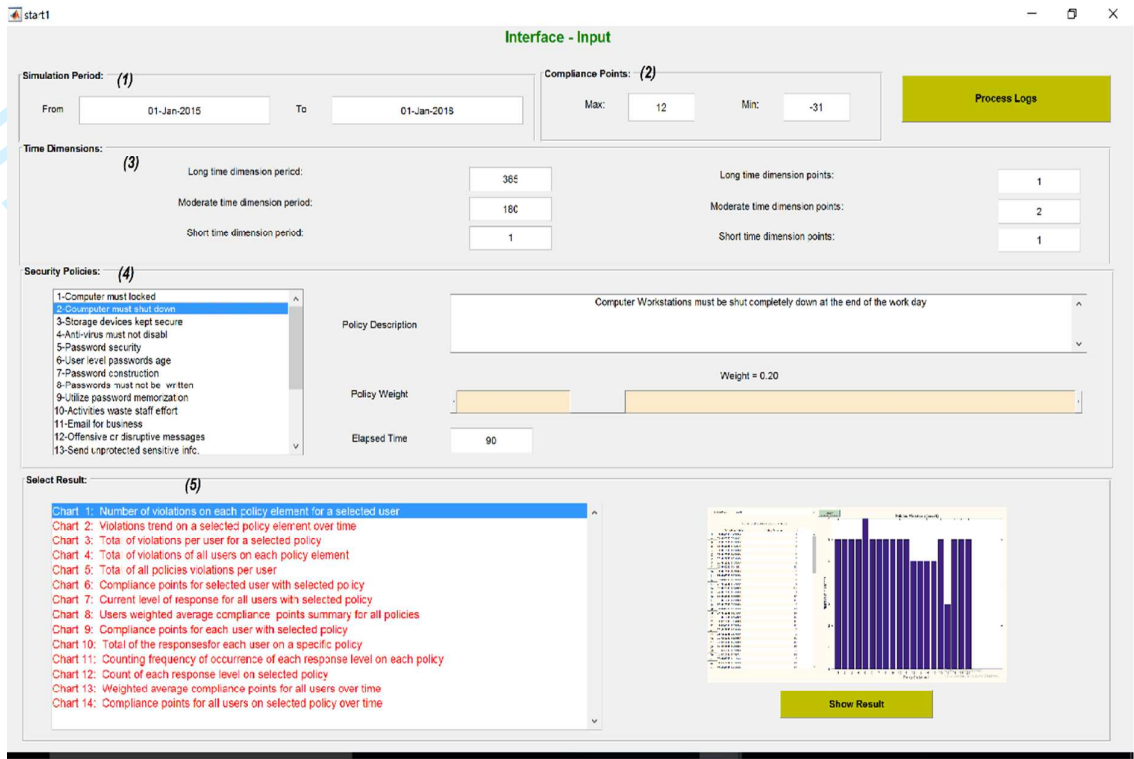


Fig. 7- Main interface of the prototype system

The main input interface was comprised of five main parts:

- 1) Simulation period. The simulation duration could be entered through this part. The simulation period had two values: start date (From) and end date (To).
- 2) Compliance points level: The maximum and minimum level of compliance points could be set via this part.
- 3) Time dimensions: Each time dimension type has two values for settings: duration, meaning the time period between violations; and points, which is used in the compliance points system. The default value of the duration was set in days but it could have been set in seconds, minutes or hours. As seen in Figure 2, each time dimension type had a specific duration value, as follows:
 - Short time dimension = 1 - This means the duration between violations is considered short if it is less than 1 day.
 - Moderate time dimension = 180 - This means the duration between violations is considered moderate if it is greater than 1 day and less than 180 days.
 - Long-time dimension = 365 - This mean the duration between violations is considered long if it is greater than 180 days.
- 4) Security policies: It is possible to enter and manage the settings of each element of the security policies via this part of the interface. These settings are as follows:
 - Policy weight: Each element of the policies has a weighted average number based on its importance. Therefore, there is a GUI slider within the interface that displays a range of values (from 0.1, 0.2, 0.3,, 0.9 till 1) and has an indicator, or knob, which shows the current setting.
 - Elapsed time: It is possible to set and change the value of the elapsed time for each policy element via this part of the interface.
- 5) Results selection, from this part of the interface, it is possible to select a desired type of the results and present them with their data and graphs. These results include the following:

- Violations trend on a selected policy element over time.
- Total number of violations of all users of each policy element
- Current level of the response taxonomy for all users with a selected policy
- Total number of responses for each user for a specific policy element
- Counting the frequency of occurrence of each response level for each policy element
- Number of violations of each policy element for a selected user
- Total number of violations per user for a selected policy element
- All policies violations per user
- Compliance points for a selected user with a selected policy
- Users weighted average compliance points summary for all policies
- Compliance points for each user with selected policy
- Weighted average compliance points for all users over time
- Compliance points for users on selected policy over time

Some of the above options from the results section are further explained in the following sections.

4.3.1 Number of violations of each policy element for a selected user

The prototype system enables queries about the total number of violations for each policy element for any users. Thus, a comprehensive report about a user's violations of each policy element is provided by the system, which can assist an organisation in measuring users' behaviour. For example, in Figure 8, the example of non-compliant User C is selected in order to present his violations of each element of the policies.

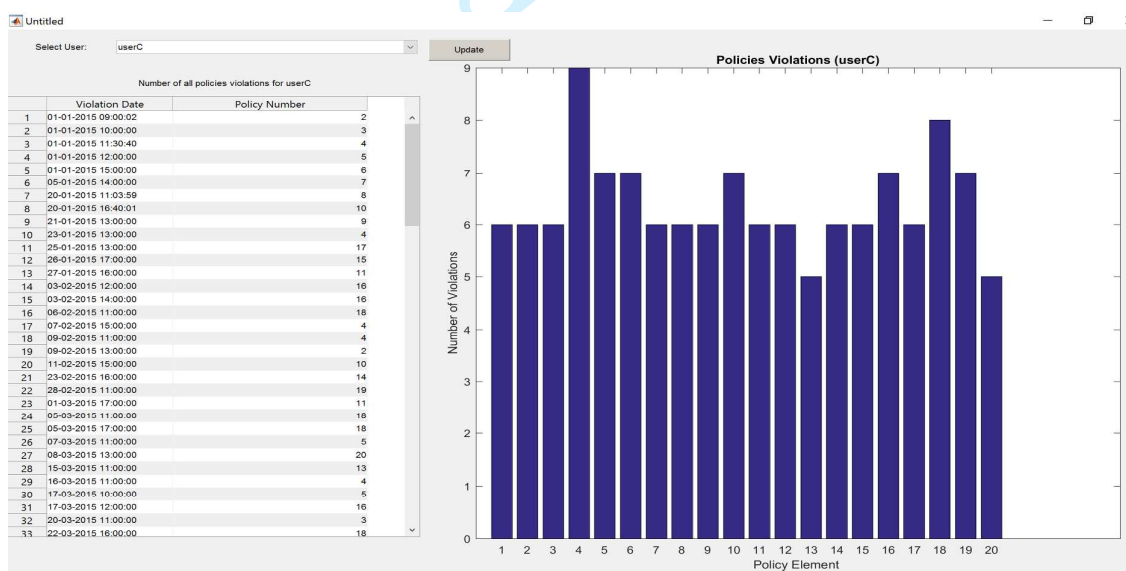


Fig.8- Screenshot for number of violations on each policy element for the User C

4.3.2 Compliance points for a selected user with a selected policy

The trend of the compliance points of a user with any security policy element over time can be presented in a chart. For example, the trend of User D's compliance with element 2 of the security policy over the simulation period is presented in Figure 9.

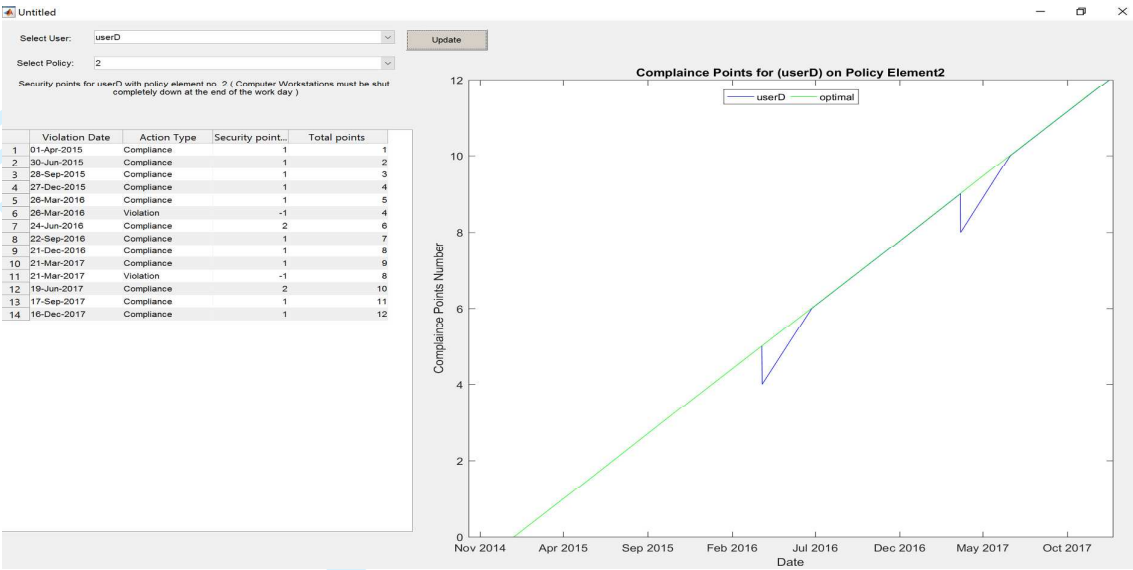


Fig. 9- Compliance points of User D for policy element 2

As demonstrated in the chart, there are two lines; one is for User D’s compliance points and the other is for the optimal points that the user is supposed to have. As seen, User D lost points twice during the three years. For more details, on the left side of the chart is a log or history of all actions taken by the prototype system in terms of increasing or deducting points from the user compliance points rate for that policy element.

4.3.3 Violations trend on a selected policy element over time

The system also offers the option to view from the perspective of violation trends over time for each policy element. This can help an organisation to gain some useful information on each policy element, such as the peak number of violations of a specific policy element in a certain period of time. In Figure 10, all the users’ violations (Users A-E) of policy element 16 over the three years of the simulation are presented in the form of a graph and data. By using this graph, it is easy to identify which particular period has a maximum or minimum number of violations.

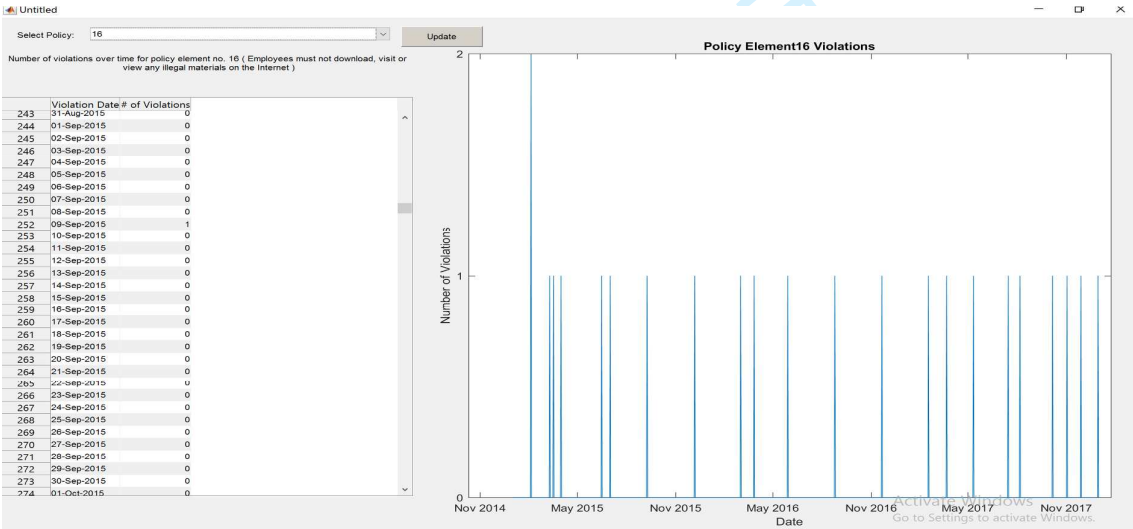


Fig. 10- Violations trend for policy element 16

4.3.4 Weighted average compliance points for all users over time

The trend of the weighted average compliance points of all users with all elements of the policies over a time is presented in this chart. Therefore, an organisation will be able to keep track of each user's behaviour with the whole policy. Figure 11 shows the trend of the weighted average compliance points of all the users over the simulation period of three years.

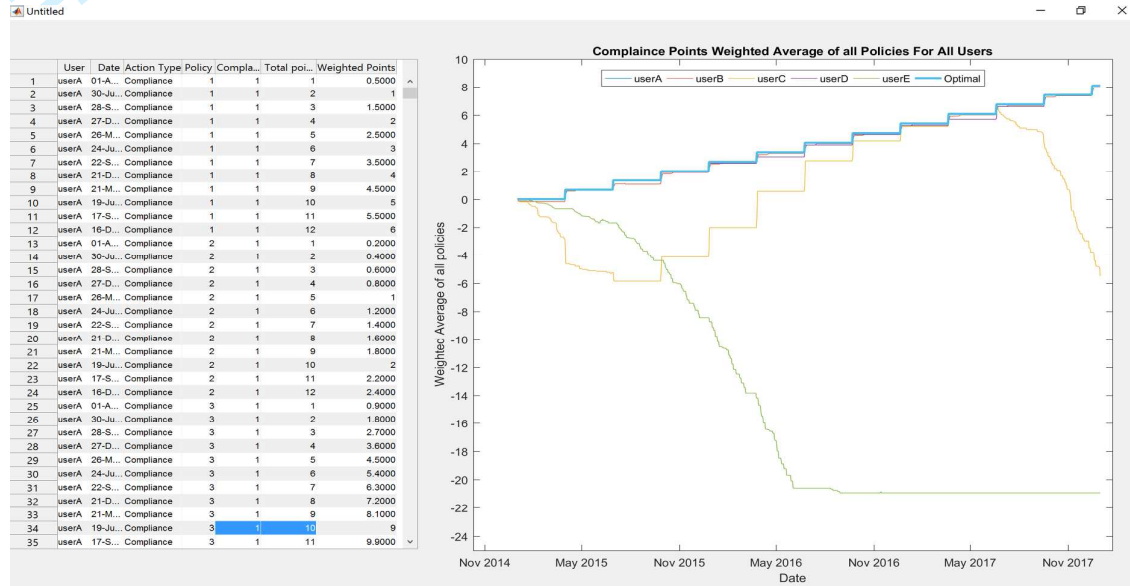


Fig. 11- Weighted average compliance points for all users over time

As seen in the chart, the optimal weighted average compliance points trend over the three years is presented. As such, any user's weighted average compliance points can be compared against the optimal, which gives an insight into user behaviour over a certain period of time.

As an example, User C weighted average compliance points give a clear image of his/her behaviour during the three years of the simulation, during which time User C had three main changes of behaviour. Firstly, he/she lost compliance points due to his/her non-compliance behaviour in the period from the beginning of the simulation almost until November 2015. Secondly, after that date, the user changed his/her behaviour towards compliance, matching the optimal points in November 2016. User C continued with compliance behaviour in line with the optimal level almost until July 2017. However, the third change of User C's weighted average compliance points was from almost July 2017 until the end of the simulation when User C lost points due to his/her non-compliance behaviour.

4.3.5 Compliance points for users on selected policy over time

The trend of the users' compliance points with a selected policy element, the minimum level of the compliance points and the optimal points for that policy element are all presented in this chart of the simulation period. To explain this output of the prototype system, the users' behaviour in relation to policy element 9 is selected as an example. Figure 12 shows the trend of compliance points of all users for policy element 9.

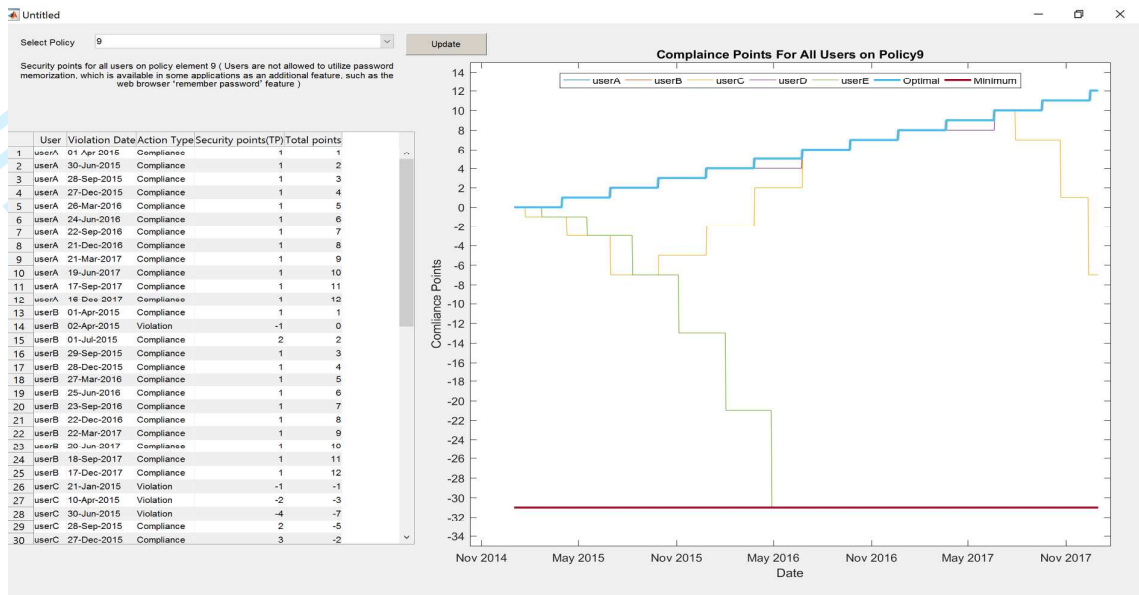


Fig. 12- Screenshot for Compliance points for users on policy element 9 over the simulation period

As can be seen in the chart, all the users' compliance points plus the optimal compliance points and the minimum points are presented over the three years. The trend of the optimal points increases 1 point every three months during the three years because the elapsed time setting of policy element 9 is 90 days. User A's compliance points for policy element 9 exactly match the optimal level for that policy during the three years. However, if we look at the worst case, which is User E, we find that their compliance points dropped from the beginning until the end of the simulation, which means this user exhibited security noncompliant behaviour with this policy element during the three years.

5 Evaluation of the proposed Model

In addition to the practical simulation of the proposed model, a further qualitative evaluation method was carried out. The main objective behind this evaluation was to gain feedback received from experts from different sectors including industry and academic. The internet was used to search for the appropriate experts, and the selection criteria were made based on the following points:

- Members of scientific conferences committees related to the research area
- Authors of work thematically related to research articles in scientific journals.
- Scientists from related fields working also as lecturers or as administrative staff members in educational institution.
- Practitioners and professionals in the field of information security, information security officers or administrations.

The participants, who were all experts on the subject matter, were carefully selected and a set of questions was accurately designed and presented to the experts. There was a detailed interview with the participants and different aspects regarding the proposed model were discussed, using the open-ended questions. In total, 14 experts (7 academics and 7 practitioners) have taken part in this evaluation.

All the interviews were conducted remotely over Skype video calls, except one interview which was held on the basis of a face to face meeting. Because the interviewees were in different countries, a Skype interview was selected as an effective way to hold the interviews with the experts. Prior to the expert interview, a brief video about the research concept, the proposed model and the prototype system was prepared and sent to each expert in order to help them to have an overview of the

conducted research and to be familiar with it. The demonstration video is a proximately 15 minutes in length.

In general, all the interviewed academics and practitioners agreed that the research problem undertaken was valid, as well as they strongly believed that it is still open issue.

Feasibility at the operational level, 11 of the experts indicated that the proposed model is very feasible and attainable at operational level. One expert was of the belief that the model would be feasible for large organisations with adequate resources in place but it might be not easy for a small or medium size enterprise. Two participants mentioned that the approach is feasible but the hardest part will be the reporting of non-compliance with security policies.

According to using the concept of the response taxonomy for non-compliance behaviour, the feedback of the experts on this concept were of the general opinion that it would make difference in changing users' behaviour towards compliance. Some of them believe that the positive issue was using of targeted response for users' behaviours, which is the response taxonomy concept within the model.

Thoughts on using the concept of compliance points system, experts were of general opinion that the proposed concept would be very beneficial. They found the strength of the model to be that employers will have more proof and assurance that their users are following policies, adds a lot of value on this issue. Also, they were of opinion that the model presented an approach that can measure users' compliance and can give them points. added that it would provide huge and effective type of output and results to highlights where the areas or departments that need more focus are or more enhancement, more security awareness, more security training, more attention from the information security side. The strength of the approach was, the system provides an in-depth data for analysis, which can certainly point out the potential security holes with in an organization at user level

Possibility of Implementation of the proposed model, this question of evaluation was designed to investigate to what extent the proposed model can be implemented from the interviewed experts' point of view. The experts were of the belief that it would be possible to deploy such a system. They thought that it is very feasible, because nowadays compliance issues are raising and organisations are searching for new solutions to measure it. Some experts also stated that how feasible a system will be for an organization will depend on a number of things: 1) Organizational policies on monitoring user activities. 2) Determining cost of investment & its return. 3) Life cycle of the system.

Usefulness of the proposed model, it is vital to investigate the benefits that an organisation may gain by implementing such a model. The interviewees generally agreed that the model would be beneficial to organisations. They indicated that it will be useful for an organisation, but users may do not like been monitored or compared. Moreover, they added that this model will help the administrator by saving the time and focus only on security policies that have noncompliant behaviours.

As regards weaknesses, the concern of ethical and psychological issues regarding monitoring users' behaviours was raised by tow experts. Furthermore, some experts thought that the used data to run the prototype system was not real data. Some concerns regarding the proposed model were raised, which are the psychological factor that the model may have upon users, the ability for monitoring users' behaviours technically and the ethical issue of the behaviour monitoring. Another aspect, legal factors need to be regarded. For example, some organisations may disagree to a system that permanently monitoring the users' behaviour. Moreover, in practical side, it may be very tricky to setup a system and get the desired effects.

1
2
3
4
5
6
6 Conclusion and Future research

7 The main objective of this research was to define and propose an advanced model or approach that
8 able to provide a comprehensive framework for raising the level of compliance amongst end-users,
9 with the aim of describing a framework how to score security policy compliance and violations along
10 with a taxonomy for the response strategy. This objective was achieved by investigating the current
11 state of the art to define the gap as regards the information security policies and users' behaviours, by
12 carefully reviewing the possible and most appropriate approaches to tackle the problem. From the
13 perspective of the authors, the proposed framework can assist an organisation to gain insight into two
14 different aspects regarding the security policy itself and users behaviour. Gaining insight on an
15 implemented security policy. It is important for any organisation to know the extent of success of the
16 implementation of its security policy. As such, the proposed framework attempts to fulfil this aim.
17 Some examples of how an organization might gain insight on its security policy are listed below:

- 18
19
 - Policy elements with low compliance levels
 - Statistics about response levels:
 - Policy elements with high compliance levels
 - Level of compliance points for each policy element
23

24
25 Gaining an insight into users' behaviour. The proposed framework assists organisations in monitoring
26 and measuring users' behaviour with each element of the security policy in a dynamic way. some
27 examples of how an organisation could gain insight on its users' behaviour are listed below.

- 28
29
 - Users' violations
 - Statistics about response levels
 - Weighted average compliance points of each user
 - User's level of compliance points for each element of the policy
33

34
35 Thus, a comprehensive model was designed and a prototype system developed to simulate the
36 proposed model using different scenarios to validate the defined concept, as well the proposed model
37 and its prototype system were evaluated by experts within the research domain. The overall feedback
38 of the interviewed experts about the research, as a whole and the proposed model, was very
39 encouraging and positive. In addition, the strengths and limitations of the proposed model were
40 recognised and flagged for further research work. However, a complete version of the prototype
41 system need to be developed based on the proposed model and implemented in a real environment
42 within an organisation. This will be beneficial in order to understand the effectiveness of such a
43 system in encouraging users to be compliant with information security policies. Moreover, making the
44 system working in a live environment will facilitate evaluating the system and finding any limitations.
45
46

47
48
REFERENCES

49 Al-Omari, A., El-Gayar, O. & Deokar, A., 2011. Security policy compliance: User acceptance
50 perspective. In *Proceedings of the Annual Hawaii International Conference on System Sciences*.
51 pp. 3317–3326.
52
53 Alfawaz, S., Nelson, K. & Mohannak, K., 2010. Information security culture: A behaviour
54 compliance conceptual framework. In *Conferences in Research and Practice in Information*
55 *Technology Series*. pp. 47–55.
56
57
58
59
60

- 1
- 2
- 3 Alotaibi, M., Furnell, S. & Clarke, N., 2016. Information security policies: A review of challenges
- 4 and influencing factors. In *2016 11th International Conference for Internet Technology and*
- 5 *Secured Transactions (ICITST)*. pp. 352–358.
- 6
- 7 Alotaibi, M., Furnell, S. & Clarke, N., 2015. Towards dynamic adaption of user's organisational
- 8 information security behaviour. In *Australian Information Security Management Conference*. pp.
- 9 28–36.
- 10
- 11 Bashorun, A., Worwui, A. & Parker, D., 2013. Information security: To determine its level of
- 12 awareness in an organization. In *2013 7th International Conference on Application of*
- 13 *Information and Communication Technologies*. Ieee, pp. 1–5. Available at:
- 14 <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6722704>.
- 15
- 16 CERT® Division, 2013. Unintentional Insider Threats : A Foundational Study. , (August), p.91.
- 17 Available at: www.sei.cmu.edu.
- 18
- 19 Colwill, C., 2009. Human factors in information security: The insider threat – Who can you trust these
- 20 days? In *Information Security Technical Report*. Elsevier Ltd, pp. 186–196. Available at:
- 21 <http://linkinghub.elsevier.com/retrieve/pii/S1363412710000051> [Accessed September 8, 2014].
- 22
- 23 Cosic, Z. & Boban, M., 2010. Information Security Management - Defining Approaches to
- 24 Information Security Policies in. In pp. 2005–2007.
- 25
- 26 Cushing, T., 2012. Humans: Still The Weakest Link In The Security Chain. Available at:
- 27 [https://www.techdirt.com/articles/20120810/18401819991/humans-still-weakest-link-security-](https://www.techdirt.com/articles/20120810/18401819991/humans-still-weakest-link-security-chain.shtml)
- 28 [chain.shtml](https://www.techdirt.com/articles/20120810/18401819991/humans-still-weakest-link-security-chain.shtml) [Accessed April 24, 2016].
- 29
- 30 Da Veiga, a. & Eloff, J.H.P., 2010. A framework and assessment instrument for information security
- 31 culture. In *Computers & Security*. Elsevier Ltd, pp. 196–207. Available at:
- 32 <http://linkinghub.elsevier.com/retrieve/pii/S0167404809000923> [Accessed September 20, 2014].
- 33
- 34 EY'S Global information Security Survey 2013, 2013. *Under cyber attack EY 's Global Information*
- 35 *Security Survey 2013*, Available at: [http://www.ey.com/Publication/vwLUAssets/EY_-](http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf)
- 36 [_2013_Global_Information_Security_Survey/\\$FILE/EY-GISS-Under-cyber-attack.pdf](http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf).
- 37
- 38 HM Government, 2015. *Technical Report*, Available at:
- 39 [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf)
- 40 [302-information_security_breaches_survey_2015-full-report.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf).
- 41
- 42 ISO, 2013. *ISO / IEC 27001:2013 Information technology — Security techniques —*
- 43 *Information security management systems — Requirements*,
- 44
- 45 Jones, A. & Colwill, C., 2008. Dealing with the Malicious Insider. In *Australian Information Security*
- 46 *Management Conference*.
- 47
- 48 Kirlappos, I., Parkin, S. & Sasse, M.A., 2015. “ Shadow Security ” as a tool for the learning
- 49 organization. In *SIGCAS Computer & Society*, pp. 29–37.
- 50
- 51 Peltier, T.R., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective*
- 52 *information security management*,
- 53
- 54 SANS, 2014. Information Security Policy Templates. Available at: [http://www.sans.org/security-](http://www.sans.org/security-resources/policies/general)
- 55 [resources/policies/general](http://www.sans.org/security-resources/policies/general) [Accessed May 15, 2015].
- 56
- 57 Silowash, G., Cappelli, D. & Moore, A., 2012. *Common Sense Guide to Mitigating Insider Threats*
- 58 *4th Edition*, Available at:
- 59 <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA585500>
- 60 [Accessed January 21, 2015].
- Stahl, S. & Pease, K.A., 2011. *Seven Requirements for Successfully Implementing Information Security Policies and Standards*,

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Information and Computer Security