Fagade, T., & Tryfonas, T. (2017). Hacking a bridge: An exploratory study of compliance-based information security management in banking organization. *Journal of Systemics, Cybernetics and Informatics*, *15*(5), 74-80.

Hacking a Bridge: An Exploratory Study of Compliance-based Information Security Management in Banking Organization

Tesleem FAGADE
Cryptography Group, University of Bristol
Bristol, United Kingdom
tesleem.fagade@bristol.ac.uk

and

Theo TRYFONAS
Cryptography Group, University of Bristol
Bristol, United Kingdom
theo.tryfonas@bristol.ac.uk

ABSTRACT

This work is approached through the lens of compliant security by drawing on the concepts of neutralization theory, a prominent postulation in the criminology domain and the 'big five' personality construct. This research is conducted based on a case study of ISO/IEC27001 Standard certified banks, to empirically evaluate the link between cybersecurity protocols violation and how employees rationalise security behaviour. We propose that compliance-based security has the propensity for a heightened sense of false security and vulnerability perception; by showing that systemic security violation in compliance-based security models can be explained by the level of linkages from the personality construct and the neutralization theory. Building on the survey responses from banking organization employees and the application of partial least square structural equation modelling (PLS-SME) analysis to test the hypotheses and validate survey samples, we draw a strong inference to support the importance of individual security scenario effect as a vital complementary element of compliance-based security. Based on our initial findings, conceptual principles and practical guidelines for reducing insider threats and improving employees' compliance is presented. We then suggest how information security protocol violations can be addressed in that context.

Keywords: Information security, standards and compliance, personality traits, compliant security behaviour, rationalization theory, PLS-SEM, Insider threats

1. INTRODUCTION

The ubiquitous and interconnected nature of information systems, coupled with the ever-increasing cyber-capabilities of adversaries, means that information security (IS) is central to the protection, dependability and management of information assets for businesses and organizations. Banking and financial organizations operate in a dynamic and complex environment where risk management is an endless game between system defenders and adversaries, such that, threats to critical assets could compromise capital gains, human resource, time and competitive advantage for businesses. To protect information assets and ensure business continuity, organizations take measures to reduce the risk of security breaches by implementing information security guidelines and protocols. In response to the increase in cyber security incidents on critical infrastructures, industry regulators make it a mandatory requirement for operators to implement security policies in accordance with industry standards and regulations. For instance, under the Executive Order 13636, the US Federal Government introduced a technical framework and regulation aimed at protecting critical national infrastructure (CNI) cybersecurity and buildings. Likewise, the EU put forward a proposal for a specific European Directive relating to the CNI operators, in both private and public enterprises for the management and regulation of cybersecurity issues [1]. In banks and financial organizations, information security risk is part of the overall management of operational risk. Any failure to implement appropriate security controls is considered a compliance issue, which can attract sanctions from industry regulators. Compliant security is the acceptance of external entity in the form of corporate governance, legislative and industry regulations. However, compliance-based security is determined by factors like the level of organisation security control requirements, the adoption, application and interpretation of different standards within the context of specific need [2]. One of such standards is the ISO/IEC27001, which is particularly relevant to this work and how it is applied in a regional case study.

The ISO/IEC27001 is an international standard for best practices for Information Security Management Systems (ISMS), which outline comprehensive requirements for safeguarding organisation information assets. It defines baseline requirements and controls which can be used to assess risk under the principle of confidentiality, integrity and availability [3]. However, the ISO Standard does not address how to capture the thought process of system adversaries. Also, the standard does not specify, name or recommend any method of control for a given risk scenario but only provides a generic risk analysis and risk treatment plan that is applicable to all types of organizations. Although standardisation and regulatory demands play an important part in attracting budgets and attention of C-level executives in the areas of information security, there are increasing challenges to balance real information security threats with compliance requirements, thereby leading to a heightened false sense of security and vulnerability perception. In today's fast-paced threat environments, the reality is that organizations can meet compliance requirement without necessarily being secured. Hence, the natural research question is why compliance-based information security is considered a far-fetched approach? The rest of this paper is organised as follows; Section 2 covers the motivation for this study and related work. Research model and hypotheses are described in section 3. In section 4, research method, including the validation of measurement and test of hypotheses are presented. Implications of this study outcome for organisations are discussed in section 5, while section 6 focuses on how to mitigate information security compliance-gaps. Finally, discussion and conclusion are covered in section 7, where the key findings and proposition for future work is presented.

2. RELATED WORK AND THE MOTIVATION

The first challenge of information security management in banking organizations is the balance of incentives for the optimal mitigation of cybersecurity risks. Cybersecurity economic model suggests that depending on a combination of incentives, organisation policymakers may eventually stop investing in risk assessment and only focus on compliance-based security, which could lead to unintended consequences [1]. Central to organisation cybersecurity risk evaluation and investment decisions are C-level executives; who may not have a comprehensive understanding of their organisation security capabilities, information assets and threat vectors, yet decide the budget for security investment. Most often, not only are C-level executives' understanding of risk tolerance in misalignment with the IS risk faced by their organizations [4] but C-level executives usually, opt for compliance-based security solutions because it is easy to implement [5]. A lot of security discussions hubs on why security by compliance is a far-fetched approach and why compliance-based security risk management may not be appropriate for organizations [6]. For instance, it is considered that technology and adversary expertise evolves much faster than standards, but the most significant limitation to compliance-based security is the human factor. Researchers suggest that the human element is the major uncertainty and weakest link in any security posture [7], [8], as a consequence of lacking information security policies compliance [9]. Apart from technical capabilities, the biggest threat to IS, leveraged through malicious and unintentional security protocol violation, is the human behaviour [10]. There have been suggestions for more empirical research to link employee non-compliance with psychosocial factors and behavioural theories [11], in attempts to explain the reason why employees fail to comply with regulations relating to cyber crimes. For instance, [12], [13] explored the theory of planned behaviour to argue that perceived expectation, attitude and subjective norms are indicators of behavioural intention. It is further suggested that through training and awareness programs, compliant behaviour can be attained. However, training is not sufficient to enforce compliance, despite the amount of resources that organizations disburse to address security awareness gaps [8]. In the aim to enforce compliance, some organizations also introduce motivation elements of reward and punish for deliberate non-compliance, so that employees can be discouraged from violating cybersecurity protocols. However, studies [14] have shown that deterrence draws on the principle of rational behaviour, and information security standards like ISO/IEC27001 is also based on the assumption that people fit within a certain rational frame of reference. Therefore, contrary to rational assumption, deterrence measures sometimes yield negative consequences, given that motivation differs across organizations [15], [16].

We approach this work through the lens of personality traits and the neutralization theory, to show that the level of systemic risk of security protocol violation in compliance-based security model can be explained by the level of linkages from the personality construct and the neutralization theory. It is believed that this study will complement the wider body of information security research by highlighting the relevance of personality traits and neutralization techniques to compliance-based security management.

3. RESEARCH MODEL AND HYPOTHESES

Our model is comprised of two concepts that are based on the personality construct and the neutralization theory. Description of the two concepts with respect to this work and the hypotheses derived are as follows:

Personality Traits and Security Scenario Effects
Evidence from the literature has shown that individual personality traits described by the big 5 psychological constructs of Openness, Conscientiousness, Extroversion, Agreeableness and Neuroticism (OCEAN), can reveal a significant aspect of behaviour. In the context of information security, it is suggested that individuals with the same personality traits react differently to the same condition depending on associated security scenario effect like self-efficacy, sanction severity, sanction certainty and response cost [17]. Therefore, differences in compliant behaviour intentions are based on the cross-level relationship between personality types and the way we respond to security scenario effect [18]. For instance, as illustrated in Table 1, two different employees with agreeable personality and Narcissistic personality are likely to violate security protocols, if, under security scenario effects, they both show a low sense of sanction certainty.

Personality	Notation	Security Scenario Effect
Openness	O	Low sense of sanction severity
Conscientiousness	C	Low sense of response efficacy
Extraversion	E	Low sense of threat severity, threat vulnerability and response cost
Agreeableness	A	Low sense of sanction certainty
Narcissism	N	Low sense of sanction certainty

Table 1: Cross-level interaction between personality traits and security scenario effects

Similarly, an employee with openness personality but a low sense of sanction severity or another with conscientiousness characteristic but a low sense of response efficacy is likely to violate security protocols. We, therefore, hypothesize the following:

H1a: Low sense of sanction severity can negatively affect compliant security model

H1b: Low sense of response efficacy can negatively affect compliant security model

H1c: Low sense of threat vulnerability can negatively affect compliant security model

Neutralization Theory
Neutralization theory, introduced by [19], suggests that most adolescents are dissuaded from activities that violate societal norms because of associated guilts and shames. However, in order to obtain episodic relief from moral constraint, individuals adopt the technique of neutralization to offset their guilt and freely engage in delinquency without impacting on their self-image [20]. Researchers have applied neutralization techniques in various forms of rule-breaking or deviance behaviour that are not necessarily criminal [21]. Neutralization theory provides explanatory insight into how people are able to justify and break loose from restrictive societal norms and are able to rationalise rule-breaking actions without remorse [22]. Neutralization techniques have gained increasing appeal from behavioural scientists to understand and mitigate workplace deviance. Five neutralization techniques are outlined by [19], which include: denial of injury, denial of responsibility, appeal to higher loyalties, denial of victims, and condemnation of condemners. We considered three neutralization techniques within the context of IS and how they influence security protocol violation. Firstly, Denial of Responsibility is a technique adopted to justify security risk behaviour by acknowledging that although certain actions are wrong, the offender claims that the situation is forced upon them and they had no choice. This could be a case of taking jobs and sensitive corporate data home, to meet up with project deadlines. Secondly, the Denial of Injury technique is a case whereby an offender admits to the violation of security protocol but try to justify his action by assuming that, no one is harmed because of his action. A typical example of this technique in IS context is the sharing of passwords with colleagues. Thirdly, the Blaming the Victim technique, an offender acknowledges that there may be damaging consequences associated with a risky behaviour, but the offender blames the victim e.g. an organisation, a manager, a supervisor etc. as the reason for his action. An example of this in IS context is the installation of unauthorised software to access restricted websites on corporate networks. To counteract individual neutralization techniques, it is suggested that training and awareness, as well as security culture, can significantly improve compliance level in an organisation. We, therefore, hypothesize the following:

H2a: Denial of Responsibility negatively affects compliant security model

H2b: Denial of Injury negatively affects compliant security model

H2c: Blaming the Victim negatively affects compliant security model

H3a: Security culture positively affects actual compliance level

4. RESEARCH METHOD

Survey methodology can be used to study employees' opinion, attitude and behavioural patterns within the context of information security [23]. Similar to the data collection method described for the same group of banking organizations in our previous work [6], we carried out a survey to gain insights into how employee risk behaviour affects compliance-based model of IS risk management. The survey is designed to capture how ISO/IEC27001 certified financial institutions implement policies and employees behavioural response within the context of information security. The online survey of this work is conducted in line with the method described in [23], [24]. Survey questions are segmented into 3 sections; knowledge and awareness statement, security culture statement and demography. The demography of the survey group captures survey representatives for segmentation analysis, while the level of compliance is measured through security culture statements and the knowledge and awareness statements. Security culture statement assesses the behavioural pattern of employees, which could undermine effective implementation of policies. Knowledge and awareness statements test employees' understanding of security policy requirements. Overall, all questions are designed to indirectly measure risky behaviour due to security scenario effect on personality traits and link responses to neutralization techniques. The recruitment strategy for this work is based on a random selection from a presumably representative group of bank employees, including executive/senior manager level, IT department, Operations, HR and administration, and others. Job functions of the 'others' categories include marketing, accountancy, risk management, sales and predictive analysis.

The survey questions follow a Likert scale response model (strongly agree, agree, uncertain, disagree and strongly disagree), except for the question that captures the survey demography. The survey is conducted through Google Forms, an online survey application that allows real-time response, collation and analysis of data. Respondents take part in the survey over a 2 weeks period after the initial invitation via emails and after obtaining security clearance from the CISO of each bank. The average working years of all respondents is 5 years and above and the education level for all respondents is Bachelor degree and above. Gender is not factored into this survey but more emphasis is placed on the demography in terms of respondent's job functions.

The demography of respondents in terms of representation analysis is captured in Figure 1, where 15.8 % of respondents are executive/senior manager level officers, 12.3 % of respondents are from the IT department, 14 % from HR and administration, 40.4 % from Operations and 17.5 % represent 'others' categories. Figure 2 shows the snapshot of the compliance level across the survey demography.

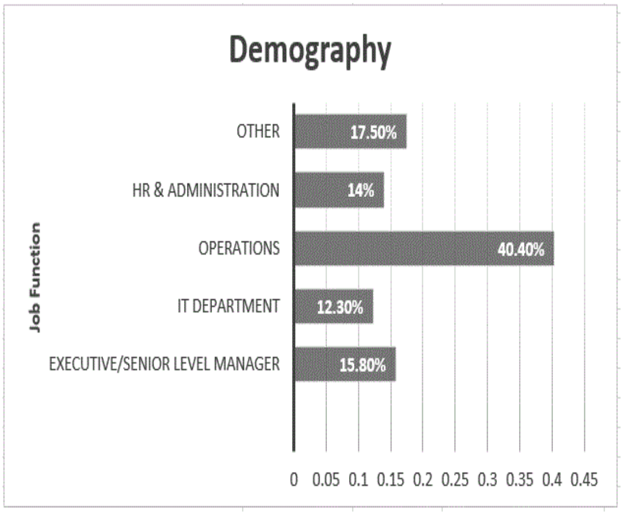

Figure 1: Demographic characteristics of respondents

The survey data is quantified by assigning range values from 1 to 5 for each survey question, such that, if a statement is true from a security standpoint, 5 corresponds to 'strongly agree' and 1 corresponds to 'strongly disagree'.

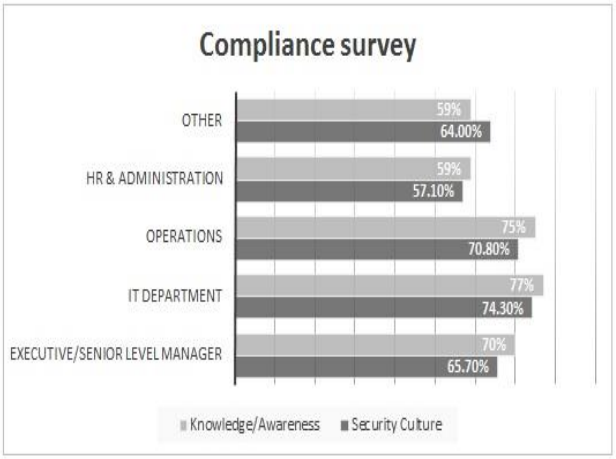

Figure 2: Compliance level

In view of the banks' reluctance to share vulnerability information, results are anonymized for subsequent analysis in this work.

Validation of Measurement

Validation and reliability test of the result as shown in Table 2 follows the recommendation of data measurement goodness-of-fit in the literature [25] [26]. Our data is validated with respect to quality and validity criteria methods for instrument item validation.

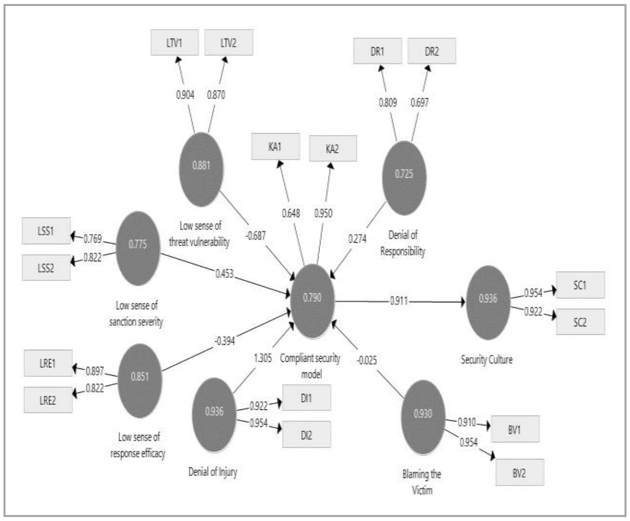

Figure 3: Structural Equation Model Results

To ascertain error-free, construct reliability and internal consistency of result, we assess values for composite reliability index for all constructs, and they are greater than the critical threshold of 0.70, indicating adequate reliability for all constructs. Similarly, the measure of convergent validity based on the average variance extracted (AVE) for each construct exceeds the recommended 0.5 threshold criteria. In addition, loadings for all indicators are above 0.70, except for DR2 and KA1, which are very close to the threshold at 0.69 and 0.64 respectively. Hence, we conclude that contemporary recommendations for the convergent and discriminant validity have been met.

Latent Constructs	**Indicators**	**Loadings**	**Composite Reliability**	**AVE**
Low sense of sanction severity (LSS)	LSS1	0.76	0.77	0.63
	LSS2	0.82		
Low sense of response efficacy (LRE)	LRE1	0.89	0.85	0.74
	LRE2	0.82		
Low sense of threat vulnerability (LTV)	LTV1	0.90	0.88	0.78
	LTV2	0.87		
Denial of Responsibility (DR)	DR1	0.80	0.72	0.57
	DR2	0.69		
Denial of Injury (DI)	DI1	0.92	0.94	0.88
	DI2	0.95		
Blaming the Victim (BV)	BV1	0.91	0.93	0.86
	BV2	0.95		
Security Culture (SC)	SC1	0.95	0.94	0.88
	SC2	0.92		
Knowledge & Awareness (KA)	KA1	0.64	0.79	0.66
	KA2	0.95		

Table 2: Latent Variables validity and reliability measurement

Structural Model Analysis

All hypotheses are tested to measure the effect of neutralization and personality traits alongside different variables on the compliance-based security model. Further data analysis is conducted with IBM SPSS Statistics 23.0 [27] and SmartPLS 3.0 [28] packages. In addition, we calculated the t-statistics by conducting bootstrapping with 3,000 subsamples. Table 3 shows the structural model result including the path coefficient for all hypotheses and the significance of the path (p-value).

Hypothesis	Path coefficients	t-value	p-value
H1a: LSS➔ Compliant security model	0.45	2.42	n.s.
H1b: LRE➔ Compliant security model	-0.39*	1.95	P<0.10
H1c: LTV➔ Compliant security model	-0.68***	0.18	P<0.01
H2a: DR➔ Compliant security model	0.27**	2.47	P<0.05
H2b: DI➔ Compliant security model	1.30***	3.64	P<0.01
H2c: BV➔ Compliant security model	-0.02	0.17	n.s.
H3a: SC➔ Actual Compliant Level	0.91***	2.99	0.01

Note: n.s. not significant

Table 3: Findings on structural relationship showing path loadings and t-values

As hypothesized, we found that H1b, H1c, H2a, H2b, and H3a are supported, while H1a, H2c are not. This implies that compliance-based security model is significantly influenced by neutralization techniques, especially DR and DI in this case. Similarly, personality traits and cross-level interaction with security scenario effects have a direct bearing on the effectiveness of compliance-based security model. This result is also supported by the results obtained in [22][29], although, this work is based on slightly different constructs.

5. ORGANIZATIONAL IMPLICATIONS

Findings in this work agree with literature that compliance-based security is a far-fetched, universal and generic approach to IS management. This study highlights the limitations of the compliance-based approach to information security and particularly reveals how the interplay between personality traits, security scenario effects and neutralization techniques can undermine the effectiveness of compliance-based security management. Individual attributes and norms directly affect the behavioural intention to comply with cybersecurity policies and guidelines. We test the effect of neutralization technique alongside different security scenario effects under the OCEAN personality construct and result suggests that, within the context of this study, two of the tested neutralization techniques have a positive effect on employee behavioural risks that may undermine the effectiveness of compliant security. Similarly, our result highlights the link of each hypothesis to security protocol violations. A possible explanation for the correlation of hypotheses in this result is that employees act of deviance is not necessarily due to lack of training on IS guidelines, but perhaps, more to do with the security implementation approach of each organisation.

Although continuous IS training and awareness program for employees cannot be overemphasised, our findings suggest that training should be delivered in such a way to achieve the most impact. For instance, addressing the security scenario effect and neutralization technique for a given employee can counteract the security gap introduced by the employee's non-compliant behaviour. In addition to compliant security, the training and awareness needs of each employee should be tailored such that individual personality traits and neutralization techniques are factored into organisation policies, guidelines and practical security procedures. This can significantly reduce security protocol violation under a compliance-based security model.

6. FOCUSING ON INFORMATION SECURITY COMPLIANCE-GAPS

In this section, we build on the empirical evidence from our previous work [30], to propose conceptual principles and practical guidelines for the enforcement of employees compliant behavioural changes. Based on the insights into how security scenario effect and neutralization technique affects employee compliant behaviour, we propose that by integrating practical security procedures into operational routines, there is a greater chance of a positive shift in employees' perception of compliance. Studies have shown that given objective situations if security becomes a quotidian practice as well as an integral part of an organisation culture, there is a considerable reduction in the likelihood of security protocol violations [31]. Using data security as an example, in this case, we describe some steps that can be taken to mitigate security compliance gaps. All traditional enterprises, organizations and government agencies, consider data as a critical pervasive asset that requires top priority response. As such, most organisations understand the need for data security but may not necessarily know how to prioritize that for all employees.

The first step to mitigating compliance gaps with respect to data security starts with the management top hierarchy. As illustrated by the compliance-gap mitigation steps shown in figure 4, Executive level sponsors should be able to demonstrate a commitment to address the threats of information security in an organization. Similarly, security and risk management leaders should be able to understand and effectively communicate regulatory obligations under the data protection laws of relevant jurisdictions.

The second step is to embed appropriate technical controls into the organization security culture through practical procedures. For instance, data protection is a requirement in an organisation information security policy, however, data protection policy subsets like regular data backups and unauthorized use of portable devices on corporate computers can be implemented to become a part of an organization work culture. Considering that employees may not feel it as a duty to carry out regular data backups, depending on how the interplay between neutralization technique or security scenario effect influences their compliance decisions. However, compliance can be enforced if data backup becomes part of the job the functions for all employees.

Technical solutions that can be leveraged as part of data security strategy, in this case, may simply be a system or a prompt device that enforces/reminds an employee to carry out data backup every day. For instance, if it is impossible for all employees that interact with information systems to log off at the end of the day without completing backups to the central server, then data backups will become one of the practical guidelines that improve employees' information security compliance. Data backups will then become practical job requirements, rather than an inconvenient security measure. Then gradually, other policy subsets can be introduced in controlled measures to support compliance. Another practical procedure could be the implementation of a system that compels users to change passwords at intervals and disabling of USB ports on all organisation computers. These measures would reduce threats posed by employees that are susceptible to social engineering, reduced the risk of unauthorized copying of confidential information and improve overall data security compliance.

The third step is compliance monitoring; usually, this should have a top-bottom approach, starting with executive level management. Through continuous auditing and compliance monitoring that involves technical and procedural controls, there is a better chance of timely response to identifying and managing compliance gaps. The fourth step is to improve resilience in order to reduce security protocol violations. By identifying compliance gaps, security management programs can be set to promote and maintain security consciousness throughout the organization. In the case of data security, improving resilience may include heightening the sense of ethical responsibility surrounding data disclosure and unauthorized alterations.

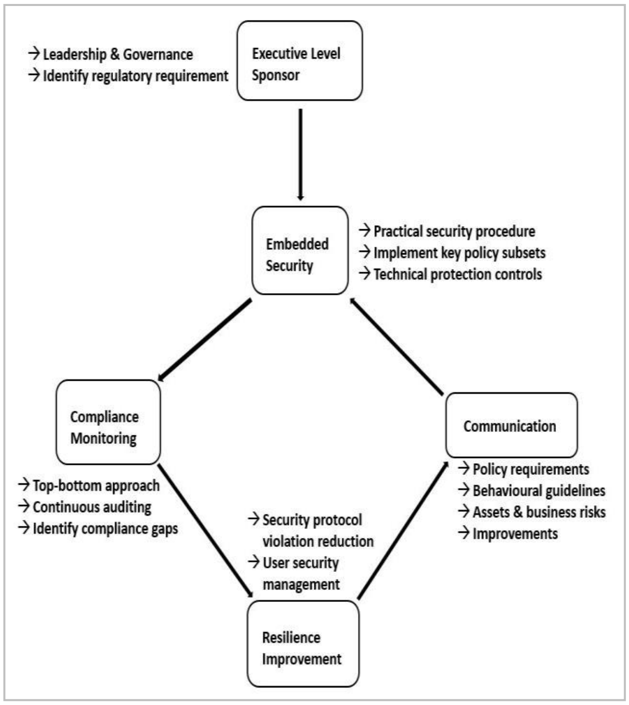
→ Leadership & Governance
→ Identify regulatory requirement
Executive Level Sponsor
Embedded Security
→ Practical security procedure
→ Implement key policy subsets
→ Technical protection controls
Compliance Monitoring
→ Top-bottom approach
→ Continuous auditing
→ Identify compliance gaps
Communication
→ Policy requirements
→ Behavioural guidelines
→ Assets & business risks
→ Improvements
→ Security protocol violation reduction
→ User security management
Resilience Improvement

Figure 4: Compliance-gaps mitigation steps.

The final step involves continuous communication of security policy requirements, behavioural guidelines and compliance impact on assets and business risks. Policy subsets should show clear guidelines and best practices for ensuring data confidentiality, integrity and availability. Through user awareness and ethical code of conduct programs, employees should become fully aware of organization's position on data protection; whereby data security is the responsibility of all employees and not just restricted to the IT department. Most importantly, it should be communicated why data is vital for business continuity, how data loss may impact on business and what measures can be taken to ensure data security. By rewriting data security policy subsets in a clear and concise fashion and, by implementing technical solutions that complement data protection policy, organisations can begin to see data security objectives as part of general security compliance scheme. To avoid productivity challenges often brought about by extra layers of technical security; technical solutions can be introduced gradually while focusing initially on components that constitute everyday security issues. Therefore, employees that often see extra security steps as in-convenient add-ons, may not be overwhelmed by the perception of reduced productivity.

7. DISCUSSIONS AND CONCLUSION

Human factor continues to represent the weakest link in organisations defence postures. The insufficient understanding of the dynamics surrounding security compliant behaviour grossly underscores that effectiveness of security by compliance. We show that, with respect to employee's personality dimension and security scenario effect, Low sense of sanction severity (LSS) and Low sense of response efficacy (LRE) negatively affects compliant security model. Similarly, in the context of neutralization technique, we show that Denial of Responsibility (DR) and Denial of Injury (DI) negatively affects compliant security model. However, for both personality trait and neutralization technique, the results have not been able to support hypothesized negative relationship for a Low sense of sanction severity (LSS) and Blaming the Victim (BV) respectively.

In general, we have shown how individual attributes and norms influence the intention to comply with cybersecurity policies and guidelines. We also discussed the wider implications of this research for organisations, suggesting how the security awareness need of each employee could be factored into customized training programs. Finally, through a conceptualized approach of practical security procedures, we addressed the practical problem of how to enforce compliance within a banking organisation workforce. It is believed that this study will have a wider implication for security managers and researchers alike. As part of future work, we hope to expand and test the validity of the observations in this study through a robust empirical model and also, suggest ways to integrate human-centric technical procedure into compliant security model.

8. REFERENCES

[1] F. Massacci, R. Ruprai, M. Collinson, and J. Williams, "Economic Impacts of Rules- versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers," *IEEE Secur. Priv.*, vol. 14, no. 3, pp. 52–60, May 2016.

[2] J. Kwon and M. E. Johnson, "Security practices and regulatory compliance in the healthcare industry," *J. Am. Med. Informatics Assoc.*, vol. 20, no. 1, pp. 44–51,

Jan. 2013.

[3] ISO/IEC 27001:2013, “Information technology - Security techniques - Specification for an Information Security Management System.,” The British Standard Institute, 2014.

[4] T. Fagade, K. Maraslis, and T. Tryfonas, “Towards Effective Cyber Security Resource Allocation: The Monte Carlo Predictive Modelling Approach,” *Int. J. Crit. Infrastructures (in Press.*, 2017.

[5] D. Danchev, “Building and implementing a successful information security policy,” *Wind. Com*, 2003.

[6] T. Fagade and T. Tryfonas, “Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks,” Springer, Cham, 2016, pp. 128–139.

[7] S. Aurigemma and R. Panko, “A composite framework for behavioral compliance with information security policies,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2011, pp. 3248–3257.

[8] K. Renaud and W. Goucher, “The Curious Incidence of Security Breaches by Knowledgeable Employees and the Pivotal Role a of Security Culture,” Springer, Cham, 2014, pp. 361–372.

[9] M. Siponen, M. Adam Mahmood, and S. Pahnila, “Employees’ adherence to information security policies: An exploratory field study,” *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, Mar. 2014.

[10] S. Bauer and K. Chudzikowski, “Mind the Threat! A Qualitative Case Study on Information Security Awareness Programs in European Banks,” *AMCIS 2015 Proc.*, 2015.

[11] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, “Future directions for behavioral information security research,” *Comput. Secur.*, vol. 32, pp. 90–101, Feb. 2013.

[12] N. Waly, R. Tassabehji, and M. Kamala, “Measures for improving information security management in organisations: the impact of training and awareness programmes,” *UK Acad. Inf. Syst. Conf. Proc. 2012*, 2012.

[13] T. Gundu and S. Flowerday, “Ignorance to awareness: Towards an information security awareness process,” *SAIEE Africa Res. J.*, 2013.

[14] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, “The insider threat to information systems and the effectiveness of ISO17799,” *Comput. Secur.*, vol. 24, no. 6, pp. 472–484, Sep. 2005.

[15] J. D’Arcy and T. Herath, “A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings,” *Eur. J. Inf. Syst.*, vol. 20, no. 6, pp. 643–658, Nov. 2011.

[16] S. Park, A. B. Ruighaver, S. B. Maynard, and A. Ahmad, “Towards understanding deterrence: Information security managers’ perspective,” in *Lecture Notes in Electrical Engineering*, 2012, vol. 120 LNEE, pp. 21–37.

[17] M. Warkentin, M. McBride, L. Carter, A. Johnston, and A. C. Johnston, “The Role of Individual Characteristics on Insider Abuse Intentions,” *Assoc. Inf. Syst. AIS Electron. Libr.*, no. 1, 2012.

[18] T. Fagade and T. Tryfonas, “Malicious Insider Threat Detection: A Conceptual Model,” in *Security and Protection of Information 2017*, 2017, pp. 31–44.

[19] G. M. Sykes and D. Matza, “Techniques of Neutralization: A Theory of Delinquency,” *Am. Sociol. Rev.*, vol. 22, no. 6, p. 664, Dec. 1957.

[20] R. Agnew and A. a. R. Peters, “Techniques of Neutralization,” *Crim. Justice Behav.*, vol. 13, no. 6, pp. 81–97, Mar. 1986.

[21] Mikko Siponen and Anthony Vance, “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations,” *MIS Q.*, vol. 34, no. 3, pp. 487–502, 2010.

[22] W. Li and L. Cheng, “Effects of Neutralization Techniques and Rational Choice Theory on Internet Abuse in the Workplace,” in *PACIS 2013 Proceedings*, 2013.

[23] A. Da Veiga, N. Martins, and J. H. P. Eloff, “Information security culture – validation of an assessment instrument,” *South African Bus. Rev.*, vol. 11, no. 1, pp. 147–166, 2007.

[24] Deloitte, “Central Asian Information Security Survey Results (2014) Insight into the information security maturity of organisations , with a focus on cyber security Introduction and Executive summary,” 2014.

[25] J. F. J. Hair, G. T. M. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, vol. 46, no. 1–2. 2014.

[26] J. F. Hair, C. M. Ringle, and M. Sarstedt, “PLS-SEM: Indeed a Silver Bullet,” *J. Mark. Theory Pract.*, vol. 19, no. 2, pp. 139–152, Apr. 2011.

[27] D. George and P. Mallery, *IBM SPSS Statistics 23 step by step: A simple guide and reference*. 2016.

[28] H. Latan and I. Ghozali, “Partial least squares: Concepts, techniques and application using program SmartPLS 3.0,” 2015.

[29] S. Bauer and E. W. N. Bernroider, “The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9190, pp. 154–164.

[30] T. Fagade and T. Tryfonas, “Hacking a Bridge: An Exploratory Study of Compliance-based Information Security Management in Banking Organization,” in *Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017), vol. 2*, 2017, pp. 94–99.

[31] J. Jackson, B. Bradford, M. Hough, A. Myhill, P. Quinton, and T. R. Tyler, “Why do people comply with the law?,” *Br. J. Criminol.*, vol. 52, no. 6, pp. 1051–1071, Nov. 2012.