International Journal of Computer Applications Technology and Research
Volume 11–Issue 03, 72-77, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1103.1004

What Triggers Violation of Information Security Policies

Sandeep Dhawan
Senior IT Director

Abstract: This paper offers a framework for information security professionals to evaluate ISP and understand policy non-adherence. It explores the different types of non-adhering behaviors and the motivations behind them. It goes on to share information about the environmental/organizational climates in which non-compliant behaviors are more or less likely to occur and briefly touches on when users are more likely to commit them. Finally, it suggests a user review process as a critical part of information security policy design and implementation.

Keywords: ISP violation intention, information security policies, IS compliance, information security behavior, internal threat agent

1. INTRODUCTION

User non-adherence to existing information security policies accounted for 88% of all reported data breaches in 2021. [1] With each data breach costing the affected organization an average of $4.4 million [2], reducing instances of information security policy violation or non-adherence must be a priority for any professional involved in drafting information security policies.

Information security systems are constructed as a protective measure, guarding the information technology (IT) of an organization or company. The threats they protect against include natural disasters, physical damage, and human behavior.

Human behavioral threats to information security can be classified as internal or external. Hackers or attackers outside the organization may implement techniques such as malware, phishing, DDoS attacks, and ransomware in attempts to gain control over valuable resources. Inside the organization or network, each user and each access point represent a potential vulnerability.

In an attempt to address and prevent user-based internal threats while complying with regulatory requirements, the designers of information security systems craft policy guidelines for the access to and use of information technology.

These detailed instructions, known as information security policies (ISP), also define what actions constitute a violation of the policy and frequently include a description of the consequences for performing such a violation. ISP take into account the wider context within which the information security system is situated, such as the industry, region, and model or structure of the organization.

Once composed, edited, and approved, the distribution method of the ISP varies by organization. ISP may be distributed directly to users, or an overview may be delivered as part of the onboarding process. Users with higher levels of access may be required to participate in more formal training.

A sufficiently robust and considered information security policy, implemented perfectly will provide the appropriate level of protection for the digital assets of a given organization. Yet, implementation is far from perfect. Professionals involved in information security policy development and implementation must therefore consider the reasons non-adherence occurs.

Investigating the origins of non-compliant behavior and the circumstances or environments that make non-adherence more or less likely allow the human element to enter the ISP at the earliest design phases. Building awareness and a culture of trust around information security improve the chances that ISP will be implemented consistently. [3] Costly data breaches could be mitigated, decreased, or avoided altogether.

2. CONTENT

2.1 ISP Creation

Not only must user behavior be a consideration from the very first draft, an ISP cannot be considered complete until it has been enthusiastically adopted by the workforce.

2.1 ISP Implementation

Information security policies must be implemented with a high degree of consistency in order to perform their stated function. A violation occurs when a user, for whatever reason, does not follow the procedures laid out in the ISP.

2.3 ISP Violation

Common ISP violations include password and log-in sharing, using old or weak passwords, and clicking on phishing links. Less common violations include the access to or theft of privileged information.

2.4 Human Element

Human behavior is complex, and therefore a certain degree of inconsistency in implementation must be expected. Cybersecurity behavior is influenced by individual decision-making styles. [4] Organizing and understanding the triggers at the root of non-compliant information security behavior is a necessary step to creating novel ways of increasing cyber-resiliance.

2.5 Awareness

As it relates to information security, the human element can be organized broadly into two categories: compliant, and non-compliant. While remaining compliant with ISP may seem obvious to professionals rooted in cybersecurity, not all users have the same level of awareness of ISP and security in general.

2.6 Compliance

Compliance has costs and benefits and carries the risk of sanctions or the chance of praise. Individual beliefs about these costs, benefits, risks, and choices further complicate our understanding of the factors that go into cybersecurity behaviors. [5] (Fig. 2)

2.7 User Intention

Non-compliant behavior can be further segmented in several different ways. One such segmentation is based on the user's intention. Actions that violate ISP unintentionally and without malice can be considered 'misbehavior'. 'Non-malicious deviant behavior' occurs when the ISP is violated intentionally, but without malice. 'Deviant behavior' involves a violation of the ISP with malicious intent. [6]

2.8 Corrective Action

2.8.1 Misbehavior

Misbehavior occurs when security awareness is low. Training and education aimed at raising security awareness should therefore be a part of ISP implementation and may need to be repeated at regular intervals to prevent the awareness from fading.

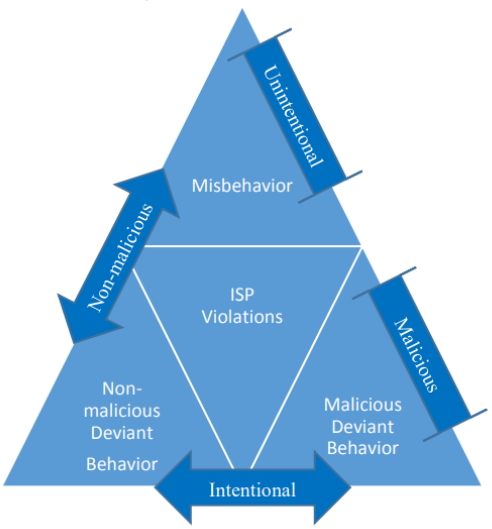
2.8.2 Malicious Deviance

Users with malicious intent cannot be relied upon to implement ISPs consistently no matter how much training or education they receive. Malicious deviation from the ISP in an attempt to damage it or profit off it is beyond the scope of the ISP to prevent.

2.8.3 Non-Malicious Deviance

Between these two extremes is a user group caught in a contradiction. They intentionally, knowingly work against their organizations' information security goals, which can have profound ramifications for the organization, but without malicious intent. At times, their intent is altruistic; when forced to choose between implementing ISP consistently and achieving their job-related tasks, these users will consistently choose the latter. [6]

Figure 1. The Triad of ITA Behaviors [6]



While it is possible to categorize individual instances of ISP non-compliance, it is not possible to characterize individual employees or users with the same labels. ISP compliance is fluid, rather than stable [7], and interacts with various stimuli

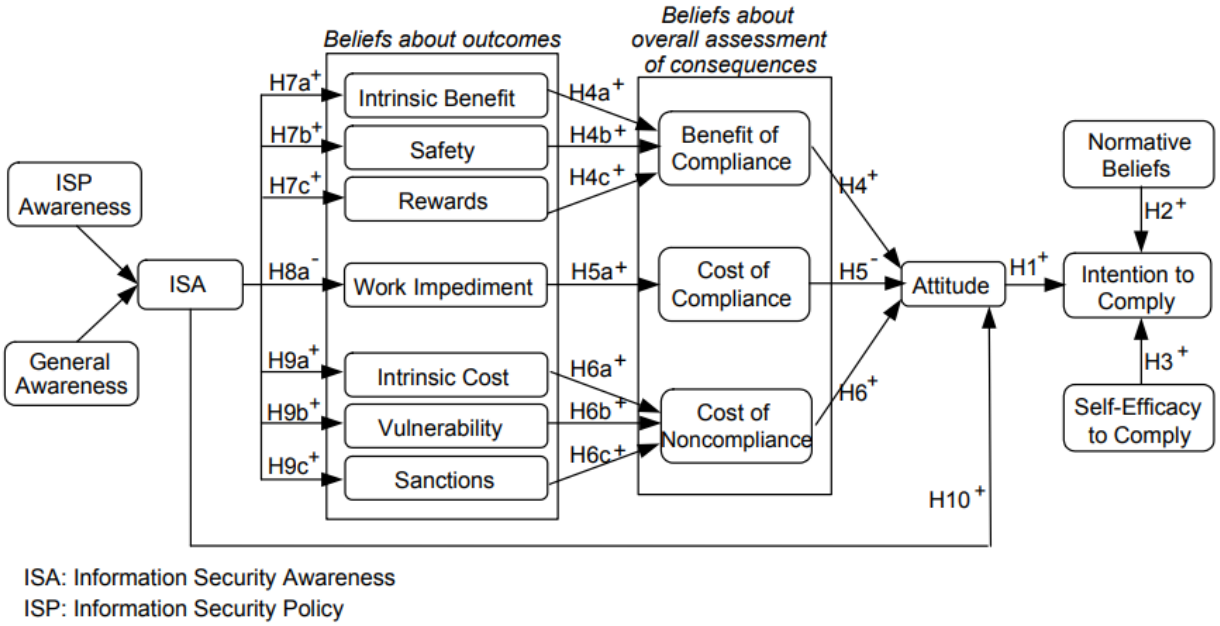
Fig.2 Model of Compliance Antecedents [5]

such as job demands, organizational structure, company culture, and personal affect.

2.9 Security-Related Stress

International Journal of Computer Applications Technology and Research
Volume 11–Issue 03, 72-77, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1103.1004

Security-related stress (SRS) has also been linked with



security non-compliance, which is closely associated with fatigue and frustration. [8]

2.10 Situational Moral Beliefs

Situational moral beliefs affect security behaviors like sharing passwords or selling confidential data.

This effect has been shown to be mitigated somewhat by the severity and certainty of being sanctioned for violations. [9]

2.11 Consequences and Rewards

Monetary rewards for remaining compliant are more effective than harsh formal consequences. Informal consequences and perceived benefits more effectively encourage compliance. [10]

2.13 Environment

During the development and training period, information security policies are functioning in a controlled environment under expected circumstances. Once training is complete, employees return to their work, where they must balance their individual motivations, values, and temperament with competing priorities in an uncontrolled environment while also sticking to security protocols. Perfect implementation of the ISP during training exercises does not guarantee the same level of adherence on the job.

2.13.1 Organizational Ethical Climate

An instrumentalist-based organizational ethical climate (OEC) can positively modify the relationship between moral disengagement and ISP violation, while a negative modification is associated with rule-and-law based OEC. [11]

2.13.2 Organizational Structure

Organizational structure also has an effect on compliance. When compared to organizations, bureaucratic institutions have the best chance of keeping information safe. Organizations with a bureaucratic organizational structure must recognize the benefit provided by this structure and weigh it carefully when confronted with opportunities for more customer-centric modes of operation. [12]

2.13.3 Professional Subculture

In terms of the intention to violate an ISP, professional subculture plays a role. [13] Individuals who share similar training experiences tend to also share similar values and attitudes about security procedures.

2.14 Individuality

Personally held values, beliefs, and attitudes toward data protection also influence user behavior. [5] A consciously developed culture of data protection can increase cyber-resiliency. [3]

In environments that function on trust and collective responsibility, peer monitoring reduces ISP violation intention. [14]

2.15 Negative Emotions

Employees with negative emotions are more likely to intentionally violate ISP. While some negative emotions are inevitable and enter the workplace from outside, others are generated by experiences in the workplace. These negative

emotions can be mediated by measures designed to increase organizational support, psychological ownership, and work engagement. [15]

3. DISCUSSION

Understanding what triggers a violation of ISP presents opportunities to decrease the likelihood of non-compliance. IS professionals responsible for the development and implementation of ISP must be aware of these possibilities in order to develop novel approaches and interventions that increase compliance.

These opportunities are distributed throughout the design and implementation process. IS professionals could begin the drafting of policies by defining the structure of the organization within which the policies will be implemented.

Another important factor to establish before the first draft begins is the cultural context within which security-affecting behaviors occur. A toxic work culture should be considered a valid security threat. While changing the culture of the organization may be beyond the power of the information security team, ISP training and education should take place in a trust-based environment.

It may also be possible to leverage non-IS-based users with an interest in cybersecurity to encourage the kind of peer-monitoring that has been shown to increase compliance. [16]

An ISP that has not been implemented in the real-world environment can only be considered a first draft. Many organizations choose to wait until after a security event has occurred to review the interaction between employees, job task completion, and security protocols. This is a costly mistake.

A user review period has the potential to identify areas of disagreement between job requirements and security expectations. Done thoughtfully, it may also encourage the kind of trust-based environment that reduces the risk of non-compliant behavior.

Further research could include investigation of novel user review processes to establish the efficacy of the proposed tool. The relationship between user review efficacy and organizational ethical climate is also ripe for exploration. Studies that track user-related variables such as security awareness, personal motivations, individual values and attitudes, professional subculture, stress, and situation moral beliefs could investigate if and how these phenomena are influenced by a user review process.

Longitudinal studies could be used to track the long-term effects of adding a user review process to the work system, including whether they increase or decrease compliance with ISP.

Since environment, culture, and peer-monitoring are crucial pieces of the ISP violation puzzle, continued study is needed on the complex social interactions that interact with and have an effect upon cybersecurity.

Taking a holistic view of the various triggers behind ISP violations allows information security professionals to identify potential threats and implement appropriate countermeasures throughout the ISP development and implementation process.

4. CONCLUSION

Users violate information security policies for a number of different reasons.

At a high level, organizational structure, ethical climate, peer relations and professional subculture all play a role.

Zooming in to look at the individual, many factors can affect both the intention to violate or comply with ISP and whether that violation actually occurs. They include security awareness, personally held moral and ethical beliefs, the agreement (or lack thereof) between job-related tasks and security policies, and the user's conception of benefits and rewards for remaining compliant or violating the ISP.

During training and implementation, empowered users can function as a review board, pointing out inconsistencies between workflow and policy. Policies that force employees to choose between task completion and security protocols are the most likely to be violated. The solutions are often low-cost and easily implemented. [17]

Empowered users can be trusted to give valuable feedback on security protocols and policies. Reconciling user intention and user execution through formal and informal review processes has the potential to close a critical gap in information security systems.

The cost of a data breach includes not only the loss of information assets but also the loss of trust from critical stakeholders. With the extraordinarily high costs and risks associated with data breaches, information security professionals must use every tool at their disposal to protect information security systems.

A formal user review process during ISP development and implementation is one such valuable tool.

5. REFERENCES

[1] IBM. (2022). *Cyber Security Intelligence Index Report.* https://www.ibm.com/security/data-breach/threat-intelligence/

[2] IBM. (2021). *Cost of a Data Breach.* https://www.ibm.com/security/data-breach
D'Arcy, J, Lowry, PB. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Info Systems J*. 2019; 29: 43– 69. https://doi.org/10.1111/isj.12173

[3] Huang, K., & Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences*. URI: https://hdl.handle.net/10125/60074

[4] Charlette Donalds, Kweku-Muata Osei-Bryson,
Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents, International Journal of Information Management, Volume 51, 2020, 102056, ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt.2019.102056.

[5]. S. Dhawan, "Information and Data Security Concepts, Integrations, Limitations and Future," IJAIST, vol.30, no.30, pp.09-13, Sep.2014

[6]van den Bergh, M., & Njenga, K. (2016). *Information Security Policy Violation: The Triad of Internal Threat Agent Behaviors*. https://www.researchgate.net/profile/Maureen-Van-Den-Bergh/publication/303408537_Information_Security_Policy_Violation_The_Triad_of_Internal_Threat_Agent_Behaviors/links/5742abfc08aea45ee84a4ef9/Information-Security-Policy-Violation-The-Triad-of-Internal-T

[7] D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69. https://doi.org/10.1111/isj.1217

[8] John D'Arcy, Pei-Lee Teh, Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization, Information & Management,
Volume 56, Issue 7, 2019, 103151, ISSN 0378-7206,
https://doi.org/10.1016/j.im.2019.02.006.

[9] Li, Han; Luo, Xin (Robert); and Chen, Yan (2021) "Understanding Information Security Policy Violation from a Situational Action Perspective," *Journal of the Association for Information Systems*, 22(3), .
DOI: 10.17705/1jais.00678

[10] Li, Yuanxiang John and Hoffman, Elizabeth, Behavioral compliance theory: an experimental and behavioral economics approach to information security policy compliance (November 15, 2021). Available at SSRN: https://ssrn.com/abstract=3252742 or http://dx.doi.org/10.2139/ssrn.3252742

[11] Chen, H., Chau, P.Y.K. and Li, W. (2019), "The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior", *Information Technology & People*, Vol. 32 No. 4, pp. 973-992. https://doi.org/10.1108/ITP-12-2017-0421

[12] Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2021). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security*.

[13] Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., & Wu, D. T. (2020). The Influence of Professional Subculture on Information Security Policy Violations: A Field Study in a Healthcare Context. *Information Systems Research*. Informs Pubs Online. https://doi.org/10.1287/isre.2020.0941

[14] Adel Yazdanmehr, Jingguo Wang, Can peers help reduce violations of information security policies? The role of peer monitoring, European Journal of Information Systems, 10.1080/0960085X.2021.1980444, (1-21), (2021).

[15] Jie Zhen, Zongxiao Xie, Kunxiang Dong & Lin Chen (2021) Impact of negative emotions on violations of information security policy and possible mitigations, Behaviour & Information Technology, DOI: 10.1080/0144929X.2021.1921029

[16] Kam, H.-J., Ormond, D. K., Menard, P., & Crossler, R. E. (2021). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal*, 1– 39. https://doi.org/10.1111/isj.12374

[17] Martha Nanette Harrell. 2014. Factors impacting information security noncompliance when completing job tasks. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer

and Information Sciences. (21) https://nsuworks.nova.edu/gscis_etd/21.

[18] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness1. *MIS Quarterly*, *34*(3), 523-548.

[19] S. Dhawan, "Information and Data Security Concepts, Integrations, Limitations and Future," IJAIST, vol.30, no.30, pp.09-13, Sep.2014