https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

User's Behaviors Influence on Cybersecurity Strategy Effectiveness

Hasna Elkhannoubi, Mustapha Belaissaoui

h.elkhannoubi@uhp.ac.ma, *Mustapha.belaissaoui@uhp.ac.ma*

Information system for decision laboratory , ENCG, Hassan I University, Settat-Morocco

Abstract—*Most of past research in the area of information systems' security has primarily focused on the technical dimension without paying attention to the human factors. The traditional conception of cybersecurity strategy hasn't take into account the organizational level, since organizations may not have employed the most critical key of success:* ***Users' behavior****. This paper focuses on users' behaviors over the cybersecurity strategy. The purpose of this study is to assert the influence of users' behaviors on the effectiveness of cybersecurity strategy via an empirical study shared with more than 2000 users. The paper describes the user's behavior modeling diagram based on Bayesian networks for user modeling, and identifies the continued usage behavior diagram based on the Expectation-Confirmation Model. In this research program we arm that users' behaviors have an important impact on data safety and security, and even if the robustness of the organization's cybersecurity strategy, the users' behavior can influence on their effectiveness. The finding may help information security professionals to define a user charter, which control user's behavior in a specific environment.*

Keywords—Cybersecurity, User's behavior, information management, information technology, human factor.

I. INTRODUCTION

Currently, the world of information and communication technologies is constantly in progress, these technologies have increased and evolved dramatically and becoming an integral part of organization's business processes. According to (Woodhouse, 2007) information is now critical to business operations and decision making activities, allowing organizations to survive and grow in competitive and tough economic environments, and governments to provide services and infrastructures to their constituents.

However, organizations need to identify the risks associated to IT (information technology) usage, especially with this strong dependency to information systems and IT in both public and private organizations. In recent years, cybersecurity has been the subject of serious discussion on IT integration in different organization's processes (Rowe, Lunt, & Ekstrom, 2011), because information safety and security are a key element to get the benefit from IT usage.

In this context and according to (Elkhannoubi & Belaissaoui, 2015) cybersecurity isn't a matter of technological choice; it affects legal, organizational and technological directions of enterprises or administrations. The eventual success of IT usage is more dependent on users' behaviours, the highest risk of successful cybersecurity strategy comes from personal integration, behaviors and usage of IT tools and services.

This paper stems from the research question, "how user's behavior can influence on cybersecurity strategy effectiveness?" because organizations investments are increasing in IT adoption, and in the same time, they are becoming aware of the importance of users' behaviour as critical prerequisites for productivity gains from IT (Hong, Thong, & Tam, 2006). It seems that more attention needs to be paid to human factor since most of research studies focus just on the technical factor. To answer our question, we addressed to various theoretical perspectives as used in Management Science such as Technology Acceptance Model (TAM), Theory of Reasoned Action (TRA), Expectation-Confirmation theory, and so forth. The main goal of this research is to extend users' behavior theory to the information security context, we contend that individuals' behaviors regarding information security practices may help in the efficacy of the cybersecurity strategy (Herath & Rao, 2009).

The content of this paper has been selected to answer a critical question rarely mentioned on computer science research, even if it's crucial to cybersecurity strategy effectiveness. the paper begins with a literature review of users' behaviors theories. Then, our method takes into account a theoretical study based on the use of password authentication method. Before conclusion, we discuss the empirical results by supporting the hypotheses that user's behaviour influence on cybersecurity strategy effectiveness.

https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

II. LITERATURE REVIEW ON USERS' BEHAVIORS

There are several ways in which behavior is conceptualized and defined. The largest number of studies (primarily from within psychology) focus squarely on the individual as the locus of behaviour (Morris, Marzano, Dandy, & O'Brien, 2012). In general, users' behavior toward IT strategies can be characterized principally by to elements: User's acceptance of IT and user's continued usage of IT.

The Computer Security Institute (CSI) in San Francisco, USA, estimates that between 60% - 80% of all network misuse is perpetrated by people inside the organization (Peltier & Blcakley, 2005).So, human factor as a "behavior" is important to enforce a gainful information system, the empirical validity of this argument has been documented in a variety of research contexts (Dhillon & Backhouse, 2000)(Lee & Kozar, 2005)(Straub Jr, 1990)(Straub & Welke, 1998).

2.1. User's acceptance of IT

2.1.1. User's acceptance of cybersecurity strategy

Despite significant investments of several organizations on their information systems, they haven't produced the intended benefits from the use of IT services. Performance gains are often obstructed by users' unwillingness to accept and use available systems (Davis, 1989) . As a definition, user acceptance is the demonstrable willingness within a user group to employ information technology for the tasks it is designed to support (Dillon, 2001). The following table (Table 1) resume three fundamental theories (Dillon & Morriss, 2007) to frame user's acceptance of IT:

Table.1: Theory/Model of users' acceptance of IT

Theories/Models	*Key factors*	*Description*
Theory of reasoned action (TRA)	*Attitude toward behavior and Subjective norm*	*TRA defines relationships between beliefs, attitudes, norms, intentions, and behavior: An individual's behavior is determined by one's intention to perform the behavior, and this intention is influenced jointly by the individual's attitude and subjective norm.*
Technology acceptance model (TAM)	*Perceived usefulness and Perceived ease of use*	*TAM was designed to predict information system acceptance and diagnose design problems before users have experience with a system.*
Motivational model (MM)	*Extrinsic motivation and intrinsic motivation*	*A significant body of research in psychology has supported general motivation theory as an explanation for behavior. Motivational theory has been applied to understand new technology adoption and use.*

2.1.2. User's behavior modeling diagram

Many researchers (Dillon, 2001) have attempted to identify psychological variables that distinguish user who accept or reject technologies. A meta-analysis of research (Alavi & Joachimsthaler, 1992), suggest that the most relevant user factors determining technology acceptance are cognitive style, personality, demographics, and user-situational variables. So, several research work on defining and characterizing user's behavior against IT.

In our work, and based on Bayesian networks for user modeling (Horvitz, Breese, & Heckerman, 2013) we define our user modeling diagram taking into account the relation between user's behavior and cybersecurity. The purpose of this diagram is to identify all user's characteristics that influence on his decision to use or reject a cybersecurity strategy.

The user modeling diagram (figure 1) represents key aspects of user's characteristics, which influence on his acceptance of cybersecurity strategy. The user's behavior is the outcome of user's action, which mainly influenced by the procedural actions, data criticality and user's needs and goals. The procedural actions include several penalization procedures and legal framework that can be represented by the security policy or user's charter. Data criticality is directly proportional to certain factors and criteria such as data classification (private or public data) and available security measures.

https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

The user's action considers all user's needs and goals. As mentioned in (Horvitz et al., 2013), goals are joined to user's attention and needs are joined to actions that will reduce the time required to achieves goals. As indicated by the diagram, user's needs and goals are typically influenced by the competency profile of user, it depends to three fundamental criteria: user's age, the assistance giving by the organization to use a system and user's background, which relatively connected to the user's initial formation (the user's profile is/isn't in relation with ISS) and the user's expertise (in relation with the user's experience).

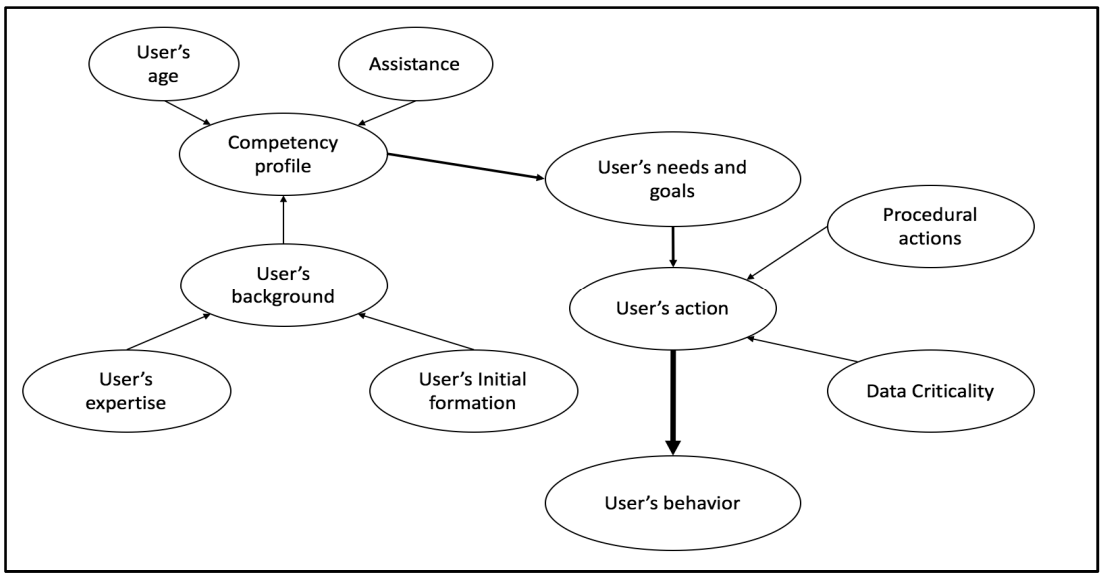

Fig.1: User's behavior modeling diagram

2.2. Continued usage behavior of IT

2.2.1. Continued usage behavior theory

Information systems' (IS) adoption is just the first step toward overall information system success (Limayem, Hirt, & Cheung, 2007). So, the eventual success of any cybersecurity strategy depend on its long-term viability and continued use rather than its first-time acceptance. Unfortunately, continued usage behavior of a cybersecurity strategy can be more difficult than its first adoption, the question can be what happens in later phases of the acceptance process?what are the factors that influence users to continue to follow a cybersecurity strategy.

IS continuance, IS continuance behaviour, or IS continuous usage describes behavioral patterns reflecting continued usage of a particular IS, this continuance refers to a form of post adoption behaviour (Limayem et al., 2007). Cybersecurity continuance use refers to a usage stage when this behaviour becomes part of normal routine activity. The cybersecurity continuance use can be determined as experience variable when each user decide to continue following the cybersecurity strategy. However, a few theoretical studies have shed light on continued usage behavior, the following table (Table 2) presents the fundamental theory (Hong et al., 2006) to frame user's continued usage behavior:

Table.2:Theory/model of user's continued usage behaviour

Theories/Models	Key factors	Description
Expectation-Confirmation Model	Initial expectations and discrepancies	ECM is a theory mainly used to study consumer satisfaction and post-purchase behaviour. Users' continued usage decisions in the context of IS or ISS is similar to consumers' repeat purchase decisions, in this context, satisfaction is considered as a key factor to push users to follow the cybersecurity strategy.

https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

The ECM originally developed by (Oliver, 1980) theorizes that consumer's post-purchase satisfaction is jointly determined by pre-purchase expectation and expectancy disconfirmation. Satisfaction, in turn, is believed to influence post-purchase attitude and consumers' intention to repurchase a product or reuse a service (Hsu, Yen, Chiu, & Chang, 2006). In the context of information systems' security, user's satisfaction about the efficiency of cybersecurity strategy influence on his decision to follow it.

2.2.2. Continued usage behavior diagram

In the IT context, the fundamental keys of continued usage behavior were developed and empirically tested by (Bhattacherjee, 2001) around an Expectation-Confirmation Model of continued IT usage (ECM-IT). Taking into account the similarity between users' continued IT usage decisions and consumers' repeat purchase decisions, this model joins the continued IT usage to three concepts:

- User satisfaction with the IT;
- Extent of user confirmation;
- Post-adoption expectations;

In our work (Figure 2), we simplify the former noticed model to explain the user's continued usage of the cybersecurity strategy based on the standard Expectation-Confirmation Model of continued IT usage.

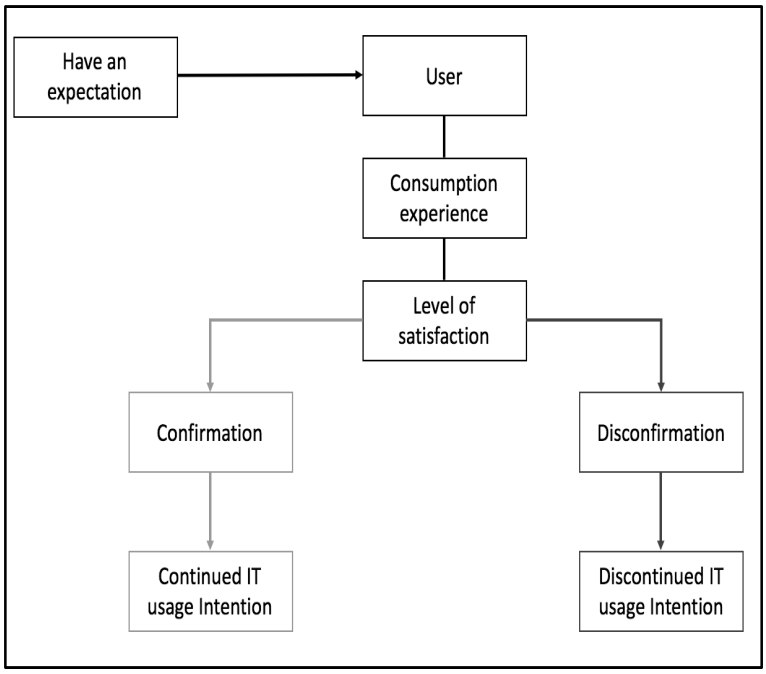

Fig.2: Continued usage behavior diagram

User decides to use a cybersecurity product /services (P/S) taking into account other users' experiences where the major determinant is the users' satisfaction. However, users' satisfaction has a positive influence on his intention to continue following the cybersecurity strategy. As a summary, to study users' continued usage behavior of a cybersecurity strategy we must study the satisfaction of users when they follow this strategy. It seems that users have always an initial expectation before using the P/S imposed by the cybersecurity strategy; then, their consumption experiences with it build a perception about its performance and facility of use; finally, these experiences confirm or dis-confirm the first expectation.

Based on the literature review presented in the two subsection below we propose a theoretical model presented in (Figure 3) which summarizes our proposed hypotheses. As shown in the figure, we propose that cybersecurity strategy effectiveness is closely related to the acceptance and the continued usage of this strategy. However, each hypothesis (H) reflects the influence of users' behavior keys on the acceptance and the continued usage of the cybersecurity strategy.

https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

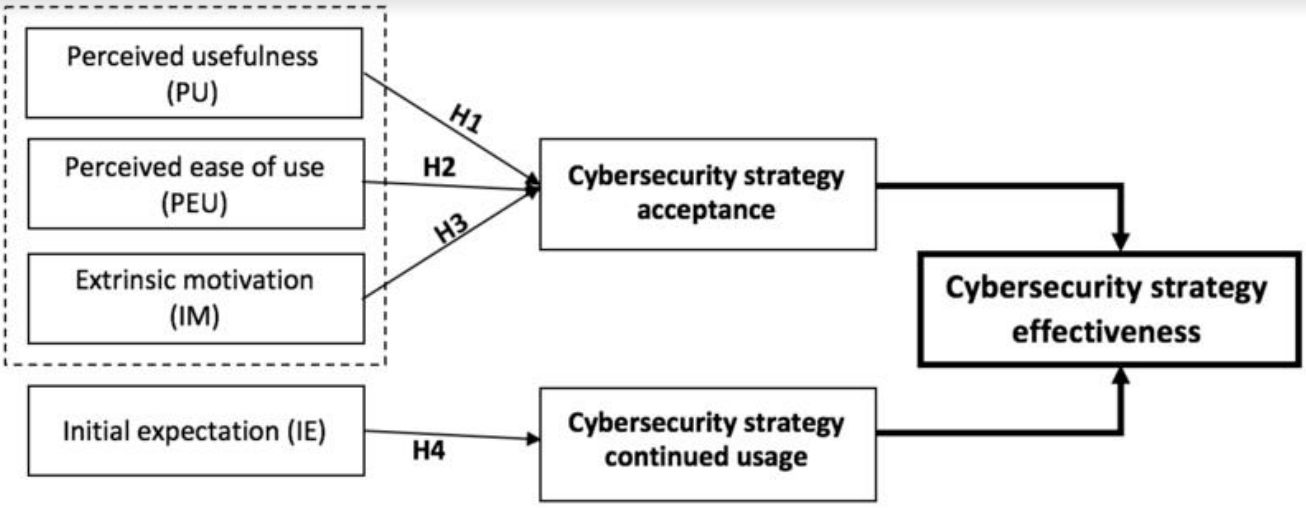

Fig.3:Research model

III. RESEARCH METHOD

3.1. Theoretical study: The password authentication method usage

Users' authentication is the first-step to maintain the privacy, integrity and availability of information. Cybersecurity strategy involve that access to information should be controlled, as indicated on the standard ISO27002 (ISACA, 2013): Access control rules and rights for each user or group of users should be clearly stated in an access control policy. However, password authentication system has historically been the first method of users' access control.

Despite a growing number of graphical and biometric authentication mechanisms, passwords remain the most familiar and commonly-used form of user authentication in organizational settings (Inglesant & Sasse, 2010).

Although, the lack of effective usage of password authentication method introduce several security breaches, in this respect, we investigate the impact of incorrect users' usage of password by not following the cybersecurity guidelines.

According to (Carstens, McCauley-Bell, Malone, & DeMara, 2004), password issues are the second most likely human error risk factors to impact information systems. For example, users usually use the same password to gain access to several systems and websites or use a simple password to recall it such as family name or phone number. In general, factors in password policy that increase the user effort include: password strength, type (character restrictions); numbers of passwords the user has to remember; and frequency of changing passwords (Inglesant & Sasse, 2010). In this study, we support the hypothesis that users' behavior influence on cybersecurity strategy by the incorrect usage of password (Figure 4).

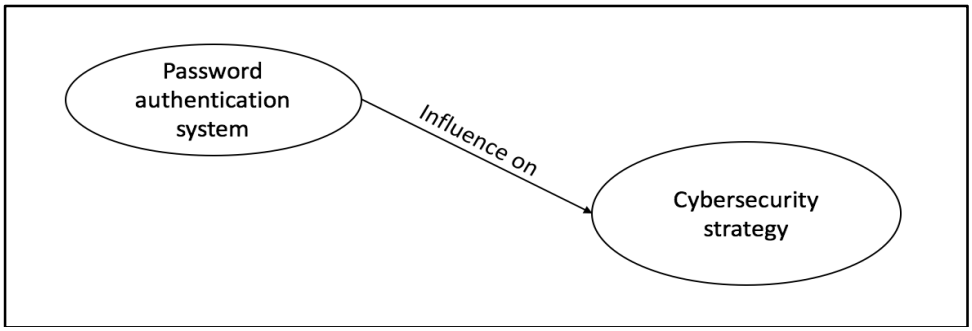

Fig.4:The influence of incorrect users' usage of password

https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

The following section introduce an empirical study taking into account our hypothesis to assert the influence of users' behavior on the effectiveness of cybersecurity strategy. We use the password authentication as example because we believe that its the most popular and familiar cybersecurity procedure used by everyone.

3.2. Empirical study

We conducted an empirical investigation in a population of password users. A password information security questionnaire had been shared with over 2000 users to determine how the way of password authentication system's usage impacts the information security and safety. This research was conducted to address the human behavior factor and influence on the effectiveness of the cybersecurity strategy. Our interest is in understanding the relationship between users' behaviors and cybersecurity strategy efficacy.

The data collected from several information system's users, as individuals (students) or employees (in public or private sector). Our empirical study doesn't take into consideration a specific context in order to introduce several kind of users. The main aim is to develop a correlation between what is improved theoretically and the social reality emanate from the empirical study. So, an e-mail soliciting participation in the survey was sent to the approximately of 2,000 computer's users and a total of 245 valid responses were collected from the current user group. The demographic profile of the survey is represented in the tableau 3:

Table.3: Demographic profile of the survey

Type	Category	Distribution
Age	- < 20 years - 20 – 40 years - > 40 years	- 3% - 67% - 30%
Sector	- Pubic sector - Private sector - Students	- 46% - 34% - 20%
Experience of using a computer	- 3 – 10 years - > 10 years	- 24% - 76%

Based upon the survey results, 28% of respondents don't use a password to log in, which mainly justified by the useless of passwords (59%), the forgotten of password (12%), the inflexibility of password usage (12%) and 17% of respondents join the no-usage of passwords to the time factor (Figure 5).

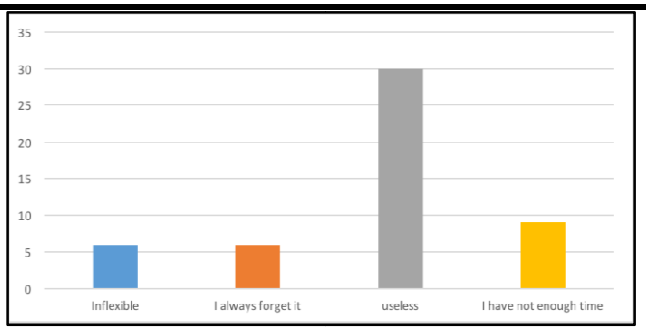

Fig.5: the reasons for no-password usage

The analysis of user's response in the first step of the survey confirms some of the aforementioned hypothesizes (H1, H2) which clarify that Attitude toward behavior, Perceived usefulness and Perceived ease of use influence on the cybersecurity effectiveness.

User's response	Hypothesis	Comment
Useless	H1	Users don't believe that using a password to log in would enhance their job performance;
Inflexible & always forgot the password	H2	Users don't believe that using a password would be free of effort;
Don't have a time	H2	Users believe that using a password will take a part of their time.

About 80% of the participants to the survey are employees, 68% of them indicate that their organizations involve the use of passwords, 29% of them affirm that they don't follow the organization's procedures. Three different reasons are cited by the respondents, which confirm the other hypothesizes (H3, H4), which clarify the impact of extrinsic motivation and the initial expectation on the cybersecurity efficiency.

User's response	Hypothesis	Comment
I don't manipulate critical data	H4	Users have a wrong expectation about the manipulated data and the importance of the password usage to protect their data and the data of their network.
There are no penalties for not using it	H3	Users haven't an extrinsic motivation to follow the procedure, the user isn't driven by the external influence

https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

Difficult to apply	H2	Users believe that following organization's procedure would take more effort;

The three last questions in the survey try to identify user's behavior with the password use. The first question is related to the techniques used to remember the passwords, 122 of respondents indicate that they use personal information, 34 write it down and 15 users indicate that they save them in a mobile device. However, these practices can cause personal and organization data falsification and influence on the cybersecurity strategy effectiveness (Figure 6).

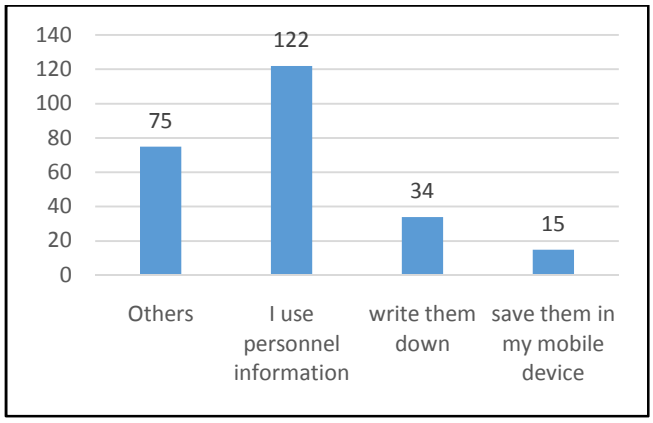

Fig.6:Techniques used to save passwords

The second question is How many different passwords do you use? 29% of respondents use one password to log in (computer and other applications) which present one of the most critical threat in each cybersecurity strategy, when the confidentiality of information is not guarantees.

However, the last question tries to find out How often users share their passwords, the result was unexpected, where 10% always share their password and 32% sometimes (Figure 7). In this case both the confidentiality and the integrity of data can't be ensured.

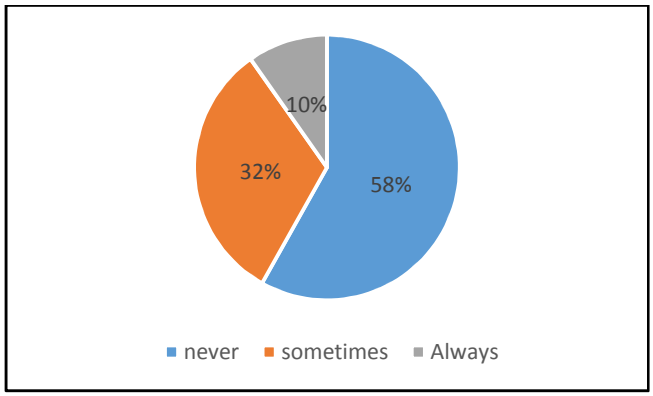

Fig.7:How often users share their passwords?

Our main sample consists of 240 computer users with several position statuses (employees or students) to identify their behaviors when they use a password to log in. However, our objective was to understand and assert the influence of users' behaviors with a basic and simple example, which is the authentication method by using a password. It seems to be clear that users' behaviors have an important impact on data safety and security, and even if the robustness of the organization's cybersecurity strategy, the users' behavior can influence on their effectiveness.

IV. DISCUSSION

The findings of this study suggest that users' behavior play an important role in determining the level of cybersecurity strategy efficacy. We propose that cybersecurity strategy effectiveness is strictly depending on the acceptance and the continued usage of the strategy, when the human factor is the critical element of success. The empirical results of our study rendered clear support for its core hypotheses: users' behavior have a direct influence on the cybersecurity strategy. However, the behavior is characterized by: the perceived ease of use, perceived usefulness, extrinsic motivation and initial expectation.

The first conclusion is that the system must be easy to use and don't involve the knowledge of a long series of rules and take into account users' feedback and awareness' level of cybersecurity issues because perceived easy of use plays a pivotal role in the user acceptance of cybersecurity strategy.

The second conclusion support that user don't believe that the cybersecurity strategy can be useful for him and can protect its data which make the perceived usefulness one of the critical keys influencing the cybersecurity strategy efficacy.

The third conclusion is that users aren't stupid but they are unmotivated, end users must be motivated to follow the cybersecurity strategy which involve an extrinsic motivation from the organization environment.

The last conclusion is that users do not think they are at risk, this initial expectation came from the user feedback and level of awareness and can be related also to a bad experience with the cybersecurity strategy which involve the needs to improve the users training and education about the cybersecurity strategy before filed application.

V. CONCLUSION

The definition of a successful cybersecurity strategy as a means of securing personal and organizational data requires a systematic approach including human factor as a key of success. This study started with an identification of users' behaviors from the theoretical studies as used in

https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

management science. At first, we shed light on the key aspects of user's characteristics based on the Bayesian networks for user modeling. Then, we explained the user's continued usage of the cybersecurity strategy based on the Expectation-Confirmation model.

In this paper, we have argued that users' behaviors have an important influence on the effectiveness of cybersecurity strategy. Drawing on previous work on users' behavior and based on an empirical study, we asserted our hypothesis by using a very known example of authentication method, which is password using. In this context, several factors have been explored and studied in order to understand how users' behaviors can influence on organization cybersecurity strategy effectiveness.

In this research program we achieved our objective by understanding the users' behaviors and asserting the important role played by users in the success of any cybersecurity strategy. The finding may help information security professionals to define a user charter, which control user's behavior in a specific environment.

REFERENCES

[1] Alavi, M., & Joachimsthaler, A. (1992). Revisiting DSS Implementation Research: A Meta-Analysis of the Literature and Suggestions for Researchers, *16*(1).

[2] Bhattacherjee, A. (2001). Understanding information systems continuance: an expectation-confirmation model, *25*, 351–370.

[3] Carstens, D. S., McCauley-Bell, P. R., Malone, L. C., & DeMara, R. F. (2004). Evaluation of the human impact of password authentication practices on information security. *Informing Science: International Journal of an Emerging Transdiscipline*, *7*, 67–85.

[4] Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

[5] Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125–128. https://doi.org/10.1145/341852.341877

[6] Dillon, A. (2001). User acceptance of information technology. *Encyclopedia of Human Factors and Ergonomics*.

[7] Dillon, A., & Morriss, M. . (2007). User acceptance of new information technology: theories and models. *Annual Review of Information Science and Technology*.

[8] Elkhannoubi, H., & Belaissaoui, M. (2015). Framework for an effective cybersecurity strategy: fundamental pillars identification, *6*.

[9] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

[10] Hong, S., Thong, J. Y. L., & Tam, K. Y. (2006). Understanding continued information technology usage behavior: A comparison of three models in the context of mobile internet. *Decision Support Systems*, *42*(3), 1819–1834. https://doi.org/10.1016/j.dss.2006.03.009

[11] Horvitz, E., Breese, J., & Heckerman, D. (2013, December). Bayesian networks for user modeling: Predicting the user's preferences. *13th International Conference on Hybrid Intelligent Systems (HIS)*, pp. 144–148.

[12] Hsu, M.-H., Yen, C.-H., Chiu, C.-M., & Chang, C.-M. (2006). A longitudinal investigation of continued online shopping behavior: An extension of the theory of planned behavior. *International Journal of Human-Computer Studies*, *64*(9), 889–904. https://doi.org/10.1016/j.ijhcs.2006.04.004

[13] Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 383–392). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1753384

[14] ISACA. (2013). *ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls, Version 2013*. ISO/IEC.

[15] Lee, Y., & Kozar, K. . (2005). Investigating factors affecting the adoption of anti-spyware systems, *48*, 72–77.

[16] Limayem, M., Hirt, S. G., & Cheung, C. M. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *Mis Quarterly*, 705–737.

[17] Morris, J., Marzano, M., Dandy, N., & O'Brien, L. (2012). *Theories and models of behaviour and behaviour change*. Forest research.

[18] Oliver, R. . (1980). A cognitive model for the antecedents and consequences of satisfaction. *Ournal of Marketing Research*, pp. 460–469.

[19] Peltier, T., & Blcakley, J. (2005). Information Security Fundamentals. *USA: CRC Press LLC*.

[20] Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113–122). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2047628

https://dx.doi.org/10.22161/ijaers/3.10.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

[21] Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441. https://doi.org/10.2307/249551

[22] Straub Jr, D. . (1990). Effective IS security: An empirical study. *Information Systems Research*, *3*, 255–276.

[23] Woodhouse, S. (2007). Information Security: End User Behavior and Corporate Culture (pp. 767–774). IEEE. https://doi.org/10.1109/CIT.2007.186