Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 1, Issue1, 2013

Complex passwords: How far is too far? The role of cognitive load on employee productivity

[Research in Progress]

Stephen Mujeye, Nova Southeastern University, USA, smujeye@nova.edu

Yair Levy, Nova Southeastern University, USA, levyy@nova.edu

Abstract

The proliferation of information systems (IS) over the past decade has increased the demand for system authentication. While the majority of system authentications are password-based, it is well documented that passwords have significant limitations. To address this issue, companies and system developers have been placing increased requirements on the user to ensure their passwords are more complex and consequently stronger. In addition to meeting a certain complexity threshold, the password must also be changed on a regular basis. In corporate environments, such increased demand can make a significant impact on employees' productivity. As the cognitive load increases on the employees using complex passwords and changing them, they may have difficulty recalling their passwords. This may hinder employees' productivity as they spend more time contacting the Help Desk to reset their passwords. As such, the focus of our study is to determine the effects of raising the cognitive load of the authentication strength for users upon accessing a system. In this work-in-progress study, we seek to provide a blueprint for a research study that will uncover the point at which raising the authentication strength for passwords becomes counterproductive. A quasi-experiment is proposed including detailed experimental procedure and data analyses. The paper ends with conclusions and implications.

Keywords: Access Control, Passwords, Password Strength, Authentication, Security, Cognitive Load Theory.

Introduction

Authentication of users is an important security issue within any type of information system (IS), be it a Web-based or corporate network. Ren and Wu (2012) defined authentication as "the act of confirming that the communicating entity is the one claimed" (p.714). Authentication ensures that only legitimate users are allowed to gain access into a system or a network. One of the most widely used methods to authenticate users is through the use of passwords (Chiasson, Forget, Stobert, van Oorschot, & Biddle, 2009). In order for passwords to be effective, they need to be complex and resist several types of password attacks (Tsai, Lee, & Hwang, 2006). Passwords by their nature are vulnerable to attacks like "dictionary attacks" and "brute force attacks" (Molloy & Li, 2011). A dictionary attack is a malicious event where an attacker builds a database populated with various combinations of possible passwords, which are referred to as "the dictionary" (Chakrabarti & Singha, 2007). The attacker then attempts to logon to the system using the passwords from that database; if one password fails, the attacker proceeds to the next one until all options in the database have been exhausted. Such process can be done

automatically using code to expedite the attack trails. Dictionary attacks can be either offline dictionary attacks, if they are non-interactive, or online dictionary attacks if they are online and interactive. Medlin and Cazier (2007) described the brute force attack as an attack that occurs when every possible combination of letters, numbers, and symbols is used in an effort to guess a password.

It appears that a need exists to better understand the balance between improving password security and its complexity requirement placed on users (Carstens, McCauley-Bell, Malone, & Demara, 2004). Moreover, it is evident that when passwords are too complex, users may forget their passwords, while it can have negative effects on productivity and task completion time. In situations where employees forget their passwords, time and resources are wasted while the employee seeks assistance in resetting their passwords. As such, the focus of our work-in-progress research was aimed at uncovering the point at which raising the authentication strength for passwords becomes counterproductive.

Theoretical Framework

A significant increase has occurred in the number of ISs developed, implemented, and used by organizations (Erlich & Zviran, 2010). One of the challenges that accompanies the increased reliance on IS is the security via enforcement of strong authentication methods. One of the branches of security is access control, which governs who gains control to the IS. Kumari and Chithraleka (2012) mentioned that the main objective of access control is to protect resources from unauthorized access at the same time ensuring authorized access. One of the prerequisites of access control, at the foundation of security, is authentication. According to Levy, Ramim, Furnell, and Clarke (2011), "User authentication is the process of verifying an attempted request of an individual (i.e. 'the user') to gain access to a system" (p. 104). Menkus (1998) stated that methods of user authentication can be further dichotomized into three categories:

- Knowledge-based authentication – what the user knows
- Possession-based authentication – what the user has
- Biometric-based authentication – what the user is

From these three categories, the most widely used method of user authentication is knowledge-based authentication. According to Erilich and Zviran (2009), knowledge-based user authentication can be further divided into different categories, which include:

- Character-based
- Image-based
- Question/answer-based

In the categories above, the password method, a character-based method is the most widely used authentication method. In order for passwords to be effective and to reduce the problem of dictionary attacks or brute force attacks, some rules must be followed (Tsai, Lee, & Hwang, 2006). The rules include:

- Reduce or eliminate the use of dictionary words

- Increase password strength by increasing complexity (which includes minimum length, use of special characters, inclusion of numbers, & uppercase letters)

As noted above, passwords are the most-used method of user authentication in all types of computer environments (Kim, 2012). Oreku and Li (2009) also referred to the password as the frontline of defense against attackers and that virtually every system uses password as a method of authenticating users. Despite this, passwords have many limitations. Meng (2012) pointed out that passwords suffer from security and usability problems. Because users have limitations in long-term memory, they tend to use short passwords that are easy to remember. The use of short and easy-to-remember passwords presents a security risk to the organization from attacks like the dictionary attack and brute force attack. Consequently, it is important for users to avoid using simple dictionary words and to use complex passwords. In order to prevent users from using weak passwords, organizations create password policies (Shay, Komanduri, Kelly, Leon, Mazurek, Bauer, Christin, & Cranor, 2010). Password policies dictate the minimum number of characters, complexity, expiration limits, and/or the number of times a user can reuse the same password. The characteristics of a password policy with some examples are noted in Table 1 (Inglesant & Sasse, 2012).

Table 1: Characteristics and Examples of Password Policy

Characteristic	Example
Length	7-8 Characters
Character Sets	At least one character from three of four classes; Character classes are uppercase letters, lower case letters, digits, and non-alphanumeric characters
Expiry	180 Days
History	Must not be similar to previous 12 passwords

Shay et al. (2010) also pointed out that while strong password policies improve security, those users may have difficulty remembering the passwords. Novakivic, McGill, and Dixon (2009) claimed that the use of strong passwords and constantly changing them can have counterproductive effects, as it places too much cognitive load on the users. As the cognitive load increases, it may result in users taking time away from performing their job functions, as well as increasing helpdesk and support requests to reset passwords (Brostoff & Sasse, 2000).

The cognitive load theory (CLT) is a seminal work based on cognitive science that equates the human mind to a processing system with working memory and storage memory (Sweller, 1988). Information that humans receive is stored in the long-term memory after working memory processes it. Miller (1956) found that the working memory is limited in such a way that the human mind can only hold seven items simultaneously. Hogg (2007) further stated that working memory is limited, which makes it difficult for humans to process complex tasks. He further defined cognitive load as “the processing of information that occurs in working memory” (p.188). The limitations of the user’s memory can affect the ability to remember complex passwords (Boechler, 2006). Novakivic et al. (2009) also pointed out that requiring users to constantly change strong passwords places a high cognitive load on them.

Experimental Research and Procedures

To investigate the effects of increasing password strength, a lab experiment will be used. Two groups, experimental and control will be used (Ellis & Levy, 2011). As noted above, organizations often require their employees to make up passwords that are more complex; however, their strength and complexity can interfere with employees completing their tasks. This research seeks to find the point at which passwords become too complex for users and become counterproductive. Two experimental groups (Group A & Group B) will be constructed with 10-15 users in each group. A third group (Group C) will be constructed as the control group, and it will also have 10-15 users. The study participants in the three groups will come from a local college in different majors at different levels in their academic levels. All users in the three groups will be randomly assigned. The experiment is planned for a period of 11 weeks.

To test the effects of increasing password strength, a system will be set up and all three groups will be asked to logon to the system. Once logged in, the users will be asked to perform specific functions. The system will track the average number of logon attempts for all the three groups. It will also track the average time it takes for each user to logon to the system, as well as the average time they will take to complete specified tasks to emulate workplace tasks. The system will have auditing mechanisms built in to track and measure all the tasks above. If any of the users request assistance with resetting passwords, the number of times reset over the period of the experiment will also be tracked.

The users will have different password strengths required based on the group membership and time within the experiment. The first experimental group (Group A) will begin with a password that is at least seven characters long, with one uppercase letter, in week one. As listed in Table 2, the authentication strength will increase in week two through week six, and their performance will be measured during each week based on:

- Average logon attempts
- Average time to log on
- Average task completion
- Number of requests for assistance

The authentication strength will be the strongest in week six, when it will increase to include a passphrase with 20-30 characters, one uppercase letter, one number, and two special characters. After the performance is measured, it will begin to decrease in weeks seven through week 11 and the performance will be measured in each of those weeks as well.

The second experimental group (Group B) will begin week one with a password that includes a passphrase with 20-30 characters, one uppercase letter, one number, and two special characters. As listed in Table 2a, it will decrease each week until week six when it will be 7-10 characters with one uppercase letter. The performance for Group B will be measured during each week based on the same criteria that was used for Group A. As listed in Table 2, the password strength for Group B will begin to increase in week seven through week 11 and the performance will be

measured each week as well. Figure 1 illustrates how the password strength will be manipulated throughout the experiment.

Table 2a: Experimental Design – Authentication Strength (AST) – Week One to Week Six

		Measure Week 1	Treatment Week 2	Measure Week 2	Treatment Week 3	Measure Week 3	Treatment Week 4	Measure Week 4	Treatment Week 5	Measure Week 5	Treatment Week 6	Measure Week 6
Assigned Randomly	Group A (Experimental Group 1)		Increase AST to7-10 characters 1 upper case 1 number		Increase AST to 7-10 characters 1 upper case 1 number 1 special character		Increase AST to 10-15 characters 1 upper case 1 number 2 special characters		Increase AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Increase AST to Passphrase 20-30 characters 1 upper case 1 number 2 special characters	
	Group B (Experimental Group 2)		Decrease AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Decrease AST to 10-15 characters 1 upper case 1 number 2 special characters		Decrease AST to 7-10 characters 1 upper case 1 number 1 special character		Decrease AST to 7-10 characters 1 upper case 1 number		Decrease AST to 7-10 Characters 1 upper case	
	Group C (Control Group)		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character	

Table 2b: Experimental Design – Authentication Strength (AST) – Week Seven to Week 11

		Treatment Week 7	Measure Week 7	Treatment Week 8	Measure Week 8	Treatment Week 9	Measure Week 9	Treatment Week 10	Measure Week 10	Treatment Week 11	Measure Week 11
Assigned Randomly	Group A (Experimental Group 1)	Decrease AST to Passphrase 15-20 characters 1 upper case 1 number 2 special characters		Decrease AST to 10-15 characters 1 upper case 1 number 2 special characters		Decrease AST to 7-10 characters 1 upper case 1 number 1 special character		Decrease AST to 7-10 characters 1 upper case 1 number		Decrease AST to 7-10 Characters 1 upper case	
	Group B (Experimental Group 2)	Increase AST to 7-10 characters 1 upper case 1 number		Increase AST to 7-10 characters 1 upper case 1 number 1 special character		Increase AST to 10-15 characters 1 upper case 1 number 2 special characters		Increase AST to 15-20 characters 1 upper case 1 number 2 special characters		Increase AST to Passphras e 20-30 characters 1 upper case 1 number 2 special characters	
	Group C (Control Group)	No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character		No Change 7-10 characters 1 upper case 1 number 1 special character	

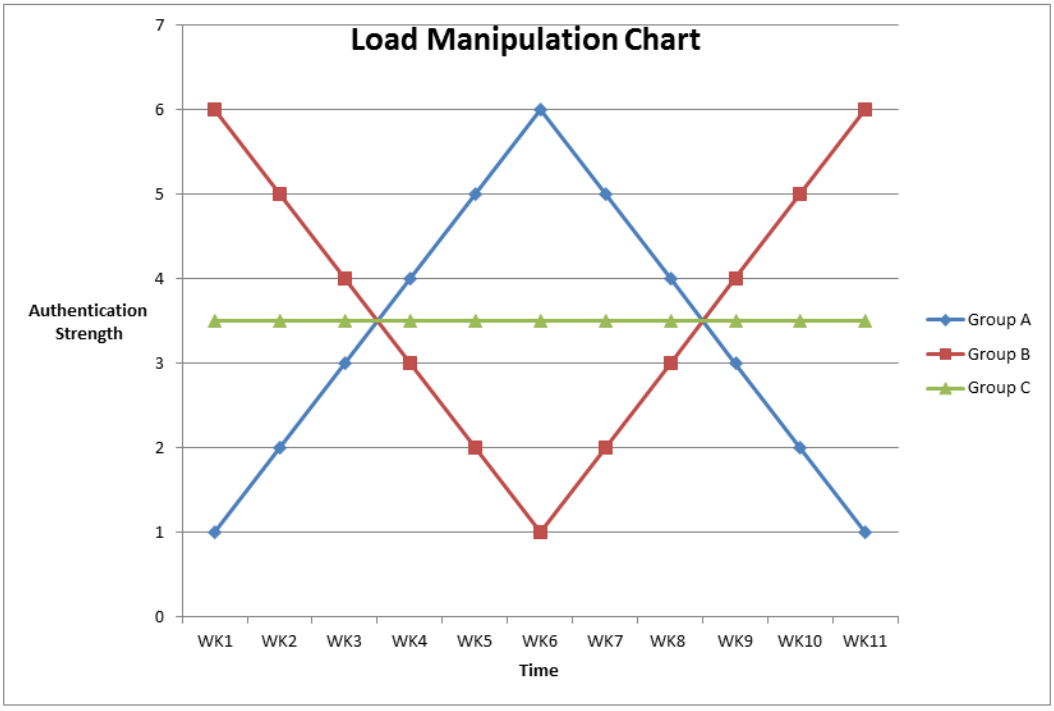

Figure 1: Load Manipulation Chart

The control group (Group C) will have the same password throughout the 11 weeks. The password will be at least 7-10 characters, one uppercase letter, one number, and one special character. The performance for Group C will be measured each week based on the same criteria used for Group A and Group B.

Problem Statement, Goals, and Hypotheses

The research problem that this study seeks to address is the obstacle of password memorability, which is further complicated by the fact that users have many passwords to recall for computers, networks, and Websites among other systems (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). Wiedenbeck et al. further noted that passwords have to be constantly changed in order to improve security, which increases the burden on the human mind and makes it difficult for users to remember their passwords. Henry (2007) pointed out that an infrequently used password that must be changed constantly, along with other security countermeasures, increases the cognitive load on users. Kinsbourne and George (1974) determined limitations to the human memory that affect humans' ability to recall complex passwords that must be constantly changed.

The need for this work is demonstrated by the work of Novakivic, McGill, and Dixon (2009). In their work, Novakivic et al. acknowledged that passwords are the main way of authenticating users, as well as that they need be strong. They also pointed out the challenge of increasing

password security, which results in a negative impact on usage. Cahill, Martin, Phegade, Rajan, and Pagano (2011) also demonstrated how increasing password complexity requirements can lead to problems when users have hard times remembering the requirements. The main goal of this study is to assess the effects of raising the cognitive load of the authentication strength for users upon accessing a system. This study will also assess the point at which raising the authentication strength for passwords becomes counterproductive. The following hypotheses are presented based on the research goals (noted in null layout):

H1: There will be no significant differences on the *number of logon attempts* between Groups A, B, and C.

H2: There will be no significant differences on the *average logon times* between Groups A, B, and C.

H3: There will be no significant differences on the *average task completion times* between Groups A, B, and C.

H4: There will be no significant differences on the *amount of requests for assistance* between Groups A, B, and C.

Following the experimental data collection, the data will be subject to pre-analysis data screening (Levy, 2006; Mertler, & Vannatta, 2010). The pre-analysis data screening will include visual observation of the data to ensure that no incorrect data entry were made and multivariate outlier analysis using Mahalanobis Distance. Additionally, normality, linearity, and homoscedasticity tests will be made to ensure the data is obeying the analyses assumptions. Specifically, factorial multivariate analysis of variance (MANOVA) will be used to test the hypotheses.

Conclusions

This work-in-progress research outlines a quasi-experiment aimed to assess the effects of raising the cognitive load of the authentication strength for users when accessing a system by varying the password requirements. The quasi-experiment was proposed to include three groups: two experimental groups (A & B), and a control group (C). Both Group A and Group B will experience an increase and a decrease in password strength throughout the experiment. The effects of the increase or decrease will be recorded each week as the performance of the users is measured. The results of this experiment should demonstrate the effects of increasing password strength on the users, while assessing their ability to sustain increased complexity of passwords and to perform given tasks. Based on the information gathered, a determination should be made about the point at which the logon attempts, time to logon, and task completion changes to a point of reduced productivity. Since the number of times users request assistance will be recorded, it is hypothesized that as the password strength increases, a change will occur in the frequency users request assistance. After the study is completed, the findings as they relate to the hypotheses will be recorded.

This work-in-progress study is anticipated to provide deeper insight as well as understanding of balancing increased authentication requirements and the capabilities of the human mind to recall such complex passwords. The results of this study are anticipated to help in providing recommendations for both the research and practice. It is the main hope of this study to uncover the level at which the authentication strength will affect the user's ability to perform other tasks.

References

Boechler, P. (2006). Understanding cognitive processes in educational hypermedia. *In C. Ghaoui (Ed.), Encyclopedia on Human Computers Interaction*, (648-651). Hershey, PA: Information Science Reference. doi:10.4018/978-1-59140-562-7.ch097

Brostoff, S., & Sasse, M. (2000). Are passfaces more usable than passwords? A field trial investigation. *Proceedings of the Human Computer Interactions Conference 2000*, London, UK, pp. 405-424.

Cahill, C. P., Martin, J., Phegade, V., Rajan, A., & Pagano, M. (2011). Client-based authentication technology: user-centric authentication using secure containers. *Proceedings of the Seventh ACM Workshop on Digital Identity Management*, New York, NY, pp. 83-92.

Carstens, D., McCauley-Bell, P., Malone, L., & DeMara, R. (2004). Evaluation of the human impact of password authentication practices on information security. *Information Science Journal*, *7*(1), 67-85.

Chakrabarti, S. & Singbal, M. (2007). Password-based authentication: preventing dictionary attacks. *IEEE Computer Society, 40* (6), 68-74.

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. C., & Biddle, R. (2009). Multiple interference in text passwords and click-based graphical passwords. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Swinton, UK, pp. 500-511.

Erlich, Z., & Zviran, M. (2010). Goals and practices in maintaining information systems security. *International Journal of Information Security and Privacy*, *4*(3), 40-50. doi: 10.4018/jisp.2010070103

Erlich, Z., & Zviran, M. (2009). Authentication methods for computer systems security. In Khosrow-PourM. *Encyclopedia of information science and technology. (*Vol. 1, pp. 288-293). Hershey, PA: Informaiton Science Reference. DOI: 10.4018/978-1-60566-026-4.ch049

Henry. P. T. (2007). *Toward usable, robust memometric authentication: An evaluation of selected password generation assistance.* Dissertation Abstracts International, 68 (09),

(UMI No. AAT 3282618). Retrieved March 31, 2013 from Digital Dissertations database.

Hogg, N. (2011). Measuring cognitive load. *Handbook of Research on Electronic Surveys and Measurements*, 188-194. Hershey, PA: Information Science Reference. DOI: 10.4018/978-1-59140-792-8.ch020

Inglesant, P., & Sasse, M. (2010). The true cost of unusable password policies: password use in the wild. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* New York, NY, pp. 383-392.

Kim, I. (2012). Keypad against brute force attacks on smartphones. *Institution of Engineering and Technology. 6*(2), 71-76.

Kinsbourne, M., & George, J. (1974). The mechanics of the word frequency effect on recognition memory. *Journal of Verbal Learning and Verbal Behavior,* 13, 63-69.

Kumari, K., & Chithraleka, T. (2012). A comparative analysis of access control policy modeling approaches. *International Journal of Secure Software Engineering, 3*(4), 65-83.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science.

Levy, Y., & Ellis, T. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of information, knowledge, and management*, 6, 151-161.

Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011). Comparing intentions to use university-provided vs. vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems, 28*(2), 102-113. doi:10.1108/10650741111117806

Medlin, B. D., & Cazier, J. A. (2007). An empirical investigation: health care employee passwords and their crack times in relationship to HIPPA security standards. *International Journal of Healthcare Information Systems and Informatics, 2*(3), 39-48.

Meng, K. (2012). Designing click-draw based graphical password scheme for better authentication. *IEEE Seventh International Conference on Networking, Architecture, and Storage*, Fujian, China, pp. 39-48.

Menkus, B. (1998). Understanding the use of passwords. *Computers & Security, 7*(2), 132-136.

Mertler, C. A., & Vannatta, R. A. (2010). *Advanced and multivariate statistical methods* (4th ed.). Glendale, CA: Pyrczak.

Miller, A. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review, 63,* 81-97.

Molloy, I., & Li, N. (2011). Attack on the gridcode one-time password. *Proceedings of the 6th ACM symposium on information, computer and communications security,* New York, NY, pp. 306-315.

Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding user behavior towards passwords through acceptance and use modeling. *International Journal of Information Security and Privacy*, *3*(1), 11-29.

Shay, R., Komanduri, S., Kelly, P., Leon, P., Mazurek, M., Bauer, L., Christin, N., & Cranor, L. (2010). Encountering stronger password requirements: user attitudes and behaviors. *Symposium on Usable Privacy and Security.* Redmond, WA, pp. 1-20.

Sweller, J. (1988). Cognitive load during problem solving: effect on learning. *Cognitive Science*, 12, 257-285.

Tsai, C., Lee, C., & Hwang, M. (2006). Password authentication schemes: current status and key issues. *International Journal of Network Security, 3*(2), 101-115.

Oreku, G., & Lin J. (2009). End user authentication (EUA) model and password for security. *Journal of Organizational and End User Computing, 21*(2), 28-33.

Ren, X., & Wu., X. (2012). A novel dynamic user authentication scheme. *International Symposium on Communications and Information Technologies,* Gold Coast, Queensland, Australia, pp. 713-717.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005) PassPoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, *63*(1-3), 102-127. doi:10.1016/j.ijhcs.2005.04.010

Acknowledgments

We would like to thank the anonymous referees for their careful review and valuable suggestions. We also would like to thank the accepting editor, Dr. Alex Koohang, for his recommendations and constructive comments.

Biographies

Stephen Mujeye is a Networking instructor at McHenry County College, Crystal Lake, Illinois. He earned a Bachelor's degree with a double major in Business Management and Business Systems Support Specialist from Siena Heights University, Adrian, Michigan. He has a Master's

degree in Information Resource Management from Central Michigan University, Mt. Pleasant, Michigan and is currently ABD and pursuing his PhD in Information Systems at Nova Southeastern University. He holds a number of industry certifications, including A+, Network+, Security+, and MCTS.

Yair Levy a Professor at the Graduate School of Computer and Information Sciences at Nova Southeastern University and the director of the Center for e-Learning Security Research (CeLSR). During the mid to late 1990s, he assisted NASA to develop e-learning systems. He earned his Bachelor's degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his MBA with MIS concentration and Ph.D. in Management Information Systems from Florida International University. His current research interests include security issues with e-learning systems, cyber-security skills, and cognitive value of information systems. Dr. Levy is the author of 'Assessing the Value of e-Learning Systems' (2006). His research publications appear in numerous peer-reviewed journals and conference proceedings. Also, Dr. Levy has been serving as a member of conference proceedings committee for numerous scholarly conferences. Moreover, Dr. Levy has been serving as a referee research reviewer for hundreds of national and international scientific outlets. He is a frequent invited keynote speaker at national and international meetings on IS, Information Security, and online learning topics. Dr. Levy's teaching interests in the masters level include MIS, system analysis and design, information systems security, e-commerce, and Web development. His teaching interests in the doctoral level include Information Systems Development (ISD) and Advanced Multivariate Research Methods and Statistics. To find out more about Dr. Levy, please visit his site: http://scis.nova.edu/~levyy/