REDUCING CYBERSECURITY RISKS AND INSIDER COMPUTER ABUSE BY BETTER SECURING THE HUMAN FACTOR: IMPROVING ORGANIZATIONAL IT SECURITY COMPLIANCE

Research Paper

Mario Silic, Swiss School of Business and Management, Switzerland mario@ssbm.ch

Ivana Silic, Swiss School of Business and Management, Switzerland ivana.silic@ssbm.ch

Dario Silic, Swiss School of Business and Management, Switzerland dario@ssbm.ch

Abstract

One of the greatest heists in the cybersecurity context resulted in $1 bln loss for financial institutions (Kaspersky, 2015) and was result of an email-spoofing attack in which employees clicked on a link that installed malicious software affecting employees machines. This simple mechanic reveals how a simple phishing email can have disastrous consequences on organizational information systems (IS).

Ensuring compliant security behaviors from employees is a "holy grail" for all companies looking to protect organizational assets. Insider computer abuse, the volitional and non-volitional security violation, is identified as one of the greatest concerns for companies. Despite numerous initiatives to encourage organizational IT security compliance, serious security incidents have increased, often stemming from employees' noncompliant and careless actions (e.g., falling for phishing). Despite the increasing relevance of the employee IS security policy compliance phenomenon, and in light of the digitization of the workplace (e.g. bring your own device, social media use, etc.), important research gaps remain in our understanding of how to effectively reduce employee non-compliant behavior.

While information security research has examined several different theories, methods and techniques for persuading employees to behave securely in organizations, employees still continue to violate IS security policies. In this research paper we set out the research gaps that remain in our understanding of the insider computer abuse and identified the contextual events that precede the IT security policy violation and lead to the employee non-compliant behavior.

Finally, we wish to advance our understanding of this phenomenon through the systematic theory development that can be published in high-ranking international journals by developing new theoretical insights about 1) how to influence employee's motivation to behave more securely and more in compliance with organizational IT security policies and 2) identify contextual factors (e.g., *culture, color, warnings, etc.) that would empower employees to take more informed and better security decisions.*

We believe that our findings can help ***recast extant research and practices*** *that should lead to potentially more effective approach to encouraging employees' security compliance.*

With this theoretical and empirical work, we show how our proposal can make multiple contributions to theory, and how important implications for practitioners can be derived.

Keywords: information security, cybersecurity risks, computer security

1 Introduction

Insider computer abuse is committed by "*employees or others who have (1) access privileges and (2) intimate knowledge of internal organizational processes that may allow them to exploit weaknesses*" (Willison & Warkentin, 2013) and can take form of non-volitional (e.g. accidental entry of data) or volitional actions (employee is deliberately doing an action but without any malicious intentions). The threats arising from organizational insiders are identified as one of the greatest concerns for Information Systems (IS) security managers (Willison & Warkentin, 2013).

One of the greatest heists in the cybersecurity resulted in $1 bln loss for financial institutions (Kaspersky, 2015) and was result of an email-spoofing attack (phishing) in which employees clicked on a link that installed malicious software affecting their machines. Not only, this simple mechanic reveals how a simple phishing email can have disastrous consequences on organizational information systems (IS), but also it confirms that phishing continues to be a major concern for organizations where, according to the recent survey, 53% of them have experienced more advanced, targeted phishing attacks in 2017 (Wombat-Security, 2018). More worrying, the incident revealed that the phishing attack started with employee's non-compliant IT security decision.

Information technology (IT) security compliance deals with techniques and processes that motivate employees to behave more securely when engaging with organizational systems and information (Bulgurcu, Cavusoglu, & Benbasat, 2010). Such compliance is of increasing concern for management and executives because of the global explosion of organizational security issues. Generally, the objective of IT security compliance is threefold: (1) to mitigate or avoid security incidents and risks that are often caused by negligent employees (Crossler et al., 2013; Lowry, Posey, Bennett, & Roberts, 2015; Willison & Warkentin, 2013); (2) to thwart criminal security behavior and computer abuse (e.g., Hu, Xu, Dinev, & Ling, 2011; Lowry et al., 2015; Willison & Warkentin, 2013);

and (3) to encourage prosocial and protective security behaviors in employees (Hsu, Shih, Hung, & Lowry, 2015; Posey, Roberts, Lowry, Bennett, & Courtney, 2013).

A number of promising studies have applied various techniques to motivate employees to adopt secure intentions and behavior—from deterrence techniques (e.g., D'arcy & Herath, 2011; Herath & Rao, 2009; Hu et al., 2011; Willison & Warkentin, 2013), to discouraging employee neutralization (e.g., Barlow, Warkentin, Ormond, & Dennis, 2013; Siponen & Vance, 2010), to increasing awareness of the risks and potential costs of noncompliance (e.g., Bulgurcu et al., 2010; Hu et al., 2011; Vance & Siponen, 2012), and even to using more explicit threats and fear appeals (e.g., Boss, Galletta, Lowry, Moody, & Polak, 2015; A. C. Johnston & Warkentin, 2010; Allen C. Johnston, Warkentin, & Siponen, 2015; Posey, Roberts, & Lowry, 2015; Siponen, Mahmood, & Pahnila, 2014).

Despite these efforts, employees remain the “***weakest link***” in organizational IT security because employee behavior can easily undermine it (Da Veiga & Eloff, 2010; Willison & Warkentin, 2013; Yang & Lee, 2015); moreover, it is ultimately the employees’ responsibility to comply and often they do not (Crossler et al., 2013; Posey et al., 2015).

Understandably, a **fundamental concern has been raised as to whether extant organizational security approaches are efficacious.** For example, deterrence techniques were designed for criminal behavior and thus may be inappropriate for mere security policy noncompliance (D'arcy & Herath, 2011; Willison & Warkentin, 2013). It may be a bad idea to employ techniques involving threats and raising risks because these can have unintended consequences, including negative employee reactance (Lowry & Moody, 2015; Lowry et al., 2015). Even popular protection motivation approaches rooted in fear may not work well in an organizational context (Warkentin, Johnston, Walden, & Straub, 2016).

Through past research we found that in order to more efficiently reduce the insider computer abuse we should try to better understand certain specific events (e.g. ignorance of warning communication or neutralization techniques) that precede the IT security policy violation and lead to the employee non-compliant behavior. Overall, through the past literature we were able to get some first insights about employee’s compliance with IT security policies within the Shadow IT (systems used by employees without explicit organizational IT approval) context.

Hence through this project we aim at answering the following **overarching research questions**:

RQ1: How can we improve employee’s motivation to behave more securely and more in compliance with organizational IT security policies?

RQ2: How can employees make better security decisions in situations in which a binary decision (continue/exit) is needed?

RQ3: What are the factors that will drive a more persuasive and effective warning communication in the unique cultural context?

RQ4: How organizations can contribute to improving employee’s compliance in the Shadow IT context?

We detail each of the above research directions in the next paragraphs where we also provide the current state of research in the field

1.1 Current state of research in the field

Research stream #1: Improving employee’s motivation to behave more securely and more in compliance with organizational IT security policies

Turning away from the negative, extrinsic approaches, security education training awareness (SETA) programs leverage a more positive approach that is often embraced by researchers and organizations. SETA programs aim to provide employees with the knowledge and motivation necessary to comply with security policies when confronted with a security risk (Burns, Roberts, Posey, Bennett, & Courtney, 2015; Crossler & Bélanger, 2009; Puhakainen & Siponen, 2010; Whitman, 2003).

Employee training is notorious for failing, because even though it often delivers the right content, employees lack the motivation to embrace the learning and actually apply it in their everyday work, thus causing performance and even reputational failures (Clardy, 2005; Hughey & Mussnug, 1997; Martocchio & Judge, 1997; Poulston, 2008). This is especially true in a security context in which most employees are not experts, lack efficacy, and do not see the relevance of caring about security in the context of their everyday work tasks and pressures.

We propose that a pragmatic solution must begin with the recognition that most security training is **not enjoyable** or **motivating**—it is often perfunctory, arcane, and outside employees' normal practice and expertise.

We posit that security training based on gamification principles (e.g., game-like features applied to non-gaming contexts) should be an effective approach for achieving higher intrinsic motivation, learning, coping skills, and subsequent security compliance. People are simply more motivated and conscientious when they have an enjoyable, immersive experience.

In particular, we argue that a ***contextualized gamification design should improve employees' organizational IT security training and compliance.*** That is, a gamified security training can be created in a way that not only it enables the right content to be delivered, but also enables employees to have enhanced immersion and increased intrinsic motivations, learning, and coping, such that their intentions and actual behaviors become more compliant with the security training and policies.

Research stream #2: Making better, more informed security decisions

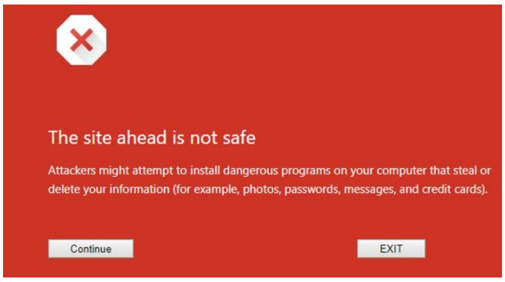
Similar to real-world situations (e.g., traffic lights), in the digital realm, individuals are confronted with computer security communication where they are asked to make a security decision. The security communication aims at informing users about potential hazards that may occur, if the user continues with his/her action (Silic, Barlow, & Ormond, 2015). The user's action usually corresponds to a binary decision, continue or exit, where the end result can have important security implications. But it can also consist of a more complex decision-making process where user is asked to evaluate the risk characteristics and consequently take a decision.

Previous research has explained that the user's ignorant behavior is due to habituation (Anderson, Vance, Kirwan, Eargle, & Howard, 2014; Sunshine, Egelman, Almuhimedi, Atri, & Cranor, 2009), where users simply do not read security communication (e.g., warning messages) and, therefore, ignore and skip them (e.g. Akhawe & Felt, 2013; Sunshine et al., 2009).

However, the problem with all of these improvements is the fact that the user is still mostly left alone in his/her decision-making process (Figure 1a). Regardless of the visual cue improvements, the decision is still purely static and based on the limited information that the user receives through security communication content or visual cues. The problem in this human-computer decision-making interaction is that for some users that have limited security knowledge (i.e., novice users) the simple security communication that is presented to them may not be sufficient to take the right decision.

We argue that in order to improve the user's adherence, additional help is needed so that the user can be better advised, informed or given time to think about the consequences of his/her actions.

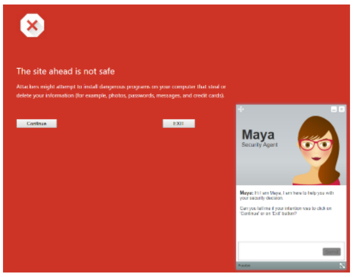
In particular, we argue that an alternative course of action has to be proposed to the user to that user can take a better and more informed security decision. For example, one way of achieving this is through a novel application of a **Security Bot (Chat Bot)** (Figure 1b) as part of the warning message with the objective to engage into the conversation with the user by textual means in order to provide a real-time conversational support to user in order to make a better, more informed and smarter security decision.



The site ahead is not safe

Attackers might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

Figure 1a. Warning Message (Google Chrome v42)



The site ahead is not safe

Attackers might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

Maya: Hi! I am Maya, I am here to help you with your security decision.

Can you tell me if your intention was to click on 'Continue' or on 'Exit' button?

Figure 1b. Warning Message with Security Bot

Research stream #3: Factors that will drive a more persuasive and effective warning communication in the unique cultural context

People make thousands of decisions every day of their lives. Many of these decisions are based, for example, on the color inputs that we have to process. If a driver sees a green light, then he or she will continue, but seeing a red light will send a signal to stop the car as danger could be ahead. Interestingly, research has already found that color plays an important role in psychological functioning in which color influences affect, cognition, and human behavior (Elliot & Maier, 2014). Emotion was another dimension found to be closely tied to color preferences (Kaya & Epps, 2004). Color can be seen as an important trigger that affects the way humans perceive objects surrounding them, which influences their psychological reactions and consequently, their behavioral intentions (Valdez & Mehrabian, 1994).

Research has established a clear relationship between the red color and threat, failure, and avoidance (e.g., Genschow, Reutner, & Wänke, 2012; Kliger & Gilad, 2012; Shavit, Rosenboim, & Cohen, 2013).

These contradictions (i.e., different meanings of the same color application) are true not only for the red color but also for all other colors. A key explanation for this can be found in the fact that “color meanings and, therefore, color effects are context specific. The same color can have different meanings in different contexts, leading to different implications” (Elliot & Maier, 2014, p. 109). Color effects and meanings in one context may not be true and work in another context. Notably, in the information systems (IS) context, and in particular in the IS security context, studies dealing with color effects on the human reasoning and decision-making processes are relatively scarce.

We argue that different factors (such as color) will drive a more persuasive and effective warning communication in the unique cultural context different. Color is just one of the possible factors and further research is needed to understand what other factors could have similar impact on the warning communication.

Research stream #4: How organizations can contribute to improving employee's compliance in the Shadow IT context?

In todays' hyper-connected world in which speed, productivity, adaptability and efficacy are driving and defining individual's capabilities to be faster and more efficient, individual behavior is often characterized through accessing, acquiring or using the widely available tools, processes or systems that did not receive prior formal Information Technology (IT) department approval. This behavior, termed Shadow IT (but also Rogue IT, Stealth IT, Client IT, shadow systems, workaround systems, or feral systems), represents one of the biggest threats for organizational IT security ecosystems (Silic & Back, 2014). Past research has identified the negative and the positive aspects of Shadow IT. It can spark innovation (Silic, Silic, & Oblakovic, 2016) or it can be more beneficial or efficient than using legacy systems (Behrens & Sedera, 2004; Harley, Wright, Hall, & Dery, 2006).

Although "Shadow IT is a currently misunderstood and relatively unexplored phenomena" (Silic & Back, 2014, p. 274), past research has addressed various aspects of Shadow IT, such as IT governance challenges (Györy, Cleven, Uebernickel, & Brenner, 2012), causes of Shadow IT (Behrens & Sedera, 2004) and its risks and consequences (Behrens, 2009; Behrens & Sedera, 2004; Silic & Back, 2014).

We argue that the Shadow IT antecedents are key to understand as not only by better understanding the Shadow IT mechanisms organizations could improve their IT security, but more importantly employees would have lower needs to use the non-previously approved Shadow IT systems.

Overall, in this research we propose to study four research streams, mutually connected, and their relationship with the insider computer abuse. The four research streams are illustrated on Figure 1 with the impact on each of the IT security ecosystem (employee and organization).

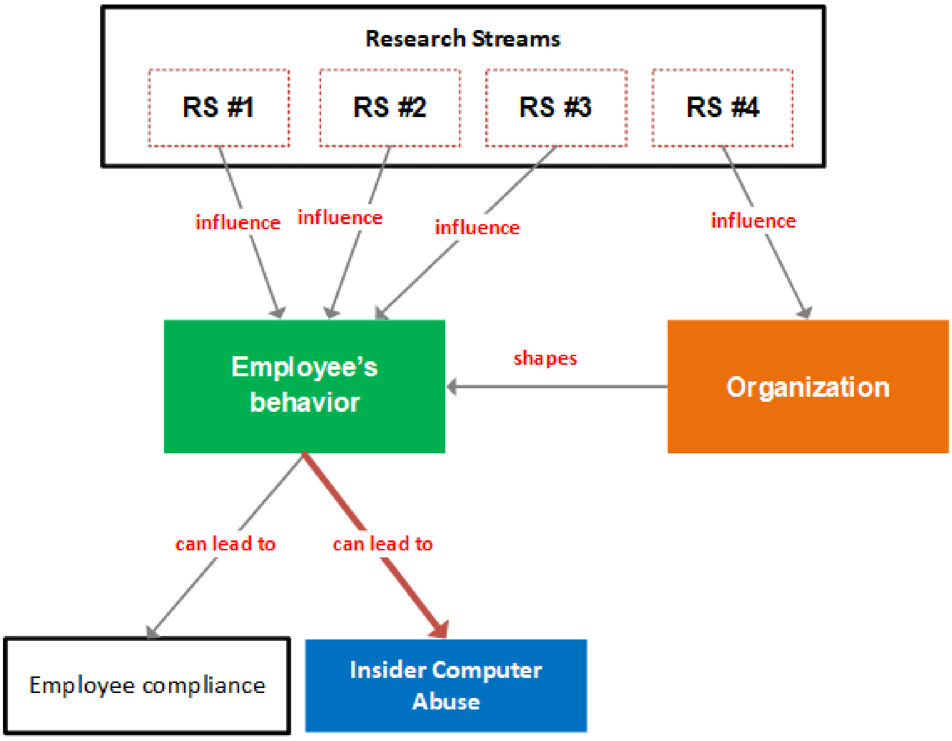


Figure 1. Four research streams we propose to study

1.2 Current state of personal research

We undertook some preliminary research to better scope and understand the employee compliance with IT security policies. Supported by the **GFF Basic funding in 2014, GFF Project funding in 2015** and recently by **SNSF Project grant in 2017** we were able to get some first insights about employee's compliance with IT security policies within the Shadow IT (systems used by employees without explicit organizational IT approval) context and contextual events that precede employee's non-compliant behavior.

These previous phases enabled us to build strong foundations for this larger study by setting out the research gaps that remain in our understanding of the insider computer abuse and confirming the importance of studying the topic of employee compliance with IT security policy.

On top of the below published research, we have recently **received acceptance** for two majors works in the **A and B ranked journals** and we are in the **3rd revision in a B journal** in that provided us much more advanced insights and theoretical justifications about how to further leverage and position employee-organizational IT security compliance vs motivation/engagement dimensions:

- Silic, M., & Lowry, P. B. (2019). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. **Journal of Management Information Systems (JMIS) (accepted 01-Aug-2019).**
- Silic, M. (2018) Breaking Bad: Understanding Black Hat Hacker's Nerve Management. **2nd revision** at **Information Systems Frontiers ISF (accepted 27-Aug-2019).**
- Silic, M. (2018), Marzi, G; Caputo, A and Bal, M. Gamification of the HRM system: the impact on work engagement through job satisfaction and motivation. **3rd revision** at **Human Resource Management journal** (A journal)

Firstly, to better understand the role of organizational/individual inertia and neutralization and deterrence theories in predicting and explaining the employee insider threat through Shadow IT usage we published 4 journal papers:

- Sillic, Mario. "Improving warning messages adherence: can Maya Security Bot advisor help?." **Security Journal** (2019): 1-18.
- Silic, M. Critical Impact of Organizational and Individual Inertia in Explaining Non-Compliant Security Behavior in the Shadow IT context. **Computers & Security**, 80, (2018), 108-119.
- Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage**. Information & Management**, 54(8), 1023-1037
- Silic, M and Back, A. Shadow IT–A view from behind the curtain. **Computers & Security**, 45, (2014), 274-283.

Secondly, we wanted to get some first insights about the phishing risks within the organizational boundaries. We published 1 journal paper:

- Silic, M and Back, A. The dark side of social networking sites: Understanding phishing risks. **Computers in Human Behavior**, 60, (2016), 35-43.

Thirdly, to understand the complex interplay between color and user's decision-making processes we published 1 conference paper:

- Silic, M; Njavro, M; and Oblakovic, G. (2017) Understanding Color Risk Appropriateness: Influence of Color on a User's Decision to Comply with the IT Security Policy—Evidence from the US and India. Presented at **International Conference on HCI in Business, Government, and Organizations**, pp. 412-423.

Fourthly, we wanted to expound more and get some preliminary insights about the unique employee-warning messages context. Hence, we published 2 research studies:

- Silic, M; and Back, A. (2017) Deterrent Effects of Warnings on User's Behavior in Preventing Malicious Software Use. Proceedings of the 50th Hawaii International Conference on System Sciences - **HICSS**.
- Silic, M; Cyr, D; Back, A; and Holzer, A. (2017) Effects of Color Appeal, Perceived Risk and Culture on User's Decision in Presence of Warning Banner Message. Proceedings of the 50th Hawaii International Conference on System Sciences – **HICSS.**

<u>Finally</u>, we wanted to understand how gamification can impact work engagement on a broader level. We published 1 study:

- Silic, M; and Back, A. (2017) Impact of Gamification on User's Knowledge-Sharing Practices: Relationships between Work Motivation, Performance Expectancy and Work Engagement. Proceedings of the 50th Hawaii International Conference on System Sciences - **HICSS**

Overall, the above research provided some initial insights about the employee compliance in the unique organizational context and as such, they are very useful in providing further research gaps and justifications for the research streams proposed in this research plan.

1.3 Detailed Research Plan

Overall, for the four research streams our objective is to produce and publish at least 15 research papers (see Appendix A. for tentative list of publications) targeting high ranked journals within the period of 3 to 5 years.

Theoretical support

Through our previous grants we have already gathered some initial theoretical insights that we expand in this project. In particular, we have identified flow theory, signal detection theory, C-HIP Model, social facilitation theory, cognitive-affective model of communication (CAMC), reversal theory and color theory that provide solid theoretical foundations for the initial research investigations we intend to further develop. In addition to these theories, we will also use theory of organizational and individual inertia, status quo framework and various others cultural, motivational and psychological theories that we intend to use in the unique user-decision making context (e.g., warning context).

Collaboration with other researchers

One of the important aspects of this research plan is the planned collaboration with other renowned researchers that will not only help in improving the quality of our publication outcomes but should also bring the multi-disciplinary collaborations (e.g., from psychology) through the international dimension to the research project.

Since 2017, we started collaboration with several renowned scholars, such as ***<u>prof. dr. Paul Benjamin Lowry</u>*** who in 2018 was ranked the 1st most productive IS scholar in the world for publishing in the top-6 journals, or with ***<u>prof. dr. Dianne Cyr</u>***, who will facilitate and guide the website cultural design. All these and future collaborations should enable us to improve the quality of our research outcomes and should provide positive outlook about our future research contributions as they have recently leveraged our scientific outcomes enabling us to produce work that is currently in second or third revision at top A/A+ journals such as *MIS Quarterly, Journal of Management Information Systems JMIS or Human Resource Management Journal*.

Data collection

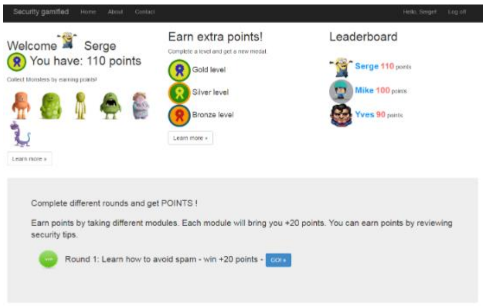
Access to data was identified as one of the key challenges when investigating the insider computer abuse, explained by the fact that organizations are not very willing to participate and provide access to researchers to investigate the phenomenon (Crossler et al., 2013; Mahmood, Siponen, Straub, Rao, & Raghu, 2010; Vance, Lowry, & Eggett, 2015). Our aim is to collect data based on employee intentions and the actual user behaviors. In order to achieve this objective, we have secured the following data sources:

- **Google Chrome/Chromium/Mozilla Firefox**: we entered in collaboration with Google Chrome, Chromium project and Mozilla Firefox developers who agreed to implement some of our research questions into the Beta version of the web browsers which would then be distributed to the test channels where users' behavior would be tracked – we believe this represents a very valuable data source as it can provide insights from an interesting channel (web). Indeed, employees by ignoring digital warnings displayed by a web browser (Chrome or any other browser), install malicious software that can bring important risks to organizational assets.

- **Companies/Organizations**: Nine organizations (3x large US international corporations, 1x large French multinational company, 1x medium size national banking institution, and 4 universities (3 US based and 1 UK) have agreed to take part in the data collection process.

- **.Net web application**: We have developed a web application (hosted at Amazon AWS) which enables us to conduct series of tests regarding security warning experiments (e.g., color). The application will allow us conducting various field and lab experiments and can provide rich datasets on actual employees' behaviors that we measure through different tools and techniques.

- **Security Gamified platform:** We have developed for this research plan an advanced online gamified platform to conduct various IT compliance training related studies which should enable us to gather rich data on employee's actual security compliance behaviors.



Welcome Serge
You have: 110 points
Collect Monsters by earning points!

Earn extra points!
Complete a level and get a new medal.
Gold level
Silver level
Bronze level

Leaderboard
Serge 110 points
Mike 100 points
Yves 90 points

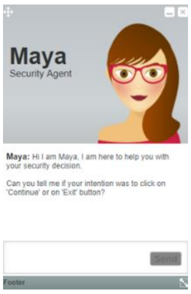
Complete different rounds and get POINTS !

Earn points by taking different modules. Each module will bring you +20 points. You can earn points by reviewing security tips.

Round 1: Learn how to avoid spam - win +20 points -

Figure 2. Security gamified platform we created for this research plan

- **Security Bot:** As part of this research plan, we implemented security chat bot by using SIML (Synthetic Intelligence Markup Language). The chat bot software provides a conversational feature during the interaction with the user and will enable us to test different theoretical insights when it comes to user-decision making choices.



Maya: Hi I am Maya, I am here to help you with your security decision.

Can you tell me if your intention was to click on 'Continue' or on 'Exit' button?

Figure 3. Security bot

Conceptual Framework

Our proposed conceptual framework (Figure 4) provides the high-level view of the approach we intend to follow from: our 4 research streams will be based on the 5 data collection sources with the objective to address 4 overarching research questions and ultimately produce at least 15 research papers within the period of 5 years.

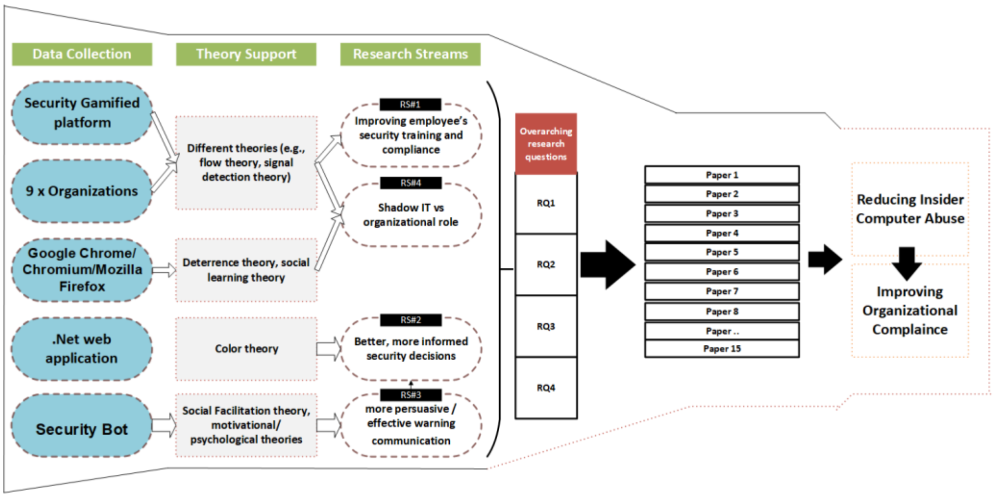

Data Collection
Theory Support
Research Streams
Security Gamified platform
9 x Organizations
Google Chrome/ Chromium/Mozilla Firefox
.Net web application
Security Bot
Different theories (e.g., flow theory, signal detection theory)
Deterrence theory, social learning theory
Color theory
Social Facilitation theory, motivational/ psychological theories
RS#1
Improving employee's security training and compliance
RS#4
Shadow IT vs organizational role
RS#2
Better, more informed security decisions
RS#3
more persuasive / effective warning communication
Overarching research questions
RQ1
RQ2
RQ3
RQ4
Paper 1
Paper 2
Paper 3
Paper 4
Paper 5
Paper 6
Paper 7
Paper 8
Paper ..
Paper 15
Reducing Insider Computer Abuse
Improving Organizational Complaince

Figure4. Proposed Conceptual Framework

Model analysis

We will use a mixed-methods approach combined with various techniques to answer our four overarching research questions. Further, we aim to design and conduct a series of field and lab experiments that we will analyze with **different event history analysis techniques** such as the statistical survival techniques - **Kaplan-Meier Survival estimator** (Kaplan & Meier, 1958). Overall, we will be using survival methods (e.g. Life Table, Cox regression, etc.) to evaluate our research questions. **The survival methods** are widely used in medical research and **our study will be one of the rare ones applying them in the Information Systems (IS) research** discipline to understand user's behaviors throughout the time. Further, we will also use structural equation modeling **(SEM)** techniques such as confirmatory factor analysis (CFA) or path analysis to test our theoretical and conceptual model.

1.4 Schedule and milestones

Our objective is to publish our work in high-ranked journal. In Table 1. different generic phases are described and in Appendix A1 we propose a tentative list of publications and journals/conferences where we aim to submit our work (e.g. Management Information Systems Quarterly (MISQ), European Journal of Information Systems, Computers & Security, Computers in Human Behavior, etc.).

Phases	Apr-20	Jul-20	Dec-20	Jun-21	Sep-22	Jun-22	Mar-23	Jun-23	Sep-23	Dec-23	Feb-24	Apr-24	
Research outline	🟩												5 years
Refine Theory	🟩	🟩	🟩										
Pretest with experts		🟩	🟩										
Pretests / Data validation			🟩										
Data collection launch			🟩	🟩	🟩	🟩							
Data analysis						🟩	🟩	🟩					
Writing of the papers						🟩	🟩	🟩	🟩	🟩			
Internal reviews									🟩	🟩			
Paper revision(s)							🟩	🟩	🟩	🟩	🟩		
Paper Submissions							🟩	🟩	🟩	🟩	🟩	🟩	

Table 1. Timetable for the research work

1.5 Relevance and impact

Despite the increasing relevance of the employee compliance behavior phenomenon, serious research gaps remain in our understanding of how the non-compliant deviant acts can be better mitigated and managed. The importance of studying the employee compliance was highlighted both by academia and practitioners. Several recent practitioner surveys highlighted the role of employee compliance in combatting cybercrime where it is estimated that the annual cost to the global economy from cybercrime is more than $400 billion (KPMG, 2017; McAffee, 2018; PwC, 2018; Young, 2018). Also, several IS security scholars pointed out that the body of work related to employee compliance is still relatively modest and has not matured as other IS disciplines have (Crossler et al., 2013; Mahmood et al., 2010; Moody, Siponen, & Pahnila, 2018; Safa, Von Solms, & Furnell, 2016; Siponen & Vance, 2014; Willison & Warkentin, 2013).

With our study we aim to advance the current understanding of employee's security compliance from the theoretical and practical standpoints by publishing our work in high-ranking international journals. Our study is **the continuation of the previous preparatory phases** (GFF project funding supported by the University of St Gallen) and the SNSF project during which we acquired in depth theoretical understanding of the employee compliance topic (e.g., about the contextual events that precede insider computer abuse).

Theoretical contributions

Our research offers several significant and novel contributions to the Information Systems security literature.

Firstly, we believe that our findings can help recast extant research and practices that should lead to potentially more effective approach to encouraging employees' security compliance. That is, we believe that our research can potentially offer a novel approach on how to better motivate employees to behave in a more compliant way.

Secondly, in the existing IS security literature, the theoretical relationship between the gamification of "serious" systems and the way to encourage employees' security compliance and employee's motivation to be compliant, to the best of our knowledge, was not yet adequately addressed. We aim to fill this gap by explaining this relationship in depth by providing novel insights supported by different theories (e.g., flow theory, signal detection theory, etc.), where we suggest that motivating actual behavioral changes in employees, rather than mere intentions, can be accomplished by appealing to strong intrinsic motivations through "gamified" systems. We argue that employees who are intrinsically motivated may be more persuaded to behave securely.

Thirdly, we aim at explaining which factors can influence and help in taking better and more informed security decisions. That is, we believe that different contextual factors such as color or having an alternative course of action (e.g., security bot) can play an important role in driving better security decisions. Notably, the consequences of better understanding of these contextual factors could positively impact the way information systems are designed and can potentially offer a new way to rethink how security decision should be presented to the employees (e.g., passing from static continue/exit action to a more dynamic security decision mode).

Fourthly, theory-driven factors will be derived to propose a model that would lead to reducing individual computer abuse and increasing compliance by revealing factors that drive a more persuasive and effective warning communication in the unique cultural context. We believe that cultural aspects were largely unexplored thus far and further investigations will provide theoretical justifications about the relationship between culture and security compliance decision.

Fifthly, we will propose a new theoretical model that will explain the role of organization in driving employee's security compliance. We intend to investigate the role of organizational but also individual inertia in shaping employee's security culture.

Finally, we believe that our work could be well received by the IS community and could be consequently, well cited because several prominent IS security scholars (e.g.Crossler et al., 2013; Mahmood et al., 2010; Moody et al., 2018; Siponen & Vance, 2014; Willison & Warkentin, 2013) have **highlighted** not only **the importance of the topic** under study, but also the value of investigating the phenomenon from the **"black-hat" perspective** (i.e. getting access to organizational data on non-compliant employees behaviors where organizations are usually not very open to divulge the sensitive information).

Practical implications

Our research proposal offers several important implications for practitioners. Clearly, one of the challenges that practitioners have to cope with is why employees are not more compliant or why repeatedly, they continue to commit illegal activities. Our research will not only offer the theoretical answers to these questions, but can be used by practitioners to implement clearer, more robust and more efficient deterrent controls and safeguards but also more intrinsically motivated systems where employees could be better trained to take a more informed security decision. For companies like Google (with which we intend to collaborate), Microsoft (Internet Explorer) or Mozilla Foundation (Firefox web browser) our research can have important implications as we intend to suggest how Web browser could better communicate digital warning messages to users in order to achieve better end user (e.g. against malware) protection. Also, if our findings hold, we aim at offering a novel way of introducing a more dynamic security decision making environment (e.g., security bot) in which employee would not be left alone anymore in his/her security decision making situations. Other industries (e.g. the banking sector) can have valuable and practical insights on why employees turn to

IS security policy violations at first place, and how they can be motivated not to enter into the abuse cycle at all.

Further, our study can have important implications to designers of information systems as our findings may suggest that different contextual and cultural elements should be taken into consideration when building the security system. For example, it could be that color black will be more efficient in certain cultures when compared to red. Overall, by better adapting security mechanisms to the unique cultural traits could lead to a more efficient security system that would be adapted to the cultural needs.

Our study will also contribute to a better understanding of what organization might be doing wrongly in their security approach. That is, it could be that organizational inertia is also causing the employee's insecure behavior and does not help in motivating employee to behave more securely. Maybe adapting organizational policies and procedures (e.g., Shadow IT) could create a better security environment for employees and would motivate them more to avoid performing potentially insecure IT behavior.

Purpose of the project for personal postdoctoral work and for personal scientific career

With this project we aim to make a significant contribution to the IS security field by advancing new theoretical insights related to employee compliance with IT security policies.

In particular, this project represents an ideal way to move forward to the goal of taking my scientific contributions to a new level, as well as enabling me to enter into the "Cybersecurity" research community which should 1) positively impact my research outcomes and 2) be highly beneficial to practitioners and my personal scientific career as result of this research plan.

Overall, this project should largely enable me to get the full professorship position and continue my academic path.

Ultimately, with this research project the objective is to make **society and economy a safer place in the challenging Cybersecurity context by working with renowned researchers, industry partners and organizations on proposing novel ways to improve employee's security decisions.**

References

References

Akhawe, D., & Felt, A. P. (2013). Alice in Warningland: A large-scale field study of browser security warning effectiveness. *Proceedings of the 22nd USENIX Conference on Security*: USENIX Association.

Anderson, B., Vance, T., Kirwan, B., Eargle, D., & Howard, S. (2014). Users Aren't (Necessarily) Lazy: Using NeuroIS to Explain Habituation to Security Warnings.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & security, 39*, 145-159.

Behrens, S. (2009). Shadow systems: The good, the bad and the ugly. *Communications of the ACM, 52*(2), 124-129.

Behrens, S., & Sedera, W. (2004). *Why do shadow systems exist after an ERP implementation? Lessons from a case study.* Paper presented at the 8th Pacific Asia Conference on Information Systems, Shanghai, China.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly, 39*(4), 837-864.

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

Burns, A., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2015). *Assessing the Role of Security Education, Training, and Awareness on Insiders' Security-Related Behavior: An Expectancy Theory Approach.* Paper presented at the 2015 48th Hawaii International Conference on System Sciences (HICSS).

Clardy, A. (2005). Reputation, goodwill, and loss: entering the employee training audit equation. *Human Resource Development Review, 4*(3), 279-304.

Crossler, R. E., & Bélanger, F. (2009). The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage. *Journal of Information System Security, 5*(3).

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643-658.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. doi:10.1016/j.cose.2009.09.002

Elliot, A. J., & Maier, M. A. (2014). Color psychology: Effects of perceiving color on psychological functioning in humans. *Annual Review of Psychology, 65*(January), 95-120.

Genschow, O., Reutner, L., & Wänke, M. (2012). The color red reduces snack food and soft drink intake. *Appetite, 58*(2), 699-702.

Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the Shadows: IT Governance Approaches to User-Driven Innovation. *ECIS*, 222.

Harley, B., Wright, C., Hall, R., & Dery, K. (2006). Management Reactions to Technological Change The Example of Enterprise Resource Planning. *The Journal of Applied Behavioral Science, 42*(1), 58-75.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6

Hsu, J. S., Shih, S., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282-300.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

Hughey, A. W., & Mussnug, K. J. (1997). Designing effective employee training programmes. *Training for Quality, 5*(2), 52-57.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly, 34*(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS quarterly, 39*(1), 113-134.

Kaplan, E. L., & Meier, P. (1958). Nonparametric estimation from incomplete observations. *Journal of the American statistical association, 53*(282), 457-481.

Kaspersky. (2015). The greatest heist of the century: hackers stole $1 bln. Retrieved from https://www.kaspersky.com/blog/billion-dollar-apt-carbanak/7519/

Kaya, N., & Epps, H. H. (2004). Relationship between Color and Emotion: A Study of College Students. *College Student Journal, 38*(3), 396.

Kliger, D., & Gilad, D. (2012). Red light, green light: Color priming in financial decisions. *The Journal of Socio-Economics, 41*(5), 738-745.

KPMG. (2017). *Cybercrime survey report 2017*. Retrieved from https://home.kpmg.com/in/en/home/insights/2017/12/cybercrime-cybersecurity-law-enforcement-agencies.html

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information systems journal, 25*(5), 433-463.

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information systems journal, 25*(3), 193-230.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS quarterly, 34*(3), 431-433.

Martocchio, J. J., & Judge, T. A. (1997). Relationship between conscientiousness and learning in employee training: mediating influences of self-deception and self-efficacy. *Journal of Applied Psychology, 82*(5), 764.

McAffee. (2018). *Economic Impact of Cybercrime - No Slowing Down*. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS quarterly, 42*(1).

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS quarterly, 37*(4), 1189-1210.

Poulston, J. (2008). Hospitality workplace problems and poor training: a close relationship. *International Journal of Contemporary Hospitality Management, 20*(4), 412-427.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly, 34*(4), 757-778.

PwC. (2018). *The Global State of Information Security® Survey 2018*. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Shavit, T., Rosenboim, M., & Cohen, C. (2013). Does the color of feedback affect investment decisions? *International Journal of Applied Behavioral Economics, 2*(3), 15-26.

Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. *Computers & Security, 45*, 274-283.

Silic, M., Barlow, J., & Ormond, D. (2015). *Warning! A Comprehensive Model of the Effects of Digital Information Security Warning Messages*. Paper presented at the The 2015 Dewald Roode Workshop on Information Systems Security Research, IFIP, Dewald

Silic, M., Silic, D., & Oblakovic, G. (2016). Influence of Shadow IT on Innovation in Organizations. *Complex Systems Informatics and Modeling Quarterly CSIMQ*(8), 68-80.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management, 51*(2), 217-224.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems, 23*(3), 289-305.

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., & Cranor, L. F. (2009). *Crying Wolf: An Empirical Study of SSL Warning Effectiveness.* Paper presented at the USENIX Security Symposium.

Valdez, P., & Mehrabian, A. (1994). Effects of color on emotions. *Journal of Experimental Psychology: General, 123*(4), 394.

Vance, A., Lowry, P. B., & Eggett, D. L. (2015). Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations. *MIS Quarterly, Forthcoming*.

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC), 24*(1), 21-41.

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. *Journal of the Association for Information Systems, 17*(3), 194-215.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM, 46*(8), 91-95.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS quarterly, 37*(1), 1-20.

Wombat-Security. (2018). 2018 State of the Phish. Retrieved from https://www.wombatsecurity.com/state-of-the-phish

Yang, C.-G., & Lee, H.-J. (2015). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers, 18*(2), 253-263.

Young, E. (2018). *Cybersecurity regained: preparing to face cyber attacks - 20th Global Information Security Survey 2017–18*. Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf