Shadow IT Behavior of Financial Executives in Germany and Italy as an Antecedent to Internal Data Security Breaches

Nicola Castellano
Universita di Pisa
nicola.castellano@unipi.it

Carsten Felden
Technische Universität Freiberg
carsten.felden@bwl.tu-freiberg.de

Robert Pinsker
Florida Atlantic University
rpinsker@fau.edu

Abstract

Data security breaches have been consistently identified in literature as significant, negative events. While most of the related research focuses on externally initiated breaches, far fewer studies provide clarity related to internally initiated breaches. The risk of internal breaches may be dramatically increased by shadow information technology (IT). Our study examines German and Italian financial executives' decisions to engage in shadow IT in combination with two potential mitigation techniques (severity of sanctions in violation of IT policy and outcome effect related to breach risk). While Italian executives act as predicted, German executives engage in a different decision-making process whereby a self-service business culture brought on by perceived increased IT capabilities supersedes the level of cybersecurity awareness and a strong IT usage policy. Results also suggest an outcome effect favoring increased likelihood of breaches may lessen the likelihood of shadow IT usage. Our study adds an international component to existing data security breach and shadow IT research, while also contributing to the IT usage policy, neutralization theory, dynamic capabilities, outcome effect, and self-service literatures.

1. Introduction

Intensive data analysis combined with hybrid (i.e., working in the office or at home during the week) or remote work arrangements, have led to an individualization of data processing [1]. Omnipresent in these work environments is the concept of self-service business analytics (henceforth, self-service), which enables data users to implement their own information technology (IT) channels to be able to solve business problems. If these IT channels are not known/accepted/supported by the centralized IT department, then the channels represent "shadow IT" [2, 3]. Shadow IT is any software, hardware, or IT service processes that are used and/or developed autonomously by user employees or their departments without including the company's own IT department [4]. While there is some anecdotal evidence of positive outcomes related to shadow IT use (e.g., increased task efficiency) [5], the negative consequences are not as clear. We argue that using shadow IT channels to complete daily tasks creates a potentially costly scenario where a financial executive (e.g., the Chief Financial Officer [CFO]) may be unaware of or unconcerned with the associated IT risk [6]. Specifically, we examine financial executives' decisions to use shadow IT, which could lead to data security breaches (DSBs).

The World Economic Forum estimates that $5.2 trillion is at risk of DSBs [7]. Further, Kaspersky Lab notes that approximately 90% of breaches occur from social engineering techniques (i.e., phishing attacks) [8]. Clarity on insider breach antecedents is scarce in the extant academic research [9], but recent anecdotal sources are starting to point the finger at shadow IT messaging channels [3]. Thus, the purpose of our study is to examine German and Italian financial executives' shadow IT decisions as a potential cause of internal of DSBs.[1] Our areas of exploration include the executive's level of cybersecurity awareness (CSA) and two shadow IT mitigation techniques (IT usage policy and breach outcome effect).

Investigating a sample of 229 experienced executives, we consistently find a significant country x CSA interaction. Specifically, high CSA German executives are more likely to engage in shadow IT behavior than those with a low level of CSA and relative to their Italian peers. This result provides evidence of the self-service behavior and dynamic IT

[1] Germany and Italy represent two symbolic archetypes of Northern and Southern European cultures, respectively (Del Junco and Brás-dos-Santos 2009). We examine financial executives, because of their high level of involvement in information systems use (e.g., end-user computing research; Leon et al. 2010).

URI: https://hdl.handle.net/10125/80105
978-0-9981331-5-7

capabilities guiding German executive behavior over-and-above cyber risk knowledge. Similarly, we also consistently find evidence that German financial executives are more likely to engage in shadow IT behavior than Italian financial executives and increasing the salience of DSB risk significantly reduced the likelihood of both countries' executives' shadow IT behavior. We do not find any evidence that CSA or a strong IT usage policy deters shadow IT behavior. Overall, our study's results suggest differences between the executives' shadow IT behavior exist more at an individual business environment/firm level than at a country/cultural level.

Our findings add theory-based and practice-based contributions to multiple Information Systems (IS) literatures: all of which takes place in US settings. The findings also add to our understanding of outcome effects in the DSB literature, which primarily focuses on external DSBs/hacks [9, 10]. Our findings suggest a firm environment-effect to shadow IT behavior and by extension, internal cyber policies and risk. Adding considerations related to a self-service work environment and the theory of dynamic capabilities put specific conditions on when increasing employee CSA would be effective as a preventive firm control against DSBs. Our study proceeds as follows. The next section provides a literature review of shadow IT research. Then, we consider CSA with self-service and dynamic capabilities to determine potential reasons for country-level differences and follow with associated mitigation strategies. Our research method is next presented, followed by the results and study conclusions.

2. Literature Review and Hypothesis Development

2.1. Shadow IT

In principle, shadow IT serves to support business processes, more precisely, the process activities of the users. For the IT department, shadow IT represents a form of loss of transparency and control. Shadow IT includes solutions that are uncontrolled, technically discoverable, and hidden, but completely removed by IT monitoring [11].[2] For example, firms may have several different messaging apps (e.g., WhatsApp) used by employees on an ad-hoc basis either for cost or productivity reasons [3]).

Although shadow IT is not new (two-thirds of IT managers acknowledge shadow IT as an existing phenomenon in their organization) [12] it is growing in size. Perhaps more concerning is approximately 50% of IT managers are concerned about the breakdown of mission critical shadow IT [12]. The main reason for the pervasive nature of shadow IT is that tech-savvy, financial executives implement IT autonomously [13]. However, the benefits come along with managerial problems. In the case of Software as a Service (SaaS) deployed as shadow IT, studies show that 40% of employees see reliability, security, and access risks [14]. Our focus is on the security aspect of shadow IT. Firms may not realize that shadow IT use, such as through messaging apps or other remote work applications, create vulnerabilities resulting in DSBs [3]. Conversely, Myers et al. [15] contemplate that in some cases, managers might not be willing to adopt shadow IT tools if they feel skeptical about the accuracy of information produced.

More specifically, we argue shadow IT can increase internal DSB risk. The potential productivity gains and increased DSB risk represent a double-edged sword to tech savvy CFOs [16]. Data from CompTIA [17] identify more than 50% of DSBs derived from human error due to a lack of compliance with IT security policies or to a lack of expertise with websites or apps. Ironically, employees do not consider human errors as a major cyber concern [17]. Since most DSB studies focus on hacks and other externally initiated DSBs [9, 10], examining potential antecedents to internal breaches is still evolving.[3] The following sections discuss relevant theory to investigate this issue.

2.2. Cybersecurity Awareness

CSA refers to how much end users know about the cyber security threats their networks face and the risks they introduce [18].[4] Recent research argues that since end users have system access and are therefore a major vulnerability, firms should provide CSA training and education [19]. CSA effectiveness research examines the topic both at the firm and individual levels. At the firm level, both Gordon, Loeb, and Sohail [20] and Berkman et al. [21] examine

[2] Shadow IT should not be seen as end-user computing or user-managed computing. End-user computing represents a process in which the user develops applications in an environment that allows access to computer, data, and support resources (Benson 1983). User managed computing is maintenance by the computer's owner, including additional software installation or configuration (Concordia 2020).

[3] See Richardson, Smith, and Watson (2019) for a comprehensive literature review.

[4] We acknowledge that while DSB risk is an important component of a firm's cyber security practices/policies, it is not the only component.

cyber-related disclosures and find that the market positively perceives this information, although a negative tone in the disclosure is associated with a lower market value.

Our focus is on individual, executive judgment. Goss [22] states that effective information security involves control over both IT and internal personnel with system access. Several behavioral studies discuss consequent employee responses to internal controls attempting to prevent access to systems by unauthorized parties [23, 24]. The main concern in this literature is phishing.[5] Vishwanath, Herath, Chen, Wang, and Rao [25] and Brios, George, and Zmud [26] argue that domain-specific knowledge related to CSA can reduce an employee's susceptibility to being successful phished, although the authors concede that said knowledge must be gained through experience.

Phishing-related research implies that the user unwittingly surrenders sensitive system access information to unauthorized parties. While that can be a serious concern for many firms and lead to DSBs, it is not directly related to shadow IT. A related line of research suggests that CSA is not sufficient on its own to curtail non-compliance of cybersecurity-related policies improving the chances of vulnerabilities and eventually DSBs [27]. We next explore this possibility.

2.3 Self-Service and CSA

Goss [22] argues that firms should understand their employees' intent to comply with cyber-related policies in order to be able to gauge DSB risk. A related stream of research discussed in Vishwanath et al. [27] indicates that some beliefs have an immediate, preconscious impact on judgment [28]. In our context, these beliefs, if strong enough, would supersede CSA by itself. Strong beliefs in task efficiency and expediency are represented in the literature by the concept of "self-service."

Self-service shifts software-supported data analysis away from the prepared solution by an IT department to dynamic execution by the specialist user [29]. A self-service scenario in Germany is typical, for example, in contexts where specialist users develop spreadsheet programs or work with analytics tools: often in conjunction with database management systems. Thus, self-service represents the move away from a centralization of the analysis towards a decentralization of analytical information systems, so that more professional-oriented users with technical skills (e.g., financial executives) can act individually in the organizational context.

If self-service exists as an instantiation of shadow IT, a significant drawback is that there is little thought and effort related to all integration aspects of the IT, including installation. Coordination between executive users and IT takes time. Therefore, if an executive needs to complete a task requiring integration of new IT and/or data sources (web, social media, etc.), that executive must weigh the importance of task expediency relative to IT support.

While a self-service belief is consistent with many German financial executives engaging in analytical tasks, it is largely anecdotal. From a theory-based perspective, self-service is consistent with the dynamic capabilities construct. The development of new capabilities can be understood as an enabler to new business models [30], management approaches [31], business structure [32], or operational procedures in business departments. Dynamic capabilities are defined as the ability to reconfigure a firm's operational capabilities to face current needs [33]. The implementation of self-service analytics, either as an official approach or in the context of shadow IT, is part of an organic shift towards digitized data. Some subjects such as organizational structure and organizational culture are less common in the study of the digital transformation than business processes and business models. Changes in organizational structures, such as flattened hierarchy and the integration of more tele-workers [32], and an agile culture can contribute to more flexible and agile organizations, which might be better suited to face the digital transformation [34]. However, these same changes cause leadership challenges and pressure on the work organization [35] that are often not identified in prior research.

The prior literature on digital transformation suggests maturity models, structured steps approaches, and views linked to the development of dynamic capabilities as ways to manage the changes and accompanying expectations introduced in their firms.[6] For example, firms could benefit from a flexible change model [34] and the development of operational and dynamic capabilities [30]. As the unpredictability related to expedient completion of tasks requiring new IT or using IT in a new (i.e., remote) environment increases, an extension of the concept of dynamic capabilities such as executive improvisational capabilities (relevant in the context of self-service,

[5] Phishing is an email-based deception where an individual camouflages emails to appear as a legitimate request for personal and sensitive information (Bose and Leung 2007).

[6] We recognize the vastness of the digital transformation construct. Our intent is not to test this construct, per se, but rather to link it to motivating self-service, shadow IT behavior of financial executives.

shadow IT behavior), could help firms increase their flexibility when it is not possible to plan a configuration change [33]. New projects and new business model clash with the old business organizations, which can hinder progress or prevent real transformation [36], but hide activities like shadow IT.

In sum, both the anecdotal, self-service literature and theory of dynamic capabilities are linked to the German business environment. The same evidence is not as prevalent in the Italian business environment, despite the digitization of data and consequent usage of data analytic software being a global phenomenon. Given the self-service prevalence in the German business environment, we predict that if task expediency beliefs (i.e., self-service) are perceived as more important than CSA, high CSA German financial executives will be more likely to engage in shadow IT behavior than either their Italian counterparts or low CSA German financial executives (i.e., an interaction between CSA and country).

H1: The level of CSA and country of origin interact such that high CSA, German financial executives are the most likely group to engage in shadow IT behavior.

Now that we have discussed the possibilities why shadow IT behavior occurs, we move on to identify potential methods to mitigate said possibilities.

2.4 IT Usage Policy

Prior research shows that the extent of compliance with an IT policy is the result of a cost-benefit trade off, whereby perceived benefits are counterbalanced by formal sanctions and security risks [37]. The inclination of an executive to engage in Shadow IT behavior may be influenced by diametrically opposed factors. For example, deterrence theory postulates that a stronger IT policy may hinder the likelihood of an individual to engage in deviant behaviors [37]. In particular, severity of sanctions and likelihood of being detected are found significant predictors of individual behaviors [37, 38]. However, the relation between severity of sanctions and IT compliance is far from being unequivocal. Sanction severity may play a counterproductive effect on IT usage policy compliance when individual norms contradict the official IT policy [37]. In this context, high severity sanctions may be perceived as a lack of trust by employees and may consequently weaken their loyalty in contrast with the IT usage policy [39, 40, 41].

The contradiction of a deterrent, firm strategy in favor of personal norms is consistent with neutralization theory [42]. Neutralization theory posits individuals acting against the law, regulation or social norm will adopt a way of reasoning to legitimate themselves and minimize or avoid public blame [43]. Siponen and Vance [44] find that neutralization is a significant predictor of the employees' intentions to act in violation of firm IT security policies. Silic et al. [43] conduct a deeper dive into the topic and find evidence identifying neutralization as a significant predictor of an individual's intention to violate IT policies. Deterrence theory and neutralization theory considered in combination widen the spectrum of research by showing that the effects of deterrence on individual IS security policies compliance depend on the context. Both Li et al. [37] and Shoemaker et al. [45], provide evidence that individual behaviors are driven both by official norms and personal beliefs, but when the two conflict, the latter prevails. In our context, if engaging in shadow IT behavior is unacceptable per a formal IT usage policy, but is acceptable by an individual executive, the executive may engage in shadow IT behavior.

Additionally, when deviant behaviors are generally not stigmatized, the deterrent effect of sanctions could be less powerful [45]. This scenario could be true in a shadow IT context, since IT users may think that the information systems threats are not a dramatic danger for the firm or the cost of the sanction is perceived to be less than the benefit of the task completed expediently and independently. In our shadow IT context, the success of severe sanctions for non-compliance of IT usage policies, as well as the influence of neutralization resulting in personal norms superseding official firm norms is equally possible. Accordingly, we formulate the following hypothesis:

H2: There will be no difference in financial executives' shadow IT behavior for strong and weak IT usage policies.

2.5 Breach Risk, Outcome Effect

Given the uncertainty of effectiveness related to IT usage policies and shadow IT behavior, we now consider a second mitigation technique identified in the prior literature as affecting individual judgment: the outcome effect. The outcome effect refers to decision maker judgments being affected by their outcomes and has most prominently been analyzed in the performance evaluation literature [46]. Specifically, outcomes systematically impact evaluators' judgment of the quality of the decision. Hershey and Baron [19] find that outcomes can inform decisions in certain contexts by defining them as "good" or "bad."

Baron and Hershey [19] find that disclosing the decision process of an individual does not prevent the outcome effect in medical and gambling environments. Brazel, Jackson, Schaefer, and Stewart [47] find that even though consultation with auditor superiors (thereby informing the superiors of the auditors' decision-making process) can improve performance, the outcome effect is not mitigated by the consultation. Tan and Lipe [46] theorize that when the decision maker has significant control over the outcome, then that outcome is useful in assessing the decision maker's performance. The opposite is argued for outcomes with a low level of controllability. Their results were mixed with controllability over the decision only mattering for experienced, business individuals and bad news outcomes. The authors reason experienced, businesspeople engage in a functional decision-making whereby it is the bottom-line judgment that counts most (and positive results are rewarded, while there is no "extra blame" for negative results).

The aggregate literature suggests the outcome effect is prevalent even in experienced, businesspeople and that controllability of decisions matters for experienced individuals in bad news conditions. We extrapolate that consistent finding to a shadow IT environment and predict the following:

H3: When a related DSB risk is known, financial executives are less likely to engage in shadow IT behavior.

3. Method

3.1 Sample

Italian data was collected through an online questionnaire administered through Google Form. Respondents received an email invitation to contribute to the survey with a link that allowed them to access the questionnaire (every version had its own link). The Italian emails were sent to the Executive MBA in Auditing and Management Control alumni database from a large Italian university. The database included approximately 1,150 records randomly divided into four groups; every participant received invitation for only one version of the questionnaire. 134 responses were received for a response rate of 11.7%. Nine respondents were eliminated for having an incomplete questionnaire resulting in a final sample of 125. Respondents were solicited until almost an equal number of observations for all the four versions of the questionnaire were collected. The participants reside throughout Italy and currently work as senior financial executives (e.g., CFO) of large firms (defined as having more than 250 employees; European Union 2015).

A similar data collection process was used for the German participants. The invitation to participate the survey and the link to access the questionnaire was sent to German financial executive members of The Data Warehouse Institute (TDWI) Europe. 104 financial executives were solicited and responded for a 100% response rate.

Sample demographics are depicted in Table 1. 59.2% of the Italian sample are female compared to 35.6% of the German sample. All participants have at least a Bachelor's degree with 80% of Italians and 58.7% of Germans earning Master's degrees. The average age of participants was over 40 for both groups. Further, the executives in our sample were very experienced with both groups having an average of over 15 years of work experience, with approximately 10 years of experience with their current employer. Table 1 also shows that there is a wide variety in the number of times the executives installed software either at home or work and the executives had relatively low levels of self-reported coding experience. In aggregate, our sample comprised educated, experienced financial executives with at least some coding and software installation knowledge.

Table 1. Sample Demographics

Country	Germany	Italy
Sample size	104	125
Females	37 (35.6%)	74 (59.2%)
Education level:		
Bachelors	24 (23.1%)	22 (17.6%)
Master's	61 (58.7%)	100 (80.0%)
Doctorate	19 (18.2%)	3 (2.4%)
Average (SD) Age	43.87 (9.88)	40.78 (11.18)
Average Years (SD) Work Experience	17.74 (9.98)	15.55 (11.70)
Average (SD) Times Installing at Work	7.88 (12.15)	8.62 (14.74)
Average (SD) Times Installing at Home	15.85 (17.10)	17.73 (20.15)
Experience with Coding Languages (SD)	3.47 (2.17)	2.20 (1.69)
Years Worked for Current Employer (SD)	9.70 (7.55)	10.79 (10.90)

3.2 Research Design

After providing a welcome statement and consent to participate information, the instrument included background information on a fictional company called CBR – a multinational company with 1500 employees headquartered "in the participant's country" with operations in Germany, Italy, and the US. Participants were told additional information related to no turnover in the chief executive officer position; 6% earnings growth in past four years; CBR being highly entrepreneurial, encouraging innovation solutions to problems; a centralized IT department; and a usage policy statement requiring employees to only use IT that are approved by the IT department. After the background information, the experiment placed participants in the finance-area of CBR where most work is done in Excel. At that point, the case scenario states the following:

A software vendor has recently introduced you to a new business intelligence/analytics tool ("the tool," henceforth) which could be used to work at a faster pace. Relative to Excel, the tool is easy to use, reduces the amount of manual tasks (and data quality errors), and can be used/shared on mobile devices. However, CBR's IT department said that the new tool would take several weeks to purchase and then fully implement. If you purchase and implement the tool yourself, it would take approximately half of a day. The tool requires a greater level of access rights to sensitive CBR data than is currently granted. The IT department typically grants increased data access rights upon request from personnel in your department.

The instrument prompts the participants to respond to the dependent variable question (see below), before moving on to the IT usage policy and DSB outcome effect manipulations (where they see the same question again after each manipulation), demographic questions, and cyber awareness and culture variable scales. Participants were randomized into IT usage policy and DSB outcome conditions.

3.3 Dependent Variables

We proxy shadow IT behavior as the likelihood the executive would install a new tool on their work computer (implying that the executive would not wait for IT to conduct the installation).[7] Specifically, the question states, "On a scale of 0 to 10 (where 0 = you would not install the tool; 5 = you are not sure; and 10 = you would definitely install the tool), please indicate the likelihood that you would install the new tool yourself on your work computer." Our dependent variables represent an initial judgment (IJ), a revised judgment (RJ; after the IT usage policy manipulation), and a final judgment (FJ; after the DSB outcome effect manipulation). Thus, we have a repeated measures design where we measure the scale result each time, but also measure the magnitude of belief revision (i.e., RJ-IJ and FJ-RJ) to glean any possible additional insights.[8]

3.4 Independent Variables and Covariates

Our mixed design includes a 2x2 of manipulated variables (strength of IT usage policy [henceforth, USAGE] and DSB outcome effects [henceforth, OUTCOME]) and two measured variables (CSA, and country of current residence). The USAGE manipulation is adapted from Shoemaker et al. [45] and Malimage et al. [48] whereby the strong condition states warnings are given if the policy is violated and three warnings can result in termination. The weak manipulation states that the violator meets with the head of the department, but no official warnings are given. The OUTCOME manipulation is derived from anecdotal and academic research cited in Tan and Yu [49] and Kelton and Pennington [50]. Specifically, the manipulation involves a statement that either says "many data breaches…" (strong) or "no data breaches…" (weak) have resulted from others downloading the same analytics tool that is being offered to the participants.

Our CSA measure is adapted from Lif et al. [51] and comprises two statements: one about importance of the firm's IT and another regarding how urgent taking action against a cyber-attack would be. The Cronbach's Alpha between these two items was 0.82; therefore, we summed the items into a single measure. The country variable (henceforth, COUNTRY) was measured based on participants' current residence as either Italy or Germany.[9]

Next, all demographics from Table 1 were tested as potential covariates. Only the number of times participants installed software at work (henceforth, TIMES) was significant and included in the upcoming ANCOVA analyses.10 Additionally, we consider macro-level differences in culture as additional covariates, given the German-Italian differences mentioned earlier [52]. Hofstede and Minkov [53] identify six dimensions of a nation's value system/culture. The six dimensions are: power distance (PD); individualism (INDIV); masculinity (MASC); uncertainty avoidance (UA); long-term orientation (L-T); and indulgence (IN). Our review of the literature and untabulated correlation analyses with our DVs identified only PD, IN, and INDIV as appropriate for our context (the other three variables were tested, but nothing was significant). The scale components for all three variables all have Cronbach's

[7] IT department approval of the software tool is also part of this issue, but is included in the upcoming IT usage policy variable discussion.

[8] We also examine FJ-IJ in an untabulated analysis, but do not find any additional/incremental insights.

[9] We substitute country born in and find almost identical results.

[10] We measured participants' motivation using a seven-point scale ranging from 1 (not motivated) to 7 (extremely motivated). German executives were significantly more motivated (mean [SD] = 5.46 [1.39]) than Italian executives (mean [SD] = 4.53 [1.61]; t = 4.63, p < 0.001), but both were significantly above the midpoint (p < 0.001 for both countries), suggesting that participants on average were motivated to do their best on the task.

Alpha's > 0.80 and, thus, were summed into individual variables.[11] We split and analyze CSA and the three culture variables at the median to guard against data skewness affecting our results.[12]

4. Results

4.1 Hypothesis Testing

Recall that H1 predicts an interaction effect between COUNTRY and CSA. Table 2, panel A provides the initial results involving IJ as the dependent variable. Panel B provides the mean values for each CSA and COUNTRY.

Table 2. H1 and H2 Testing (CSA and COUNTRY)

Panel A: ANCOVA Results (n = 229)

Source of Variation	SS	DF	MS	F-Stat	p-value
COUNTRY x CSA	57.99	1	57.99	6.46	0.01
COUNTRY	99.66	1	99.66	11.10	<0.001
CSA	2.98	1	2.98	0.33	0.57
Covariates: IN	26.15	1	26.15	2.91	0.09
TIMES	35.47	1	35.47	3.95	0.05
Model	241.54	7	34.51	3.84	0.001
Intercept	1030.77	1	1030.77	114.81	<0.001

Panel B: Cell Means

Country	High Awareness	Low Awareness	Overall
Germany	6.55 (2.77) n = 53	5.33 (2.88) n = 51	5.95 (2.87) n = 104
Italy	4.32 (3.13) n = 77	5.08 (3.30) n = 48	4.62 (3.20) n = 125
Overall	5.23 (3.27) n = 130	5.21 (3.08) n = 99	

The results support H1 by showing a significant COUNTRY X CSA interaction (F-stat = 6.46, p = 0.01) in the predicted direction (the high CSA group that is more likely with the German executives to download the tool [mean [SD] = 6.55 [2.77]] than the low, German group [mean [SD] = 5.33 [2.88]] or either of the Italian executive groups [high CSA mean [SD] = 4.32 [3.13]], low CSA mean [SD] = 5.08 [3.30]]. This result provides some initial evidence that the German self-service business environment involving dynamic capabilities supersedes the level of CSA. When interpreting all main effects, we find that COUNTRY is significant with the German financial executives more likely to download the tool (overall mean [SD] = 5.95 [2.87]) than are the Italian Financial Executives (overall mean [SD] = 4.62 [3.20]); F-stat = 11.10, p < 0.001). There is a marginally significant result for the IN covariate (F-stat = 2.91, p = 0.09).[13]

IT Usage Policy (H2). Having established shadow IT differences above, we now consider mitigation techniques starting with USAGE (H2). Table 3, panel A provides the ANCOVA results and panel B includes the relevant cell means.

Table 3. H2 Testing (IT Usage Policy)

Panel A: ANCOVA Results (n = 215)

Source of Variation	SS	DF	MS	F-Stat	p-value
COUNTRY x CSA	5.01	1	5.01	0.57	0.45
COUNTRY	56.31	1	56.31	6.43	0.01
CSA	0.06	1	0.06	0.00	0.99
USAGE	11.37	1	11.37	1.30	0.26
Covariates: PD	25.01	1	25.01	2.86	0.09
TIMES	4.75	1	4.75	0.54	0.46
Model	138.09	8	17.26	1.97	0.05
Intercept	2750.86	1	2750.86	314.05	<0.001

Panel B: Cell Means

Country	High Awareness	Low Awareness	Overall
Germany	4.56 (2.67) n = 50	4.37 (2.67) n = 49	4.46 (2.66) n = 99
Italy	3.33 (3.18) n = 69	3.62 (3.31) n = 47	3.45 (3.22) n = 116
Overall	3.85 (3.03) n = 119	4.00 (3.01) n = 96	

The COUNTRY X CSA interaction term is not significant (F-stat = 0.57, p = 0.45) since the German Financial Executives are more likely to download the tool regardless of CSA level. This result is supported when examining the COUNTRY main effect (German financial executives overall mean [SD] = 4.46 [2.66]; Italian Financial Executives overall mean [SD] = 3.45 [3.22]; F-stat = 6.43, p = 0.01). USAGE is not

[11] For expositional purposes, we only present the significant culture variables (at p < 0.10) in the upcoming analyses. Further, we asked a total of three manipulation check questions (two for USAGE). Results suggest our manipulations were successful as only 12 Italian and six German executives failed at least one check and were removed from the sample.

[12] We conduct a series of additional testing to add credibility to our median split design choice where median value scores are included with the "high" condition. First, we include the median values in the "low" conditions. Second, we eliminate all median values. Third, we eliminate all values within 10 percent of the median. The last two tests were to avoid interpreting results where values were "bunched" at the median. Our inferences do not change when considering all three additional tests.

[13] Throughout hypothesis testing, we interact all three culture variables with COUNTRY, CSA, and eventually each of the manipulations. No significant results are found.

significant (F-stat = 0=1.30, p = 0.26) with PD marginally significant (F-stat = 2.86, p = 0.09). The above results do not specifically show the magnitude of potential of participants' belief revision after having received the USAGE manipulation (i.e., repeated measures).

Thus, we also examine the magnitude of judgment belief revision in untabulated analysis. We find a significant amount of belief revision in the COUNTRY X CSA interaction term (F-stat = 9.12, p < 0.01). The means suggest that it is the high CSA group that is accounting for the significance. Specifically, the high CSA German executives are reducing their likelihood to download the tool (mean [SD] = -2.24 [0.30]) significantly more than the high CSA Italian executives (mean [SD] = -0.86 [0.27]). This difference does not exist in the low CSA conditions (German executives' mean [SD] = -1.00 [0.31], Italian executives' mean [SD] = -1.37 [0.30]). These numbers also help to explain the marginally significant difference between countries overall (German executives' overall CSA mean [SD] = -1,62 [0.30], Italian executives' overall CSA mean [SD] = -1.14 [0.28]; F-stat = 2.97, p = 0.09). In aggregate, we fail to reject H2, but find some stronger support for H1. Even though the strong/weak USAGE manipulation did not differ among conditions, its presence helped to significantly reduce the high CSA German financial executives' likelihood of downloading the new tool.[14]

DSB Outcome Effect (H3). Our last shadow IT mitigation technique considers the potential impact of outcome knowledge (H3). Table 4, panel A provides the ANCOVA results and panel B includes the relevant cell means. We again find a significant COUNTRY X CSA interaction term (F-stat = 4.65, p = 0.03). Examining the means in panel B, we see a reversion back to the IJ results whereby the German executives are much more likely than their Italian counterparts to download the tool at the high CSA level (German executive mean [SD] = 5.68 [2.98], Italian executive mean [SD] = 2.95 [3.31]) and relative to those German executives in the low CSA group (mean [SD] = 4.65 [2.87]). When looking at the other variables of interest, we find consistent evidence of a significant COUNTRY main effect indicating German financial executives are more likely to download the tool (overall mean [SD] = 5.14 [2.93]) than are the Italian Financial Executives (overall mean [SD] = 3.29 [3.25]; F-stat = 21.22, p < 0.01). We also find a highly significant OUTCOME effect (F-stat = 32.33, p < 0.001) in the predicted direction. We do not find statistical significance with USAGE (F-stat = 0=1.61, p = 0.21) but the IN covariate is significant (F-stat = 3.95, p = 0.05).

Table 4. H3 Testing (Outcome Effect)

Panel A: ANCOVA Results (n = 211)

Source of Variation	SS	DF	MS	F-Stat	p-value
COUNTRY x CSA	37.68	1	37.68	4.65	0.03
COUNTRY	171.99	1	171.99	21.22	<0.001
CSA	1.32	1	1.32	0.16	0.69
OUTCOME	262.11	1	262.11	32.33	<0.001
USAGE	13.06	1	13.06	1.61	0.21
IN	32.03	1	32.03	3.95	0.05
INDIV	1.18	1	1.18	0.15	0.70
PD	9.17	1	9.17	1.13	0.29
Covariate: TIMES	16.99	1	16.99	2.10	0.15
Model	575.80	9	57.58	7.10	<0.001
Intercept	3070.07	1	3070.07	378.71	<0.001

Panel B: Cell Means

Country	High Awareness	Low Awareness	Overall
Germany	5.68 (2.98) n = 49	4.65 (2.87) n = 49	5.14 (2.93) n = 98
Italy	2.95 (3.31) n = 67	3.65 (3.13) n = 46	3.29 (3.25) n = 113
Overall	4.02 (3.40) n = 116	4.32 (3.03) n = 95	

Analogous to the H2 testing above, we also examine the magnitude of belief revision in untabulated analysis. We find a marginally significant amount of belief revision in the COUNTRY X CSA interaction term (F-stat = 3.72, p = 0.55). Considering the means, we see that it is the high CSA group that is accounting for the significance. Specifically, the high CSA German executives are reverting back towards their initial judgments by increasing their likelihood to download the tool (mean [SD] = 1.08 [1.95]) and the high CSA Italian executives make a small decrease in their desire to download the tool (mean [SD] = -0.20 [2.23]). This reversion may be recognition on the part of the German executives that they over-revised their earlier judgments when given the USAGE manipulation. The difference is not as pronounced in the low CSA conditions (German executives' mean [SD] = 0.37 [1.43], Italian executives' mean [SD] = 0.02 [1.96]). These numbers also help to explain the significant difference between countries overall (German executives' overall CSA mean [SD] = 0.79

[14] In additional testing, we interacted USAGE with all other independent variables, but do not find any significant results.

[1.72], Italian executives' overall CSA mean [SD] = -0.11 [2.13]).

We conduct additional testing to further elaborate our COUNTRYXCSA results. Specifically, we perform planned contrasts and Bonferroni analyses retesting our hypotheses. Untabulated results support the ANCOVA results reported above. Our aggregate evidence finds strong support for H1 and H3 and fail to reject H2.[15]

5. Conclusion

There is a long history of shadow IT use and end-user computer in employees ranging from entry level staff to top executives. Remote and hybrid working arrangements have significantly accelerated the use of workaround apps executives feel they need to use to be productive [3]. A major concern of firms, then, is that regardless if the IT department knows about the app use, it cannot manage the security profile adequately, risking an internally-caused DSB. According to the World Economic Forum [7], DSB risk is a global issue with $5.2 trillion in potential costs. While the extant DSB literature is predominantly US-based and focused on external hacks [9, 10], international academic research surrounding internal breach causes and mitigation strategies is scarce. Our study attempts to fill this gap in the literature.

First, we find strong evidence that German financial executives with high CSA levels being most likely to engage in shadow IT behavior (and in conjunction, increasing internal DSB risk). This finding is consistent with our IT dynamic capabilities and self-service arguments surrounding this group. Further, one aspect that continuously came up in our post-experiment debriefing was the importance of the business departments' relationship/alignment with the IT department. The Italian executives were consistently reporting more of a willingness to allow the IT department to manage all applications than were the German executives. While we controlled this aspect in our experiment, future research should further investigate this relationship and attempt to find ways to align the departments. Relatedly, future research should more closely examine the impact a self-service perspective and IT dynamic capabilities have on various judgments.

Next, multiple studies tout strong and clear IT usage policies (and employee training on said policies) as a method of encouraging compliance with IT-related behavior at firms, deterring more individualistic, IT-behavior and potentially decreasing DSB risk [54, 48]. Analogously, academic research advocates for increasing employees' CSA, perhaps even tying in the firm's IT usage policy to do so, to improve compliance and mitigate DSB risk [21, 54]. Our results contradict these suggestions, although there is some evidence that a strong IT usage policy revises shadow IT beliefs in the desired direction. While we consistently find differences in intended shadow IT behavior between the financial executives in both countries, we find only inconsistent evidence related to our macro-level, cultural covariates. Therefore, when comparing the relative influence of deterrence and neutralization theories, our findings are more closely tied to the latter theory where an individual's norms (self-service in our context) supersede the firm's norms.

Finally, we find strong evidence suggesting a breach outcome effect impacts shadow IT behavior. Combined with our lack of CSA findings, this result indicates there may be a difference in shadow IT behavior when considering one's trait vs. situational (i.e., state) cyber awareness. Future research should investigate this possibility.

Our study makes important academic and practical contributions. It adds novel insights and context to the shadow IT, international DSB, self-service, dynamic capabilities, IT usage policy/deterrence theory, outcome effect, and neutralization theory literatures. Specifically, results of intentional actions complement those of the anecdotal and phishing literatures showing internal DSBs being caused by human error. Further, our experienced sample of financial executives commonly make critical business decisions and, thus, our study builds on Myers et al.'s [15] shadow IT research involving management decision making. Yet, our results raise new questions that create opportunities for future research. For example, even though the European Union's General Data Protection Regulation (GDPR) was newly in existence during our data collection, and a potentially negative outcome effect was provided, German financial executives (on average) still pursued their own method to secure the necessary IT to complete a task – increasing the risk of an internal DSB. Future research should delve deeper into executives' behavior involving GDPR and how it has changed/not changed internal firm processes related to shadow IT and internal DSB risk.

[15] Additional testing interacts OUTCOME in all possible 2-way and 3-way interactions. No significant results are obtained. The lack of COUNTRY X OUTCOME interaction suggests a consistent pattern for the German Financial Executives relative to their Italian peers. That is, regardless of OUTCOME strength, the German Executives are more likely to download the tool.

Our study is subject to multiple limitations. First, although our participants come from two major European economies representative of northern vs. southern Europe, our results may not be generalizable to financial executives from other countries. Future research should investigate our effects of interest using financial executives from other economies including the US, South America, China, UK, etc. Next, our experimental design captures financial executives' intentions, which is separate from actual behavior. Future research should capture actual, individual behavior. Third, we cannot completely rule out the possibility that our IT usage policy manipulation is not strong enough to elicit a response, despite pilot testing involving two German managers. Finally, our sample and experimental design are exclusive to large firms and their financial executive's behavior. Thus, small and medium-sized firms are not represented.

6. References

[1] A. Abelló, J. Darmont, L. Etcheverry, M. Golfarelli, J. N. Mazón, F. Naumann, T. Pedersen, S. B. Rizzi, J. Trujillo, P. Vassiliadis and G. Vossen, "Fusion cubes: Towards self-service business intelligence," *International Journal of Data Warehousin,* vol. 9, no. 2, pp. 66-88, 2013.

[2] C. Rentrop and S. Zimmermann, "Shadow IT—Management and control of unofficial IT.," in *Proceedings of ICDS 2012, The Sixth International Conference on Digital Society: 98-102.*, 2012.

[3] S. Wood, "The security implications for private messaging apps," TechRadar, 2021. https://www.techradar.com/news/the-security-implications-for-private-messaging-apps. [Accessed 10 06 2021].

[4] A. Kopper and M. Westner, "Towards a taxonomy for shadow IT," in *22nd Americas conference on information systems*, San Diego, 2016.

[5] S. Zimmermann, C. Rentrop and C. Felden, "Governing IT activities in business workgroups: Design principles for a method to control identified Shadow IT," in *International Conference on Business Information Systems: 252-264,* 2016.

[6] S. Zimmermann, C. Rentrop and C. Felden, "Governing identified shadow IT by allocating IT task responsibilities," in *Americas Conference on Information Systems,* San Diego, 2016 .

[7] I. Ghosh, "Visualizing the massive cost of cybercrime," 2019. https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/. [Accessed 27 2 2021].

[8] A. Spadafora, "90 percent of data breaches are caused by human error," 2019. https://www.techradar.com /news/90-percent-of-data-breaches-are-caused-by-human-error. [Accessed 27 2 2021].

[9] J. Higgs, R. Pinsker, T. Smith and G. Young, "The relationship between board-level technology committees and reported security breaches," *Journal of Information Systems,* vol. 30, no. 3, pp. 79-98, 2016.

[10]T. Smith, J. Higgs and R. Pinsker, "Do auditors price breach risk in their audit fees?," *Journal of Information Systems* , vol. 33 , no. 2, pp. 177-204, 2019.

[11]W. Brenner, A. Györy, M. Pirouz and F. Uebernickel, "Bewusster Einsatz von Schatten- IT: Sicherheit & Innovationsförderung. St. Gallen.," 2011.

[12]K. Smyth and J. Freeman, "Blue Prism Rogue IT Survey 2007," *Blue Prism,* 2007.

[13]S. Behrens, "Shadow systems: The good, the bad and the ugly," *Communications of the ACM,* vol. 52, no. 2, pp. 124-129, 2009.

[14]L. Stadtmueller, "The hidden truth behind shadow IT; Six trends impacting your security posture," *50 Years of Growth, Innovation and Leadership, edited by Stratecast and Frost & Sullivan* , pp. 1-13, 2013.

[15]N. Myers, M. W. Starliper, S. L. Summers and D. A. Wood, "The impact of shadow IT systems on perceived information credibility and managerial decision making," *Accounting Horizons* , vol. 31, no. 3, p. 105–123, 2017.

[16]B. Pariseau, "NASA's shadow IT issues with cloud computing all too common," 2013. [Online]. Available: http://searchcloudcomputing.techtarget.com/news/2240203181/NASAs-shadow-IT-issues-with-cloud-computing-all-too-common. [Accessed 2 3 2021].

[17]R. Maurer, "Human error cited as top cause of data breaches," 2015. https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/human-error-top-cause-data-breaches.aspx. [Accessed 26 5 2021].

[18]L. Kim, "Cybersecurity awareness: Protecting data and patients," *Nursing Management* , vol. 48, no. 4 , p. 16–19, 2017.

[19]J. C. Hershey and J. Baron, "Judgment by outcomes: When is it warranted?," *Organizational Behavior and Human Decision Processes,* vol. 62, no. 1, p. 127, 1995.

[20]L. Gordon, M. P. Loeb and T. Sohail, "Market value of voluntary disclosures concerning information security," *Management Information Systems Quarterly,* vol. 34, no. 3, pp. 567-593, 2010.

[21]H. Berkman, J. Jona, G. Lee and N. Soderstrom, "Cybersecurity awareness and market valuations," *Journal of Accounting and Public Policy,* vol. 37, pp. 508-526, 2018.

[22]D. Goss, "Operationalizing cybersecurity – framing efforts to secure U.S. information systems," *The Cyber Defense Review,* pp. 91-110, 2017.

[23]A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Computers & Security 68,* vol. 68, pp. 160-196, 2017.

[24]D. D. Caputo, S. L. Pfleeger, J. D. Freeman and M. Johnson, "Going spear phishing: Exploring embedded training and awareness," *IEEE Security & Privacy,* pp. 28-38, 2014.

[25]A. Vishwanath, T. Herath, R. Chen, J. Wang and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems* , vol. 51, pp. 576-586, 2011.

[26]D. P. Brios, J. F. George and R. W. Zmud, "Inducing sensitivity to deception in order to improve decision making performance: a field study," *Management Information Systems Quarterly* , vol. 26 , p. 119–144, 2002.

[27]A. T. Vishwanath, B. Harrison and Y. Ng, "Suspicion, cognition, and automaticity model of phishing susceptibility," *Communication Research* , vol. 45, no. 8, pp. 1146-1166, 2018.

[28]I. Ajzen, "Nature and operation of attitudes," *Annual Review of Psychology,* vol. 52, pp. 27-58, 2001.

[29]A. G. Naish, "Cloud-based self-service analytics," in *Proceedings of the 59th World Statistics Congress*, 2013.

[30]D. Teece and G. Linden, "Business models, value capture, and the digital enterprise," *Journal of Organization Design* , vol. 6, no. 1, p. 1–14, 2017.

[31]S. Shamim, S. Cang, H. Yu and Y. Li, "Management approaches for Industry 4.0: A human resource management perspective," in *In 2016 IEEE Congress on Evolutionary Computation (CEC). IEEE.*, 2016.

[32]K. Fettig, T. Gacic, A. Koskal, A. Kuhn and F. Stuber, "Impact of Industry 4.0 on Organizational Structures," in *IEEE International Conference on Engineering, Technology, and Innovation (ICE/ITMC)*, 2018.

[33]P. A. Pavlou and O. A. E. Sawy, "The "third hand:" IT-enabled competitive advantage in turbulence through improvisational capabilities," *Information Systems Research*, vol. 21, no. 3, pp. 443-471, 2010.

[34]A. Trübswetter, A. Zettl and S. Glende, "User-Centred Change - Shaping Corporate Transformation with Participatory Design Tools," in *Proceedings of ISPIM Conferences: 1–16*, 2018.

[35]T. Schwarzmüller, P. Brosi, D. Duman and I. M. Welpe, "How Does the Digital Transformation Affect Organizations? Key Themes of Change in Work Design and Leadership," *Management Revue*, vol. 29 , no. 2, pp. 114-138, 2018.

[36]A. Akram, M. Bergquist and M. Åkesson., "Digital Visions vs. Product Practices: Understanding Tensions in Incumbent Manufacturing Firms,," in *47th Hawaii International Conference on System Sciences*, Hawaii, 2014..

[37]H. Li, J. Zhang and R. Sarathy, "Understanding compliance with internet use policy from the perspective of rational choice theory," *Decision Support Systems* , vol. 48, p. 635–645, 2010.

[38]J. D'Arcy, A. Hovav and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* , vol. 20, no. 1, p. 79–98, 2009.

[39]T. G. Chiricos and G. P. Waldo, "Punishment and crime: an examination of some empirical evidence," *Social Problems* , vol. 18, no. 2, pp. 200-2017, 1970.

[40]J. Dubin and L. Wilde, "An empirical analysis of federal income tax auditing and compliance," *National Tax Journal* , vol. 16, no. 1, pp. 61-74, 1988.

[41]N. Piquero, M. L. Exum and S. S. Simpson, "Integrating the desire-for-control and rational choice in a corporate crime context," *Justice Quarterly* , vol. 22, no. 2, pp. 252-280, 2005.

[42]C. F. Curasi, "The relative influences of neutralizing behavior and subcultural values on academic dishonesty," *Journal of Education for Business*, vol. 88 , no. 3, pp. 167-175, 2013.

[43]M. Silic, J. B. Barlow and A. Back, "A new perspective on neutralization and deterrence: Predicting shadow IT usage," *Information & Management*, vol. 54, p. 1023–1037, 2017.

[44]M. Siponen and A. Vance, "Neutralization New insights into the problem of employee systems security policy violations," *Management Information Systems Quarterly* , vol. 34, p. 487–502, 2010.

[45]N. Shoemaker, M. B. Curtis, L. Fayard and M. Kelly, "What Happens When Formal and Informal Norms Conflict for IT Usage?," *Journal of Information Systems*, vol. 34, no. 2, pp. 235-256, 2020.

[46]H.-T. Tan and M. G. Lipe, "Outcome effects: The impact of decision process and outcome controllability," *Journal of Behavioral Decision Making* , vol. 10, pp. 315-325, 1997.

[47]J. F. Brazel, S. B. Jackson, T. J. Schaefer and B. W. Stewart, "The outcome effect and professional skepticism," *The Accounting Review* , vol. 91 , no. 6, pp. 1577-1599, 2016.

[48]K. Malimage, N. Raddatz, B. S. Trinkle, R. E. Crossler and R. Baaske, "Impact of deterrence and inertia on information security policy changes," *Journal of Information Systems*, vol. 34, no. 1, pp. 123-134, 2020.

[49]H.-T. Tan and Y. Yu., "Management's responsibility acceptance, locus of breach, and investors' reactions to internal control reports," *The Accounting Review* , vol. 93, no. 6, pp. 331-355, 2018.

[50]A. S. Kelton and R. R. Pennington, "Do voluntary disclosures mitigate the cybersecurity breach contagion effect?," *Journal of Information Systems* , vol. 34 , no. 3, pp. 133-157, 2020.

[51]P. Lif, M. Granasen and T. Sommestad., "Development and validation of technique to measure cyber situation awareness," in *IEEE International Conference on Cyber Situational Awareness*, London, England, 2017.

[52]J. Del Junco and J. M. Brás-dos-Santos, "How different are the entrepreneurs in the European Union internal market? — An exploratory cross-cultural analysis of German, Italian and Spanish entrepreneurs," *Journal of International Entrepreneurship*, vol. 7, pp. 135-162, 2009.

[53]G. Hofstede and M. Minkov, "Values Survey 2013 Module," 2013. https://geerthofstede.com. [Accessed 1 9 2021].

[54]N. Raddatz, K. Marett and B. S. Trinkle, "The impact of awareness on being monitored on computer usage policy compliance: An agency view.," *Journal of Information Systems, forthcoming.* 2021.