ICIS 2022 Proceedings

IS and the Future of Work

Dec 12th, 12:00 AM

Algorithmic Technologies as Threat to Who We Are: The Effect an IT Identity Threat has on Employees' Work Engagement

Anne-Sophie Mayer
Vrije Universiteit Amsterdam, a.s.mayer@vu.nl

Franz Strich
Chair for Human Resource Management & Intrapreneurship, f.strich@deakin.edu.au

Marina Fiedler
University of Passau, marina.fiedler@uni-passau.de

Recommended Citation

Mayer, Anne-Sophie; Strich, Franz; and Fiedler, Marina, "Algorithmic Technologies as Threat to Who We Are: The Effect an IT Identity Threat has on Employees' Work Engagement" (2022). *ICIS 2022 Proceedings*. 2.
https://aisel.aisnet.org/icis2022/is_futureofwork/is_futureofwork/2

Algorithmic Technologies as Threat to who we are: The Effect an IT Identity Threat has on Employees' Work Attitude

Short Paper

Anne-Sophie Mayer
Vrije Universiteit Amsterdam
De Boelelaan 1105, 1081 HV Amsterdam
a.s.mayer@vu.nl

Franz Strich
Deakin University
221 Burwood Highway, Victoria 3125
f.strich@deakin.edu.au

Marina Fiedler
University of Passau
Innstraße 27, 94032 Passau
marina.fiedler@uni-passau.de

Abstract

Organizations' introduction of algorithmic technologies fundamentally affects employees' work processes, tasks, and responsibilities in organizations. Employees often find their professional identities threatened by the introduction of IT (a phenomenon labeled as IT Identity Threat). While prior studies have examined which mechanisms employees use to deal with such a perceived threat, it remains unclear how an IT Identity Threat affects employees' work attitude in response to advanced IT such as algorithmic technologies. Employees' work attitude is a recognized antecedent to workers' well-being or performance. Based on a mixed-method study in the banking industry, our study reveals that an IT Identity Threat negatively affects employees' work engagement. Further, our study uncovers how this effect comes about by showing that an IT Identity Threat decreases employees' perceived autonomy and experienced responsibility for their work outcomes. Overall, both factors contribute to a negative relationship between an IT Identity Threat and employees' work engagement.

Keywords*: algorithmic technologies,* IT Identity Threat, work engagement, perceived autonomy, experienced responsibility for work outcomes

Introduction

> "More and more work processes and tasks are automated, so I sometimes wonder if my job will be needed in the future or if machines will completely take it over. And then, I ask myself what kind of job I will do in the future and if my skills are still valuable. So, this makes me really scared, and the idea is really disengaging." (Employee, Risk management, Banking Industry)

Employees' professional identity is a core element of their self-perception of what they do and who they are as a member of their profession (Chreim et al., 2007; Nelson & Irwin, 2014; Pratt et al., 2006). In general, identity can be described as a set of meanings or beliefs individuals use to make sense of their environment (Bernardi et al., 2019; Burke & Stets, 2009; Craig et al., 2019). For specialized professionals such as doctors, judges or accountants, their identity attachment is particularly strong because they define themselves in relation to their job and their socially constructed work environment (Pratt et al. 2006).

Employees' identity is subject to change and adapts to new situations and experiences (Carter & Grover, 2015). Thereby, employees compare new situations to existing expectations associated with their identity (Petriglieri 2011). Generally, employees strive to maintain their existing identities, seek experiences to strengthen their self-beliefs, and try to uphold a positive self-image (Craig et al., 2019; Mishra et al., 2012; Nach, 2015; Petriglieri, 2011). If the new situation matches their own identity perception, no adjustment is necessary, their identity is verified, and employees experience satisfaction and increased self-efficacy (Burke & Stets, 2009). However, in situations in which the employee's identity standard cannot be confirmed, individuals experience a loss of self-esteem (Burke & Stets, 2009; Craig et al., 2019). In these cases, individuals perceive the situation as a threat to their identity (Nach, 2015). Overall, solid and positive identities are important for employees' well-being, performance, and job satisfaction (Carter & Grover, 2015; Carter et al. 2020; Nach & Lejeune, 2010). In contrast, negatively perceived identities can result in dissatisfaction and resistant or even defensive behaviors (Craig et al. 2019; Kim & Kankanhalli, 2009; Petriglieri, 2011).

With advancing technological progress, organizations increasingly introduce algorithmic technologies to enhance productivity, competitiveness, and innovation (Benbya et al., 2021; Faraj et al., 2018; van den Broek et al., 2021). These algorithmic technologies can supplement or even substitute employees' work processes, tasks, and responsibilities (Bailey et al., 2019; Craig et al., 2019; Faraj et al., 2018). Whereas the introduction of supplementing IS technologies has long been discussed in IS research, algorithmic technologies provide new challenges to employees' work perception. First, algorithmic technologies can potentially substitute for entire work processes (Bailey et al., 2019; von Krogh, 2018; Strich et al., 2021). Consequently, employees may by unable to reinforce and strengthen their identities (Craig et al., 2019; Petriglieri, 2011). Second, algorithmic technologies may restrict employees' interactions with their social and technological environment (Lindenbaum et al., 2020), further impeding their identity validation. Third, algorithmic technologies may adapt to changing parameters or new data (Benbya et al., 2020), confronting employees with less predictable decision outcomes (Dourish, 2016). Finally, whereas previous IS is characterized by employees' conscious engagement (Carter & Grover, 2015), algorithmic technologies potentially detach employees from autonomously derived decisions. Overall, algorithmic technologies provide a promising avenue for organizations to leverage economic outcomes. However, they may also hold potentially adverse effects for employees' identity.

The increasing use of algorithmic technologies significantly affects how employees perform their work, achieve their goals, define themselves in the workplace, and consequently challenges their identity (Strich et al., 2021). Recent literature introduced the concept of IT identity to describe positive self-identification and engagement with IT usage (Carter & Grover 2015; Carter et al. 2020b). However, employees can also perceive IT induced changes as a threat to their professional identity (Craig et al. 2019; Nach 2015; Nach and Lejeune 2010; Petriglieri 2011). This phenomenon is labeled *IT Identity Threat* and describes "the anticipation of harm to an individual's self-beliefs, caused by the use of an IT" (Craig et al. 2019, p. 269). The concept was developed to enhance the understanding, explicability, and prediction of IT resistance behavior. Craig et als' (2019) work showed that an IT Identity Threat is a predictor of IT resistant behavior, and thus, an important concept in the field of IT.

Prior studies have investigated how employees respond to identity threats caused by new technologies Nelson & Irwin, 2014; Petriglieri, 2011; Strich et al., 2021. For instance, Nelson and Irwin (2014) disclosed how librarians who felt the introduction of online search engines threatened their identity, were initially dismissive of the new technology. Yet, after recognizing the technology's potential for their own profession, they reconsidered and reconceptualized their self-image and adapted their identity to address the threat. In the context of algorithmic technologies, Strich and colleagues (2021) showed that employees engage in mechanisms to either protect or strengthen their professional identity, which significantly changed through the use of decision-substitutive AI systems. Overall, when confronted with an IS induced threat to their identity, individuals redefine their tasks, and try to develop a new understanding of themselves and their identity in the workplace (Nach, 2015; Nelson & Irwin, 2014; Pratt et al., 2006).

While previous research mainly focused on employees' response mechanisms to IT Identity Threats, we know little or nothing about how an IT Identity Threat affects employees' work attitudes. Work attitudes refer to employees' opinions, beliefs, and feelings about aspects of their work and are important determinants of employee behavior (Albrecht et al., 2015; Harter et al., 2002; Macey & Schneider, 2008; Rich et al., 2010). If employees have a positive attitude to their work, they are more likely to put extra effort into their work to meet the organization's goals, remain loyal with the organization, and perform better (Harter et al., 2002; Kahn, 1990; Rich et al., 2010). Consequently, our paper sheds light on the following research question:

> *How does an IT Identity Threat in the context of algorithmic technologies affect employees' work attitudes?*

To answer our research question, we build on findings from ongoing research based on a mixed-method approach. We deployed a developmental approach by first exploring the field through qualitative interviews and followed by an online survey to quantify our initial findings to generalize our results. We chose this method for our research for two major reasons. First, combining qualitative and quantitative methods allows us to examine exploratory and confirmatory questions within the same emerging research setting (Venkatesh et al., 2013; Venkatesh et al., 2016). So far, little is known about the impact of algorithmic technologies on IT Identity Threat and its effect on employees' work attitude, and a mixed-method approach provides the opportunity to gain in-depth insight into this new phenomenon (Venkatesh et al. 2013). Second, mixed-method research offers more robust and more accurate inferences than a single method approach (Teddlie and Tashakkori 2009; Venkatesh et al. 2013).

Our manuscript makes three contributions: First, we uncover how an IT Identity Threat impacts employees' work engagement, considering organizations' increasing digitization and the ever-faster development of technologies (Benbya et al. 2021; Chanias et al. 2019; Craig et al. 2019). Second, we uncover the mediating effect of employees' perceived autonomy and responsibility for work outcomes. Finally, we emphasize how organizations can mitigate the adverse effects of an IT Identity Threat.

Method of the Qualitative Study

To investigate the effect of an IT Identity Threat on employees' work attitude, we first wanted to know whether and how an IT Identity Threat is visible in the workplace where algorithmic technologies are used. Therefore, we interviewed employees working in different departments (e.g., human resources, service, consulting, and risk management) of a German bank. Our case company makes extensive use of algorithmic technologies in a wide range of departments to enhance and even substitute processes and tasks. Therefore, we considered this company especially suitable for studying the phenomenon of an IT Identity Threat in algorithmic technologies concerning employees' work attitude.

Overall, we conducted 15 semi-structured exploratory interviews at our case company between September and December 2019. Interviews were conducted face-to-face and by telephone and lasted 44 minutes on average. All interviewees have experienced the transition from non-algorithmic work to working with algorithmic technologies. The interview centered around questions such as "What algorithmic technologies do you use in your daily work?", "How do you perceive working with algorithmic technologies?", or "How has your work been affected by the use of algorithmic technologies?". All interviews were audio-recorded and transcribed verbatim.

We analyzed our interviews by using a grounded theory approach (Glaser and Strauss 1967; Locke 2001). We started with open coding, followed by selective coding of the interviews. All authors first coded the interviews independently. Then, we discussed and revised the identified categories until all authors agreed on the codes and their allocation. In the first round, open coding allowed us to gain an overview of how interviewees perceived algorithmic technologies and how they had affected their work life and work attitude. We went through all interviews and sorted quotes into an emergent set of topic-related categories. Based on these initial results, we compared our codes with relevant literature to find theoretical constructs that might reflect what we found in our interviews. Additionally, we aimed at uncovering relationships between our categories to shed light on possible interactions. Eventually, from our interviews, we were able to derive testable hypotheses about the effects of an IT Identity Threat in the context of algorithmic technologies.

Qualitative Findings: An IT Identity Threat in the Banking Industry

In a first step, we wanted to know whether there were instances of an IT Identity Threat in our case company, and if so, and how this happened. Therefore, we first asked interviewees about their job itself, the kind of algorithmic technologies they used in the workplace, how present algorithmic technologies were in their daily work, and how they perceived the increasing introduction and use of algorithmic technologies as part of the organization's digital transformation. These questions contributed to our in-depth understanding of the interviewees and the job environment they are working in. We found that algorithmic technologies are increasingly introduced and used in multiple departments and areas of the bank as part of the overall digital transformation strategy. Therefore, these algorithmic technologies could fundamentally affect how employees perform their work because they could take over work processes, tasks, and responsibilities to an extent formerly unheard of.

Thereby algorithmic technologies enhanced the automatization and digitization of work processes. One example of such a technology in our case company is the recent introduction of an algorithm to process the majority of the onboarding process (e.g., automatically generating welcome emails to new employees, reminders of missing documents, processing employees' data, etc.). Previously, employees manually performed the entire work process, from application evaluation to setting the contracts. Another example is the recent introduction of algorithms for commercial consulting (e.g., calculating investments, advising on insurance and loan conditions, etc.). Whereas consultants assessed and advised customers independently, the newly introduced systems can now derive customer-specific recommendations.

Our interviews disclosed that due to the increasing introduction of algorithmic technologies for a variety of different tasks and work processes as part of the bank's digital transformation, an increasing number of the employees' initial work processes, tasks, and responsibilities changed:

> "When I started my job, customers called me directly, and I took care of their requests. We often first had some small talk; I would ask how the kids were or how the house building was going. I have known most of my customers for a long time. And then we would take some time to go through their request, checking whether there was a forgotten password, a new credit card, or a change in the account's limits – I helped everyone. But now we have an automated system that receives most customers' requests. Now, only customers with special inquiries that the system cannot handle are forwarded to me, and my major job is processing the information from the system. This is really frustrating sometimes, and I miss my job where I was the customer's first contact person." (Employee, Service department)

Further, the introduction of algorithmic technologies had changed employees' work processes, tasks, and responsibilities and thereby seemed to threaten their identity. One major reason is that introducing various algorithmic technologies affected employees' daily work routines and their perception of their profession itself. For instance, one interviewee working in commercial customer consulting reported:

> "The private customer consulting has already been infiltrated by many autonomous systems, but so far our part has still been quite independent. But now we also have systems that derive their own decisions on loan amounts and the terms and conditions. It is just a matter of time before they take over our consulting business as well, which concerns me a lot. I still want to advise my customers independently and not only punch in some data that any idiot can do." (Employee, Commercial customer consulting)

Another interviewee expressed her thoughts by stating:

> "It is quite frustrating because I always loved my job, and I think I am doing quite a good job. But what can you do if technologies can do your job more and more, and even with greater speed and accuracy?! IT is definitely threatening – it makes me quite sad sometimes and a bit scared." (Employee, Service department)

These quotes indicate that the increasing use of algorithmic technologies that fundamentally affect the way employees perform their work causes an IT Identity Threat. Thus, we find that an IT Identity Threat is a relevant phenomenon in employees' daily work.

IT Identity Threat and its Effect on Employees' Work Engagement

We wanted to understand how the IT Identity Threat affects employees' work attitude in a second step. Therefore, we asked our interviewees how an IT Identity Threat had changed or influenced their work and their work engagement.

Most of our interviewees who perceived an IT Identity Threat reported that they experienced their jobs as less joyful and to be less enthusiastic about their job. For instance, one interviewee working in the bank's internal administration department stated that the increasing use of algorithmic technologies made her feel less needed and shifted her job from a service assistant to an assistant of the new technologies. This interviewee stated:

> "I have always been enthusiastic about my work but there are days when I am not really motivated anymore because many tasks I really enjoyed are now taken over by IT. So yeah, it is not the same anymore." (Employee, Internal administration)

Another interviewee mentioned similar feelings and reported:

> "I became a controller because I have always loved numbers and working with numbers. But basically, my job is becoming more and more a technical job that focuses on controlling and supervising the IT systems and not the numbers anymore. So, I feel that I used to be more enthusiastic about what I do and to be honest, there were times when I enjoyed my job more." (Employee, Controlling)

Similarly, one interviewee said:

> "The organization introduced [an IT system] last year with abilities that come quite close to mine, which is rather concerning. And of course, there are rumors that the company wants to replace employees in the future by new technologies. And I can already feel that right now. So, to be honest, I always used to put a lot of effort into my work – even more than was required – but this development makes me feel less enthusiastic about my work and so I do what I have to do, but I'm no longer motivated to put extra effort into it." (Employee, Service department)

Overall, our interviews disclosed that employees who feel the introduction of an algorithmic technology threatens their professional identity, tend to feel less enthusiastic about their job, and are thus less engaged. Comparing these findings to previous research, we found that our codes reflected how employees experienced their work engagement (Hackman & Oldham, 1975, 1976).

Employees' work engagement is an important antecedent to their personal connection and devotion to their work (Kahn, 1990; Rich et al., 2010; Schaufeli et al., 2006), as well as to their commitment, concentration, and performance (Albrecht et al., 2015; Bakker et al., 2008; Macey & Schneider, 2008; Schaufeli et al., 2006). Furthermore, recent literature indicates that the use of IT positively influences employees' work engagement if the employees identify with the technology and rely on it to extend their abilities (Carter et al., 2020a). However, it remains unclear how the introduction and use of algorithmic technologies relate to employees' work engagement in cases where they feel the technology threatens their identity. Therefore, we propose that an IT Identity Threat has a negative impact on employees' work engagement in the context of algorithmic technologies:

H1: An IT Identity Threat negatively affects employees' work engagement.

Mediating effects of an IT Identity Threat

During our interview phase, two dominant themes emerged regarding how an IT Identity Threat affects employees' work engagement in the context of algorithmic technologies. These themes referred to (1) the degree to which our interviewees perceived themselves as autonomous in doing their work and (2) the individual perception of how responsible they felt for their work outcomes. Thus, we aimed to understand which role these factors play in the context of an IT Identity Threat and how they might help to explain the effect of an IT Identity Threat on employees' work engagement.

Perceived autonomy

First, we found that an IT Identity Threat negatively affects employees' perceived autonomy. Our interviews disclosed that algorithmic technologies could often autonomously take over entire work processes, tasks, and responsibilities that employees formerly performed. Thus, employees often perceive that algorithmic technologies remove a certain degree of their autonomy regarding decisions on how to perform their work. For instance, one interviewee said:

> "I work in commercial customer consulting, and nowadays, an increasing number of really advanced ITs are already used in this area. These systems completely change the way I process and perform my work. For example, I always decided how to advise my customers, what kind of loans and insurance I could offer them, and what kind of long-term strategy is the best for the company. Now I have to use systems that structure how I advise my customers and give concrete advice on what allegedly would be best for the customer. So, I only have a limited voice now, which I think restricts my work." (Employee, Commercial customer consulting)

Especially, employees who perceive an IT Identity Threat tend to feel that in using algorithmic technologies, they have reduced autonomy because they perceive algorithmic technologies as posing a serious threat toward taking over their initial job. One employee stated:

> "To be honest, my job has changed a lot since the digital transformation and I really feel that I'm not really needed anymore. This makes me scared of course, because I know that I can be replaced by technologies at any time. I mean, when I started my job at the service desk, I did all transfers, deposits, or account openings on my own. Now, technology is doing it for me and basically has taken over my job. Even if customers call me, I have to use a system in which I only have to enter the data without any other option or freedom." (Employee, Service department)

Additionally, employees who perceive an IT Identity Threat pointed out that the far-reaching effect of algorithmic technologies restricts their autonomy. As one employee said:

> "We always worked with IT, but since we have this digitalization agenda that promotes the digital transformation of the entire organization, IT took over more and more of our initial jobs. Whereas I basically decided everything on my own with some IT system support, now the IT is largely able to take over most parts of my job, even to the point of taking decisions for me. This is quite concerning, to be honest." (Employee, Internal administration)

Consequently, our interviews indicate that an IT Identity Threat negatively affects employees' perceived autonomy. While autonomy is an important determinant of employees' work engagement (Hackman & Oldham, 1975, 1976 ; Morgeson & Humphrey, 2006; Zhang, Jex, Peng, & Wang, 2017), an IT Identity Threat seems to diminish the positive effect autonomy has on employees' work engagement. Thus, the decrease in employees' perceived autonomy caused by an IT Identity Threat partially explains the negative effect of an IT Identity Threat on employees' work engagement. Consequently, we propose:

H2: An IT Identity Threat negatively affects employees' perceived autonomy.

H3: Employees' perceived autonomy mediates the negative effect of an IT Identity Threat on employees' work engagement.

Experienced responsibility for work outcomes

Second, we found that an IT Identity Threat negatively affects employees' experienced responsibility for their work outcomes. Our interviews disclosed that introducing algorithmic technologies impacts employees' responsibility for their work outcomes. Interviewees reported that these technologies could autonomously perform work processes, tasks, and responsibilities. Further, many algorithmic technologies can derive decisions that employees formerly made. In these circumstances, technologies take over certain employee responsibilities. Such a responsibility shift became apparent in our interviews. For instance, one interviewee reflected:

> "When I started my job, I was entirely responsible for all investment consulting. For example, if a client wanted to invest money without much risk, I was responsible for finding such an investment opportunity. If it turned out later that I had chosen a high-risk investment for him, I would have been responsible for it and would have had to answer for it. Now, we have a system that makes suggestions depending on the customer's preferences in terms of risk tolerance, income, etc., and I usually follow these suggestions because the management prefers that we stick to the system. If something doesn't fit later on, it's no longer my responsibility, but lies with the system. And I can prove that transparently, and always refer back to the system's decision. So, this can be an advantage, but mostly I find it

> rather sad, because I loved having my own responsibility for what I do." (Employee, Financial Consulting)

In our interviews, we found that employees who perceive an IT Identity Threat tend to feel less responsible for their work outcomes if they use algorithmic technologies. As one employee put it:

> "I think the increasing use of technologies in the workplace are definitely a threat, although the management always refers to IT's potential. But in my opinion, ITs hold a threat to human work, because machines are often cheaper and better. So that makes me scared sometimes, yes. And not only can technologies do my job; they also make the job less interesting. I mean, for example, I was always responsible for a huge bunch of tasks and processes, but now most of them can be managed by automated systems. So, you lose responsibility and it is becoming more difficult to realize what you are actually doing, or what your responsibility and your value is." (Employee, Risk management)

Consequently, our interviews reveal that an IT Identity Threat negatively impacts on employees' experienced responsibility for their work outcomes. While responsibility for work outcomes is an important determinant of employees' work engagement (Hackman & Oldham, 1975, 1976; Morgeson & Humphrey, 2006; Zhang et al., 2017), an IT Identity Threat diminishes the positive effect responsibility for work outcomes has on employees' work engagement. Thus, the decrease in employees' experienced responsibility for their work outcomes caused by an IT Identity Threat seems to explain the negative effect of an IT Identity Threat on employees' work engagement. Therefore, we hypothesize:

H4: An IT Identity Threat negatively affects employees' experienced responsibility for their work outcomes.

H5: Experienced responsibility for work outcomes mediates the negative effect of an IT Identity Threat on employees' work engagement.

Overall, we find in our interviews that an IT Identity Threat negatively affects employees' work engagement and their perceived autonomy and experienced responsibility for their work outcomes. Further, our interviews suggest that employees' perceived autonomy and experienced responsibility for their work outcomes mediate an IT Identity Threat's negative effect on employees' work engagement. Figure 1 summarizes the five hypotheses derived from our qualitative interviews with employees of a bank. In a next step, we will test our hypotheses with a quantitative field survey at our case company using an online self-report questionnaire. Our case company makes extensive use of algorithmic technologies in a wide range of departments to substitute employees work processes. We plan to operationalize IT identity threat using the recently introduced measure by Craig et al. (2019), measuring the three dimensions of an IT Identity Threat: (1) loss of worth-based self-esteem, (2) loss of competence-based self-esteem, and (3) loss of authenticity-based self-esteem. Further, we plan to assess employees' work engagement using the five-item version of the Utrecht Work Engagement Scale (Bledow et al., 2011). To measure employees' perceived autonomy, we will use the three-item measure of decision-making autonomy used in the Work Design Questionnaire (Morgeson & Humphrey, 2006). Finally, we will assess employees' experienced responsibility for their work outcomes using the Experienced Responsibility for Work Outcomes subscale put forward in the Job Diagnostic Survey (Hackman & Oldham, 1975).

Conclusion

Our research makes three contributions by studying how an IT Identity Threat caused by algorithmic technologies affects employees' work attitude. First, we uncover how an IT Identity Threat impacts employees' work engagement. Thereby, we extend Craig et al.'s work (2019) which studied the phenomenon in an educational context. Second, our study reveals how the adverse effect between an IT Identity Threat and employees' work engagement can be explained by identifying two mediating factors: employees' perceived autonomy and responsibility for work outcomes. Finally, our research also highlights how organizations can use these levers to mitigate the adverse effects of an IT Identity Threat. Despite algorithmic technologies' capabilities, employees who feel valued regarding their autonomy and responsibility retain valuable success factors in countering an IT Identity Threat.

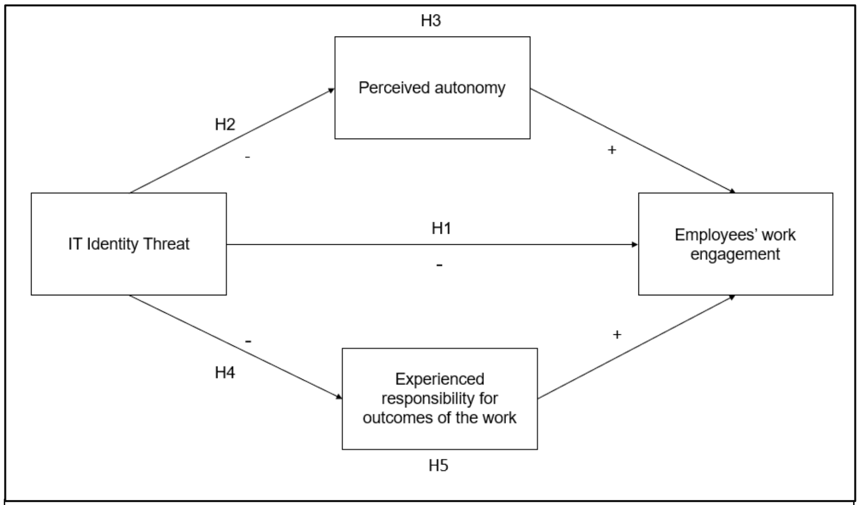
H3
Perceived autonomy
H2
-
+
IT Identity Threat
H1
-
Employees' work engagement
-
+
H4
Experienced responsibility for outcomes of the work
H5

Figure 1. Conceptual model derived from the interviews

References

Albrecht, S. L., Bakker, A. B., Gruman, J. A., Macey, W. H., and Saks, A. M. 2015. "Employee Engagement, Human Resource Management Practices and Competitive Advantage: An Integrated Approach," *Journal of Organizational Effectiveness* (2:1), pp. 7–35.

Bailey, D., Faraj, S., Hinds, P., von Krogh, G., and Leonardi, P. 2019. "Special Issue of Organization Science: Emerging Technologies and Organizing," *Organization Science* (30:3), pp. 642–646.

Bakker, A. B., Schaufeli, W. B., Leiter, M. P., and Taris, T. W. 2008. "Work Engagement: An Emerging Concept in Occupational Health Psychology," *Work and Stress* (22:3), pp. 187–200.

Benbya, H., Pachidi, S., and Jarvenpaa, S. L. 2021. "Special Issue Editorial: Artificial Intelligence in Organizations: Implications for Information Systems Research," *Journal of the Association for Information Systems* (22:2), p. 10.

Bernardi, R., Sarker, S., & Sahay, S. 2019. "The role of affordances in the deinstitutionalization of a dysfunctional health management information system in Kenya: An identity work perspective," *MIS Quarterly* (43:4), pp. 1177–1200.

Bledow, R., Schmitt, A., Frese, M., and Kühnel, J. 2011. "The affective shift model of work engagement," *Journal of Applied Psychology* (96:6), pp. 1246–1257.

van den Broek, E., Sergeeva, A., and Huysman, M. 2021. "When the Machine Meets the Expert: An Ethnography of Developing AI for Hiring," *MIS Quarterly*.

Burke, P. J., & Stets, J. E. 2009. *Identity Theory*. Oxford, England: Oxford University Press.

Carter, M., and Grover, V. 2015. "Me, Myself, and I(T): Conceptualizing Information Technology and Its Implications," *MIS Quarterly* (39:4), pp. 931–957.

Carter, M., Petter, S., Grover, V., and Thatcher, J. B. 2020a. "IT Identity: A Measure and Empirical Investigation of Its Utility to IS Research," *Journal of the Association for Information Systems* (21:5), pp. 1313–1342.

Carter, M., Petter, S., Grover, V., and Thatcher, J. B. 2020b. "Information Technology Identity: A Key Determinant of IT Feature and Exploratory Usage," *MIS Quarterly* (44:3), pp. 983–1021.

Chanias, S., Myers, M. D., and Hess, T. 2019. "Digital Transformation Strategy Making in Pre-Digital Organizations: The Case of a Financial Services Provider," *Journal of Strategic Information Systems* (28:1), Elsevier, pp. 17–33.

Chreim, S., Williams, B. E., and Hinings, C. R. 2007. "Interlevel Influences on the Reconstruction of Professional Role Identity," *Academy of Management Journal* (50:6), pp. 1515–1539.

Craig, K., Thatcher, J. B., and Grover, V. 2019. "The IT Identity Threat: A Conceptual Definition and Operational Measure," *Journal of Management Information Systems* (36:1), Routledge, pp. 259–288.

Dourish, P. 2016. "Algorithms and their others: Algorithmic culture in context," *Big Data & Society* (3:2).

Faraj, S., Pachidi, S., and Sayegh, K. 2018. "Working and Organizing in the Age of the Learning Algorithm," *Information and Organization* (28:1), Elsevier, pp. 62–70.

Glaser, B. G., and Strauss, A. L. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Chicago, IL: Aldine.

Hackman, J. R., and Oldham, G. R. 1975. "Development of the Job Diagnostic Survey," *Journal of Applied Psychology* (60:1).

Harter, J. K., Schmidt, F. L., and Hayes, T. L. 2002. "Business-unit-level relationship between employee satisfaction, employee engagement, and business outcomes: A meta-analysis," *Journal of Applied Psychology* (87:2), pp. 268–279.

Kahn, W. A. 1990. "Psychological Conditions of Personal Engagement and Disengagement at Work," *Academy of Management Journal* (33:4), pp. 692–724.

Kim, H.-W., and Kankanhalli, A. 2009. "Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective," *MIS Quarterly* (33:3), pp. 567–582.

Locke, K. 2001. *Grounded Theory in Management Research*, Thousand Oaks, CA: Sage.

Lindenbaum, D., Vesa, M., and den Hond, F. 2020. "Insights from "The Machine Stops" to better understand rational assumptions in algorithmic decision making and its implications for organizations," *Academy of Management Review* (45:1), pp. 247-263.

Macey, W. H., and Schneider, B. 2008. "The Meaning of Employee Engagement," *Industrial and Organizational Psychology* (1:1), pp. 3–30.

Mishra, A. N., Anderson, C., Angst, C. M., and Agarwal, R. 2012. "Electronic Health Records Assimilation and Physician Identity Evolution: An Identity Theory Perspective," *Information Systems Research* (23:3-part-1), pp. 738–760.

Morgeson, F. P., and Humphrey, S. E. 2006. "The Work Design Questionnaire (WDQ): Developing and Validating a Comprehensive Measure for Assessing Job Design and the Nature of Work," *Journal of Applied Psychology* (91:6), pp. 1321–1339.

Nach, H. 2015. "Identity under Challenge: Examining User's Responses to Computerized Information Systems," *Management Research Review* (38:7), pp. 703–725.

Nach, H., and Lejeune, A. 2010. "Coping with Information Technology Challenges to Identity: A Theoretical Framework," *Computers in Human Behavior* (26:4), pp. 618–629.

Nelson, A. J., and Irwin, J. 2014. "'Defininig What We Do - All over Again': Occupational Identity, Technological Change, and the Librarian/Internet-Search Relationship," *Academy of Management Journal* (57:3), pp. 892–928.

Petriglieri, J. L. 2011. "Under Threat: Responses to and the Consequences of Threats to Individuals' Identities," *Academy of Management Reivew* (36:4), pp. 641–662.

Pratt, M. G., Rockmann, K. W., and Kaufmann, J. B. 2006. "Constructing Professional Identity: The Role of Work and Identity Learning Cycles in the Customization of Identity among Medical Residents," *Academy of Management Journal* (49:2), pp. 235–262.

Rich, B. L., Lepine, J. A., and Crawford, E. R. 2010. "Job Engagement: Antecedents and Effects on Job Performance," *Academy of Management Journal* (53:3), pp. 617–635.

Schaufeli, W. B., Bakker, A. B., and Salanova, M. 2006. "The Measurement of Work Engagement with a Short Questionnaire: A Cross-National Study," *Educational and Psychological Measurement* (66:4), pp. 701–716.

Strich, F., Mayer, A. S., and Fiedler, M. 2021. "What Do I Do in a World of Artificial Intelligence? Investigating the Impact of Substitutive Decision-Making AI Systems on Employees' Professional Role Identity," *Journal of the Association for Information Systems* (22:2), pp. 304–324.

Teddlie, C., and Tashakkori, A. 2009. *Foundations of Mixed Methods Research*, Thousand Oaks, CA: Sage Publications Ltd.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21–54.

Venkatesh, V., Brown, S. A., and Sullivan, Y. 2016. "Guidelines for Conducting Mixed-Methods Research: An Extension and Illustration," *Journal of the Association for Information Systems* (17:7), pp. 435–494.

Zhang, W., Jex, S. M., Peng, Y., and Wang, D. 2017. "Exploring the Effects of Job Autonomy on Engagement and Creativity: The Moderating Role of Performance Pressure and Learning Goal Orientation," *Journal of Business and Psychology* (32:3), Springer US, pp. 235–251.