Subverting Organisational IT Policy: A Case in China

Full Paper

Robert M. Davison
City University of Hong Kong
isrobert@cityu.edu.hk

Carol X.J. Ou
Tilburg University
Carol.Ou@uvt.nl

Abstract

Studies of the dark side of Information Systems are encountered with increasing frequency. In this paper, we investigate how selected hotel employees in China deliberately subvert IT Policy in order to gain access to the IT applications that they believe essential to work. Following a review of the literature on IT Governance, resistance and subversion, we engage in an interpretive case study of employee practices, drawing on the Work Systems framework to analyse employees' work practices and subversive behaviour. We suggest that subversive IT behaviour may be more common than the limited literature would suggest and encourage researchers to probe these organisational practices and solutions in depth.

Keywords:

Introduction

Even though the dark side of Information Systems (IS) is broadly recognised in the literature (Zuboff, 1988; Turel et al., 2011; Tarafdar et al., 2015a, 2015b), and resistance to IS has become a respectable topic of study (Ignatiadis and Nandhakumar, 2009; Subramaniam et al., 2013), specific cases where employees deliberately subvert organisational IT policies with their own IS-supported working practices are rarely encountered in the literature. These anti-establishment practices are commonly referred to as counter-productive work behaviour (Weatherbee, 2010) and are rarely viewed in a positive light by either organisations or academics. As Markus (1983) notes, researchers have generally ignored the positive motives that may underlie such employee behaviour, while Piderit (2000) observes that it is tempting for managers to treat their employees as mere obstacles to progress.

It seems likely that these informal, IS-supported working practices are common (DesAutels, 2011; Chua et al., 2014). As digital natives enter the workforce in droves, we should expect to see more situations where employees subvert organisational IT policies and seek access to the applications they believe essential to their work (Chua et al., 2014; Shehadi et al., 2013). These employees may draw on the spirit of 'bricolage' (Lévi-Strauss, 1966) as they tinker with the elements of their 'repertoire' (Duymedjian and Rüling, 2010) in a problem-driven, spontaneous and experimental fashion, leveraging whatever resources are easily available and iteratively improving their designs. However, since these acts of employee independence are rarely condoned by organisations (Weatherbee, 2010), it is perhaps not surprising that they are equally rarely investigated: organisations are understandably wary of having their dirty washing aired in public. Nevertheless, this kind of employee behaviour is theoretically interesting because it differs from normative theoretical perspectives of technology adoption and use, most of which assume voluntary behaviour. When behaviour is not so much voluntary as driven by necessity, current theories are less helpful with respect to measuring its antecedents and consequences.

In our own prior research investigations into the way employees leverage Information Technology (IT) applications for work in Chinese organisations (Davison and Ou, 2013, 2014), we have observed that even when organisations implement restrictive policies that limit which IT applications can be used and by whom, employees are loath to abandon the social media applications upon which they depend for both networking and problem solving. In line with the literature, these employees oppose what they perceive as

unreasonable managerial restrictiveness, often citing the normative climate of what is acceptable behaviour in the local milieu (Weatherbee, 2010). Further, they create ad hoc solutions to fit their immediate needs (DesAutels, 2011). They refuse to follow managerially-approved, cliché-driven directives (cf. Weick, 1998) and instead subvert organisational IT policy. Drawing on both the literature and our practice-based observations, we suggest that there is a significant gap in our knowledge about the subversive power of IT applications in organisations. This prompts our research question: How and why do employees subvert organisational IT policy at work?

In order to answer this question, we present an interpretive case study in which we explore how and why selected hotel employees in China deliberately subvert organisational IT policies, violating normative managerial expectations and IT governance as they strive to accomplish their work. In effect, they adopt a bricolage view of IS, crafting idiosyncratic solutions that incorporate whatever IT components they can access, in order to facilitate the completion of both their regular work and additional ancillary activities that they deem critical to their positions and careers. Given the lack of support in the organisational environment, many of these activities are undertaken covertly since they violate corporate, even if not social, norms. In order to frame the way that these employees craft their personal IS, we draw on Alter's (2013) tools for the analysis of Work Systems, explicating a single case to illustrate how this subversive work is performed.

Following this introduction, we briefly introduce the relevant background literature that deals with IT policy in the context of IT governance, and subversive acts against IT policy, including resistance and bricolage. We then introduce our research methods and explain how we collected data. The case of employee subversion of organisational IT policy follows. In the discussion of the case, we highlight important theoretical considerations that will require future attention before concluding the article.

Literature Review

The IT policy that is the focus of subversive behaviour constitutes a core element in the IT governance domain. Organisations enact IT governance in order to ensure that appropriate controls are exercised over corporate data, minimising the likelihood that that data will be corrupted or leaked to unauthorised parties. It is broadly accepted that internal employee expectations should be aligned with IT policy (Avison and Fitzgerald, 1995) if those same employees are to accept the legitimacy of the IT policy and therefore if strategic business objectives that are linked with the IT policy are to be achieved. This is consistent with Alter's (2013) Work Systems, where IT governance is part of the operating environment. However, Xue et al. (2011) have noted a tendency for this alignment to be weakened when the work undertaken at corporate HQ is very different from that at the local business unit, i.e. employees may not be consulted about IT policy at all: it is simply imposed on them. The tensions that arise in such circumstances are challenging to manage (Bartlett and Ghoshal, 1998).

Despite a thorough search of the literature, we have found remarkably few studies dealing with subversion to IT policy. We first distinguish the terms 'resistance' and 'subversion'. According to the OED (2015), resistance refers to acts of "resisting, opposing, or withstanding someone or something". In contrast, subversion refers to "the action or process of undermining the power and authority of an established system or institution". Of the two terms, subversion is clearly the more aggressive or radical. In the entrepreneurship literature, e.g. Bureau and Zander (2014), and consistent with this definition, subversion is acknowledged as a tactic employed to change the status quo and create opportunities for innovations. Employee behaviours that may be described as subversive are also encountered in the literature on counter-productive work behaviour (Weatherbee, 2010; Klotz and Buckley, 2013); however, in the IS domain, the term 'resistance' is used much more frequently when referring to employee behaviour that does not conform to managerial expectations.

Lapointe and Rivard (2005) synthesise the literature on resistance to technology. Historically, this stream of literature has often viewed resistance unfavourably. For instance, resistance may be viewed by managers as a hindrance to strategic change (Ansoff, 1988) and motivated by employees' desire not to be controlled or monitored by management (Cook and Brown, 1999). Nevertheless, some scholars now view resistance more sympathetically: it is recognised that some IT applications are flawed and so resistance is reasonable (Kling, 1996; Ignatiadis and Nandhakumar, 2009). Indeed, resistance and its consequences

may even be beneficial for the organisation (Markus, 1983), for instance where they are institutionalised as organisational routines (Pentland and Feldman, 2008).

Lapointe and Rivard (2005) suggest that resistance behaviour can be manifested in four forms: apathy, passive resistance, active resistance and aggressive resistance. Each of the forms is characterised by different behaviour (see Table 1). In their summary, subversive behaviour is one of the instances of aggressive resistance. Lapointe and Rivard (2005) point out that the object of resistance must be specified, given the importance of the "content of what is being resisted" (Jermier et al., 1994). Thus, employees may resist either the implementation of an IT artifact (Joshi, 1991) or the imposition of a particular technology environment or policy.

Resistance Type	**Manifestations and Consequences**
Apathy	Lack of interest in the situation. Inaction. (Reluctant) compliance with corporate expectations for technology use.
Passive Resistance	Lack of cooperation with requirements. Preference for original ways of working. Low-key actions that are largely invisible.
Active Resistance	Positive and significant actions taken to create personal information systems that ensure work can be done but will not harm the organisation.
Aggressive Resistance	Direct opposition or deception, such as: attempts to sabotage processes; subvert the intended functionality of a system; deliberately enter incorrect data, requirements or deadlines; damage the organisation.

Table 1: Types of Resistance, their Manifestations and Consequences
(after Lapointe and Rivard, 2005).

As LaPointe and Rivard (2005) suggest, when employees are confronted with a technology environment or policy that they dislike, several outcomes may occur. They may reluctantly or apathetically acquiesce to its demands and constraints, or they may enact a behaviour that to a greater or lesser extent rejects the new status quo (cf. Hirschman, 1970). It is these latter behaviours that interest us and in particular, the ways in which employees invent solutions that circumvent the new official status quo. Aggressive resistance, accompanied by behaviour that is counter-productive, harmful to the organisation and disruptive to systems, is likely to be condemned harshly by managers and subjected to severe penalties (Weatherbee, 2010; Griffin and Lopez, 2005).

Less aggressive forms of resistance, on the other hand, although still subversive are not entirely disconnected from organisational routines and hence facilitate the completion of work (Bureau and Zander, 2014); these activities may remain below management's radar and so enjoy greater longevity. These less aggressive behaviours are often highly innovative and embody the spirit of bricolage (Levi-Strauss, 1966) because employees create flexible yet robust solutions to their problems out of whatever resources are available for recombination in new forms (Des Autels, 2011; Senyard et al., 2014). Indeed, Duymedjian and Rüling (2010, p.135) suggest, following Weick (1993), that acts of bricolage facilitate "the resilience which enables an individual … to overcome a crisis situation by maintaining both a coherence of identity and the capacity to act". The resulting personal IS are thus not mere technologies-as-artefacts, but technologies-in-use (Orlikowski, 2000), adapted to the immediate context and reflecting the bricoleur's resilient attitude to externally imposed change and versatile knowledge about what works, thereby contributing to self-efficacy (Bandura, 1977).

Research Context and Methods

In order to explore how employees subvert organisational control with IT, we focus on the case of Ravine, a global hotel management company with close to 3,700 hotels affiliated with its brands in around 100 countries, spanning the entire range from one- to five-star properties. Ravine is a major player in the Chinese market, operating over 150 hotels. In the majority of hotel properties, Ravine is not the property owner, instead providing hotel management services. These services reflect Ravine's corporate culture,

branding and operating principles, including IT policy. During the course of this research (2011-2013), Ravine's global HQ was in the process of promulgating its global IT platform to hotel property owners. This platform includes the provision for Internet-related services that are designed for use by hotel employees. Ravine's systems are not intended for hotel guest use as the hotel owner makes arrangements with a local Internet Services Provider (ISP) to cater to guest needs.

The current paper is extracted from a much larger interpretive study (Walsham, 1993, 1995) into the ways in which hotel employees leverage IT for work, drawing primarily on interview data from employees in hotels across China. We are attempting to understand the associated phenomena of subversion and bricolage as experienced and enacted by hotel employees. In order to accomplish this, we collected a rich set of data from a large number of employees in over 20 hotels. Here, we report on a fraction of this data, focusing on the specific cases of selected employees who actively subverted Ravine's IT policies through acts of bricolage in order to ensure that they could complete their work effectively. The interviews were conducted in a semi-structured fashion according to a protocol that addressed the wide variety of issues that were of interest in the larger project, viz.: the technologies used for communication, the role of interpersonal relationships (known as guanxi in Chinese) in work-related communication, the nature and impact of IT policies on the way work was conducted, and the ways in which employees subverted those IT policies that obstructed their completion of both work and other ancillary activities. Interviews lasted 30-60 minutes, were conducted in English and were not recorded, due to the sensitivity of the topic: employees freely described how they violated corporate rules. Instead, the interviewer made copious notes during and after interviews, then typed up these notes into transcripts immediately so as to be available for later analysis (Barley, 1990).

The instrumental theory (Davison et al., 2013) that we use to document and analyse the instances of subversion and bricolage that we recorded is Work Systems Theory (Alter, 2013). As Alter (ibid., p.75) remarks "A work system is a system in which human participants and/or machines perform work (processes and activities) using information, technology, and other resources to produce specific products/services for specific internal and/or external customers". The simplest depiction of a work system takes the form of a triangle (see Figure 1) where the key elements are easily identified: participants engage in work processes and activities using and creating both information and technologies in order to produce products and services for customers (who may be internal or external to the organisation). The work processes and activities are undertaken in the context of a specific organisational environment, governed by the strategies of the organisation and facilitated by infrastructural elements, including policy-oriented requirements. The two-headed arrows indicate that the various components of the model are engaged in two-way relations. Thus, participants undertake work and are influenced by that work. Work draws on information resources (whether held in formal databases, on the Internet, in paper-based documents, or even in the heads of other people) which may be updated as a result of the work done. Likewise, a wide variety of technologies support work, and knowledge about how these technologies create value in specific situations is updated and retained by the participants for future application. Meanwhile, the participants create products/services for customers – who will provide feedback that is also retained by the participants. It is notable that Alter (2013) deliberately avoids the word 'user' or 'employee', preferring to distinguish 'participants' from 'customers'.

In our analysis of the way employees employ bricolage techniques to create their own personal IS, we draw on Alter's (2013) work systems framework, which permits an easy-to-record tabular presentation of the relevant data, ensures that we collect all relevant data, and thus guides our story telling.

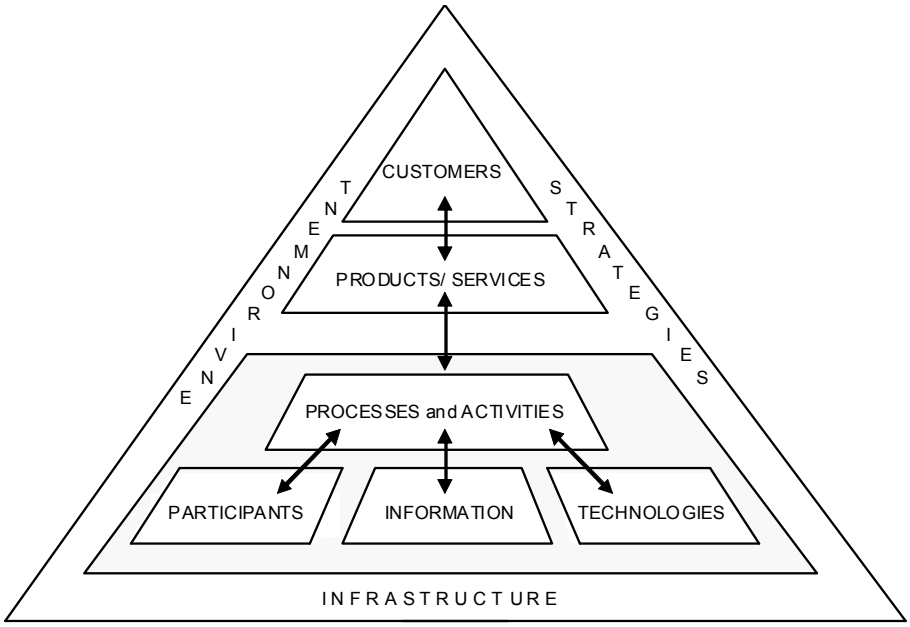

Figure 1: Work Systems Framework

Case Description

Ravine takes a strict line where IT policy is concerned. Hotel back offices generally experience very slow Internet access with bandwidth of 2 Mbps. Only software that is approved by the global VP for IT is permitted. Social media applications (such as Facebook, YouTube, QQ, Weibo and Twitter) and file sharing applications (such as Dropbox) are explicitly blocked. The policy is enforced by the simple means of channelling all Internet communications through a proxy server/firewall in Shanghai (where Ravine's regional HQ is located). Ostensibly, the reason for protecting the working environment so carefully is the need for information security. Ravine's Corporate VP for IT made this very clear in a telephone conversation with the first author when he explained: "Security is paramount. … All Ravine hotels operate standard software, globally. There is zero tolerance for malware and the risks that malware would bring". A regional VP for Southern China was a little more forthcoming when probed about the prohibition against social media software, noting that, "There is no value in chatting. Social Media applications have no role to play in Ravine's corporate culture", even though he agreed that Social Media applications were inextricably connected with the day-to-day life of citizens in China. It is important to note that while certain Western Social Media applications like Twitter, Facebook and YouTube are blocked in China, many others (both domestic and foreign) are freely accessible. A Front Office Manager in Beijing told us: "I am not allowed to use MSN. My relationship network has suffered and I have lost some contacts". Similarly, the Executive Assistant to the General Manager at a hotel in Macau reported: "I would like to be able to use MSN for communication as it would be faster and more natural".

Notwithstanding this strict IT policy that severely limits bandwidth and blocks access to social media applications, we found that certain hotel employees genuinely do need unrestricted access to Internet bandwidth in order to transmit large files to and communicate with a variety of primarily external customers. The IT Director of a hotel in Guangzhou complained: "The Sales Manager sends 10-15 emails, each with a 2 MB attachment, every afternoon. It slows down the whole network because we only have a 2 Mbps line to the Shanghai office for all emails". These employees typically work in the Marketing, Communications and PR departments, though senior managers in any part of the hotel may also have similar needs. The slow Internet speed has a severe impact on employee productivity The Marketing Manager in the same Guangzhou hotel reported: "A two minute task can take two hours. I simply cannot afford to waste so much time for so little work done. There has to be a better way".

Employees also need unrestricted access to social media because most of their customers and network contacts only use social media for all communication purposes. As a PR Manager in Wuhan reported: "Without QQ [A popular instant messenger application] I cannot work. I use QQ to contact many external parties, such as travel agents and government departments. These people refuse to use email and it is very hard to get hold of them on the phone. Therefore I must be able to use QQ". Meanwhile, the Sales Director of a hotel in Shanghai reported "I have several hundred work-related contacts on MSN, especially corporate clients, travel agents and ticketing consolidators. It is particularly useful that I can quickly identify if a person is online or not and hence available to talk". The purpose of this communication relates both to official hotel business and to ancillary activities associated with relationship management, e.g. asking for help from their personal relationship networks and also helping others who ask them for help.

Given the inadequate infrastructural environment and the inability of local IT or General Managers to improve access to IT, these employees devise innovative solutions that enable them to secure access to both the bandwidth and the social media applications they need. Although these innovations subvert corporate IT policy, they are generally undertaken with the full support of local managers who are as much the victims of the IT policy as any junior employee. As the General Manager of a hotel in Suzhou commented: "Social media is part of life. We can't block it. But we hope to encourage employees to use it responsibly". In Table 2 (below) we provide a Work Systems snapshot characterisation of the ways in which employees create solutions that ensure they gain access to the technologies they need.

Environment	Infrastructure	Strategies
Ravine provides a standardised set of IT policies for all the hotel properties it manages. One policy explicitly prohibits employees from accessing social media applications/sites such as instant messengers and microblogs. Beyond Ravine, the local environment is one where access to high bandwidth is cheap and normal. Further, access to social media applications is a normal activity for most citizens.	The standard Internet bandwidth provided by Ravine for back-office employees runs at 2Mbps. Ravine also contracts with a local Internet Services Provider to provide Internet access for hotel guests. This is typically much faster than available for hotel employees, with speeds of 100Mbps to 1Gbps. The guest network is unrestricted by Ravine, though it is restricted by Chinese government prohibitions which prevent access to applications like Facebook, YouTube and Twitter.	Ravine has no plan to change its IT policy, which channels all Internet-based communications via a proxy server located in corporate HQ. All social media applications are blocked as a matter of corporate policy. Again, there is no plan to change this policy, which affects all hotel-based employees from the General Manager downwards.

Customers (Hotel and Personal)	Products & Services
Hotel clients (individual and corporate) Travel agents, Hotel suppliers, Hotel employees, Hotel Fans/Followers, Government Departments Personal contacts (members of the personal relationship network)	Marketing Materials for travel agents and corporate clients in the form of: • E-Brochures • PowerPoint Shows • PR Information about the hotel Routine communications with hotel guests, fans and followers. External relations with suppliers and government departments Solutions to problems Requests for information

Subversive Work Practices (Bricolage Solutions to Ensure Access to Systems)		
1. Employees access their desired social media applications via the hotel's guest network, which is normally accessible wirelessly across the hotel. They gain access with personal devices such as smart phones and tablets, though some may use notebooks or even the PCs located in the hotel's executive lounge. 2. The guest network also permits the rapid transfer of large files to corporate clients. 3. If the guest network is not available or cannot be accessed, employees may save the relevant files to USB, and then upload the same files to private microsites from home, informing their clients about the new content available on the microsite.		
Interview Comments from Hotel Employees		
1. Human Resources Manager, Macau: "It is easy to tap into the guest network with a notebook, tablet or smart phone in order to access these resources, but the same method cannot be used to access corporate systems". 2. Marketing Manager, Guangzhou: "I have to use the guest network to send large files". 3. Marketing Manager, Guangzhou: "My job is to communicate, but there are no tools to achieve this, so I have no choice but to use private, self-funded resources. I have set up an offshore microsite so as to communicate with different customers". 4. Marketing and Communications Manager, Beijing: "I use the guest network for microblog marketing on Weibo [a microblog similar to Twitter]".		
Participants	**Information**	**Technologies**
Hotel employees in: • Marketing • Sales and Communication • Public Relations	Corporate documents and information Marketing information and e-brochures Personal work-related problems and solutions to others' work-related problems Transactive memory of who are the experts on particular topics	Guest Network (wifi Internet restricted to guests) Guest Network (Internet available in the Executive Lounge) USB + Offshore Microsites

Table 2: Work Systems Snapshot of Work Undertaken by Selected Ravine Employees

Discussion

Our case analysis indicates that employee subversion of the strict IT policy is common in Ravine. In scholarly research, the literature on employee resistance to managerially-imposed change is slowly growing, with new typologies of the various forms of resistance emerging (e.g. Lapointe and Rivard, 2005). Resistance often takes the form of employees refusing to use a new IS as it was designed to be used, either rejecting usage outright or modifying the way they use it so as to suit their needs. In more extreme cases, employees may deliberately try to damage or sabotage the same system.

However, the literature does not cover the situation where employees, far from resisting IT, instead demand more IT, resisting the IT policy that denies them access to needed IT applications. Such is the focus of the current paper, where we have examined how employees demonstrate a genuine need for specific IT applications, notably those often referred to as social media, as well as high levels of Internet bandwidth. Dissatisfied with the technology that management deigns to provide, employees actively subvert organisational IT policy by creating ways in which they can access their desired IT applications. This act of subversion entails elements of bricolage, i.e. leveraging whatever resources are available at hand. In this interpretive case study, we have explored the socially-driven world in which employees work and their consequent need for socially-enabling technologies.

Our findings are circumscribed by our context, a single hotel chain in China, but we would expect to see similar subversive behaviour in other Chinese hotels where restrictive IT policies are enacted. Our findings are particularly relevant for working professionals, notably those who work in such functions as public relations, marketing, sales and communications, who depend on social media applications as they engage in intensive communications with internal and external parties. We suggest that the phenomenon

of employees subverting organisational IT policies may be widespread in practice. It is likely to arise whenever the prevailing values and norms of the organisation differ from those of its employees.

The rapid entry of digital natives into the workforce (Basso, 2008; Shehadi et al., 2013; Chua et al., 2014) must also be accompanied by an infusion of new attitudes towards technology, particularly the notion of always being connected and online, where the border between social and work environments is miscible and fluid. As digital natives encounter organisations, and their cultures, that were created and are managed by people who are digital immigrants at best, digital dinosaurs at worst (Davison and Ou, 2014), so tensions can be expected to arise with respect to what kind of technology use is permitted and how employees should engage in communicative acts with internal and external stakeholders. Digital natives, just like some of Ravine's employees, are unlikely to take "No" for an answer, instead drawing on the tools and mind-set of the bricoleur who actively exploits repertoires of skills and resources, seeking to create solutions that meet immediate needs even if they subvert organisational control in the process.

Delving into how these acts of subversion occur is likely to be a fruitful topic for future research with significant relevance for organisations that hope to avoid the destructive consequences that runaway bricolage might bring. For instance, appreciating how subversive practices may not be deliberately destructive but instead represent a legitimate employee reaction to poorly designed systems and policies could provide a means of both resolving the tension and avoiding more serious consequences – if managers are willing to listen and modify their IT policies. In order to broaden the application of our findings, we now draw on our case study to elicit some of the theoretical factors that we suggest contribute to the IT-based subversion phenomenon.

In an investigation into how and why IT-based subversive acts occur, and consistent with Alter's (2013) Work Systems, issues in the broader social and organisational environment should be considered. For instance, behaviours that are considered culturally normal or accepted in the local social milieu may be taboo in the organisational context. It is also important to identify organisational strategies that influence IT governance and the associated IT-based infrastructure. In parallel with this assessment of the environment, we must consider the IT-related needs of the participants (employees) who engage with technology as they perform their work. These needs may relate both to work-related issues and personal issues, since digital natives do not readily distinguish between work and personal use of IT (Shehadi et al., 2013).

If there is a significant conflict between environmental and personal factors and if the individuals involved are sufficiently determined to obtain access to unavailable IT, then we should expect first to see resistance to the organisational IT policy. This initial resistance may take the form of attempts to negotiate with management. If the organisation is intransigent, then employees may take matters into their own hands and act as bricoleurs, subverting organisational IT policy by taking the necessary steps to secure access to the technologies that they believe are essential – whether for work or personal purposes. These steps could be characterised as a form of employee resilience in the face of adverse circumstances, with individual employees deploying and sharing their repertoires of skills and resources.

If the subversive acts are sufficiently low key, they may not be visible to or noticed by management, and so persist over long periods of time. Indeed, they may bring about the establishment of an informal shadow working environment that parallels the formal corporate environment. If on the other hand, the steps are too aggressive or include elements of wilful damage to organisational systems, then an organisational response must be expected with serious consequences for the perpetrators.

Conclusion

Employee subversion of organisational IT policy is not a topic that has received much attention from researchers. However, we suggest that this is a phenomenon that will become more salient as ever more digital natives enter the workforce and confront organisational cultures and values established under the aegis of senior managers accustomed to very different normative behaviours. Given the extent to which social media applications and other forms of IT are embedded into the lives of digital natives, it would be naïve to expect these same people to amputate integral parts of their lives and personalities: instead, we should expect them to fight to retain access to the same social media applications, whether for work or non-work purposes. Digitally fluent employees (Wang et al., 2013) have a considerable repertoire of resources and skills at hand to secure the optimal working environment, irrespective of organisational

policy or mandate. In this paper, we have explored how digital native employees in a Chinese hotel chain subvert a restrictive organisational IT policy, securing access to the resources they insist they need. We identify some theoretical components of the phenomenon that merit future investigation.

References

Alter, S. 2013. "Work Systems Theory: Overview of Core Concepts, Extensions, and Challenges for the Future", *Journal of the Association for Information Systems* (14:2), pp. 72-121.

Ansoff, I. 1988. *The New Corporate Strategy,* New York: John Wiley & Sons.

Avison, D.E., and Fitzgerald, G. 1995. *Information Systems Development: Methodologies, Techniques and Tools*. London: McGraw-Hill.

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change", *Psychological Review* (84:2), pp. 191-215.

Bartlett, C.A., and Ghoshal, S. 1998. *Managing Across Borders: The Transnational Solution*, Boston: Harvard Business School Press.

Basso, M. 2008. "2018: Digital Natives Grow Up and Rule the World", https://www.gartner.com/doc/733333/-digital-natives-grow-rule.

Bureau, S., and Zander, I. 2014. "Entrepreneurship as an Art of Subversion", *Scandinavian Journal of Management* (30:1), pp. 124-133.

Chua, C.E.H., Storey, V.C., and Chen, L.T. 2014. "Central IT or Shadow IT? Factors Shaping Users' Decision To Go Rogue with IT", *35th International Conference on Information Systems*, Auckland.

Cook, S.D.N., and Brown, J.S. 1999. "Bridging Epistemologies: The Generative Dance between Organizational Knowledge and Organizational Knowing", *Organization Science* (10:4), pp. 381-400.

Davison, R.M., and Ou, C.X.J. 2014. "Digital Work in a Pre-Digital Organizational Culture", *22nd European Conference on Information Systems*, Tel Aviv.

Davison, R.M., and Ou, C.X.J. 2013. "Sharing Knowledge in Technology Deficient Environments: Individual Workarounds amid Corporate Restrictions", *21st European Conference on Information Systems*, Utrecht.

Davison, R.M., Martinsons, M.G., and Ou, C.X.J. 2012. "The Roles of Theory in Canonical Action Research", *Management Information Systems Quarterly* (36:3), pp. 763-786.

DesAutels, P. 2011. "UGIS: Understanding the Nature of User-Generated Information Systems", *Business Horizons* (54:3), pp. 185-192.

Duymedjian, R., and Rüling, C.C. 2010. "Towards a Foundation of Bricolage in Organization and Management Theory", *Journal of Product Innovation Management* (31:2), pp. 133-151.

Griffin, R., and Lopez, Y. 2005. "Bad Behavior in Organizations: A Review and Typology for Future Research", *Journal of Management*, (31:6), pp. 988–1005.

Hirschman, A.O. 1970. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations and States*, Cambridge, MA: Harvard University Press.

Ignatiadis, I., and Nandhakumar, J. 2009. "The Effect of ERP System Workarounds on Organizational Control", *Scandinavian Journal of Information Systems* (21:2), pp. 59-90.

Jermier, J., Knights, D., and Nord, W. 1994. "Introduction: Resistance and Power in Organizations: Agency, Subjectivity and the Labor Process", in: Jermier, J., Knights, D., and Nord, W. (Eds) *Resistance and Power in Organizations*, London: Routledge, pp. 1-24.

Joshi, K. 1991. "A Model of Users' Perspective on Change: The Case of Information Systems Technology Implementation", *MIS Quarterly* (15:2), pp. 229-240.

Kling, R. 1996. *Computerization and Controversy: Value Conflicts and Social Choices* (2nd ed.), San Francisco: Morgan Kaufmann.

Klotz, A.C., and Buckley, M.R. 2013. "A Historical Perspective of Counterproductive Work Behavior Targeting the Organization", *Journal of Management History* (19:1), pp. 114-132.

Lapointe, L., and Rivard, S. 2005. "A Multilevel Model of Resistance to Information Technology Implementation", *MIS Quarterly* (29:3), pp. 461-491.

Levi-Strauss, C. 1966. *The Savage Mind*, Chicago: University of Chicago Press.

Markus, M.L. 1983. "Power, Politics and MIS Implementation", *Communications of the ACM* (26:6), pp. 430-444.

Orlikowski, W.J. 2000. "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations", *Organization Science* (11:4), pp. 404-428.

Piderit, S.K. 2000. "Rethinking Resistance and Recognizing Ambivalence: A Multidimensional View of Attitudes Towards an Organizational Change", *Academy of Management Review* (25:4), pp. 783-794.
Senyard, J., Baker, T., Steffens, P., and Davidsson, P. 2014. "Bricolage as a Path to Innovativeness for Resource-Constrained New Firms", *Journal of Product Innovation Management* (31:2), pp. 211-230.
Shehadi, R.T., Vollmer, C.A.H., and Karam, D. 2013. "Designing the Digital Workplace: Connectivity, Communication, Collaboration", http://www.strategyand.pwc.com/media/file/Strategyand_Designing-the-Digital-Workplace.pdf
Subramaniam, N., Nandhakumar, J., and Baptista, J. 2013. "Exploring Social Network Interactions in Enterprise Systems: The Role of Virtual Copresence", *Information Systems Journal* (23:6), pp. 475-499.
Tarafdar, M., D'Arcy, J., Turel, O., and Gupta, A. 2015a. "The Dark Side of Information Technology", *MIT Sloan Management Review* (56:2), pp. 600-623.
Tarafdar, M., Gupta, A., and Turel, O. 2015b. "Editorial: Special Issue on 'Dark Side of Information Technology Use': An Introduction and a Framework for Research", *Information Systems Journal* (25:3), pp. 161-170.
Turel, O., Serenko, A., and Giles, P. 2011. "Integrating Technology Addiction and Use: An Empirical Investigation of Online Auction Users", *MIS Quarterly* (35:4), pp. 1043-1061.
Vodanovich, S., Sundaram, D., and Myers, M.D. 2010. "Research Commentary – Digital Natives and Ubiquitous Information Systems", *Information Systems Research* (21:4), pp. 711-723.
Wang, E.Q., Myers, M.D., and Sundaram, D. 2013. "Digital Natives and Digital Immigrants: Towards a Model of Digital Fluency", *Business and Information Systems Engineering* (5:6), pp. 409-419.
Weatherbee, T.G. 2010. "Counterproductive Use of Technology at Work: Information & Communications Technologies and Cyberdeviancy", *Human Resource Management Journal* (20:1), pp. 35-44.
Weick, K.E. 1993. "The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster", *Administrative Science Quarterly* (38:4), pp. 628-652.
Weick, K.E. 1998. "Introductory Essay: Improvisation as a Mindset for Organizational Analysis", *Organization Science* (9:5), pp. 543-555.
Xue, L., Ray, G. and Gu, B. 2011. "Environmental Uncertainty and IT Infrastructure Governance: A Curvilinear Relationship", Information Systems Research (22:2), pp. 389-399.
Zuboff, S. 1988. *In the Age of the Smart Machine: The Future of Work and Power*, New York: Basic Books.