MIS Quarterly Executive

Volume 23 | Issue 4 Article 5

December 2024

Dealing Effectively with Shadow IT by Managing Both Cybersecurity and User Needs

Steffi Haag

Andreas Eckhardt

MIS Quarterly Executive

Dealing Effectively with Shadow IT by Managing Both Cybersecurity and User Needs

"Shadow IT"—information technology that is not endorsed by a company's cybersecurity policies—is proliferating. Shadow IT typically arises when employees either create their own IT or use unapproved third-party solutions. While shadow IT may be effective in helping workers tackle various challenges, the unsanctioned nature of shadow IT can also pose significant cybersecurity risks for organizations. This article identifies four archetypal practices for managing cybersecurity and user needs that encourage, or discourage, employees to use shadow IT. From these archetypes, we propose 10 recommendations to help IT leaders deal effectively with shadow IT—by both reducing associated cybersecurity threats and improving the user experience for workers.[1]

Steffi Haag
Heinrich Heine University Düsseldorf (Germany)

Andreas Eckhardt
University of Innsbruck (Austria)

The Cybersecurity Threat

A 2019 study found that most organizations across all major industries—including financial services, healthcare, high tech, manufacturing, legal, retail and the public sector—are using nearly 2,000 cloud services,[2] on average, with 90% of these services being adopted by employees without the approval or knowledge of the company's IT department. This use of technologies that are not endorsed by a company's cybersecurity policies is called "shadow IT."

For example, when using shadow IT, employees might organize project tasks using easily accessible tools like Trello, discuss company matters among themselves using WhatsApp, share large files effortlessly through services like Dropbox and collect ideas on virtual whiteboards like Mural to enhance teamwork. Shadow IT had already been observed in the 2000s as a means to circumvent legacy enterprise resource planning (ERP) systems.[3] However, with the recent rise in popularity of large language models (LLMs), such as those of OpenAI's ChatGPT, another big wave of shadow IT use in organizations is underway.[4]

1 Jeffrey Proudfoot is the senior accepting editor for this article.
2 *Cloud Adoption and Risk Report 2019*, McAfee, 2019, available at https://cloudsecurity.mcafee.com/cloud/en-us/forms/white-papers/wp-cloud-adoption-risk-report-2019-banner-cloud-mfe.html?source=MFE_Website&lsource=MFE_Website.
3 Scott, S. V. and Wagner, E. L. "Networks, Negotiations, and New Times: The Implementation of Enterprise Resource Planning into an Academic Administration," *Information and Organization* (13:4), October 2003, pp. 285-313.
4 Jackson, B. "How to Avoid Fueling 'Shadow AI' with the Right Policy for Generative AI Chatbots," *Forbes Technology Council*, 2023, available at https://www.forbes.com/sites/forbestechcouncil/2023/04/27/how-to-avoid-fueling-shadow-ai-with-the-right-policy-for-generative-ai-chatbots/.

DOI: 10.17705/2msqe.00104

Even though the motivations for using shadow IT are typically not malicious, the practice introduces various cybersecurity risks.[5] These include the potential for data loss and leaks, regulatory breaches (such as violations of the General Data Protection Regulation, or GDPR) and increased vulnerability to cyberattacks if sensitive corporate data is processed and stored on third-party servers. Additionally, shadow IT can lead to difficulties in data recovery, lack of integration with existing systems and the spread of malware and viruses.

Shadow IT thus represents an insider threat to a company's cybersecurity posture. Research suggests that one in five companies has faced a cybersecurity incident linked to shadow IT,[6] imposing an average cost of over $4.88 million in 2024.[7]

Managing shadow IT has long been a challenge for IT departments trying to monitor and control the tech tools used by employees. With so many new digital technologies that are easy to use and access, employees are increasingly drawn to shadow IT to help with day-to-day tasks. This reality makes full control over, or elimination of, shadow IT impossible. On the plus side, shadow IT can also increase employees' effectiveness.[8] This means that, when assessing cybersecurity risks to deal with shadow IT, the advantages that shadow IT may bring to a company should also be acknowledged.[9]

This article explains how IT leaders can balance the cybersecurity risks posed by shadow IT against its potential benefits. The insights described below are drawn from interviews conducted over more than three years; the interviews covered 44 employees at 34 companies situated in various industries who did, or did not, use shadow IT in response to their respective company's IT initiatives related to cybersecurity and user effectiveness. (For more on our research, please see the Appendix.)

By gathering insights from IT "users" (employees), we were able to analyze how site managers, compliance officers, project managers and Scrum coaches, for instance, perceived the actions of their IT departments and whether they responded with shadow IT use or not. This article thus:

- Identifies four archetypal practices of companies dealing with shadow IT. These cases differ in the actions companies took to manage cybersecurity and user needs, as well as in how users responded (or did not respond) regarding their use of shadow IT.
- Identifies two main shadow IT user groups: 1) goal-oriented actors (GOAs), who are characterized by their tech-savviness, cybersecurity expertise and their intentional use of shadow IT to accomplish tasks, while carefully considering and mitigating cybersecurity risks, and 2) followers, who mimic GOAs' use of shadow IT but often with a limited understanding of the cybersecurity implications.
- Proposes 10 recommendations to help IT leaders better deal with shadow IT.

Our research suggests that there is neither a universal solution for managing shadow IT nor can IT leaders fully control or eliminate shadow IT use. Instead, leaders need to find the right balance between the risks and benefits of shadow IT use for their organization. Finding the right balance for a given organization, in turn, requires a focus on and comprehensive management of users' needs in order to limit dissatisfaction and turnover among employees.

Four Archetypes for Dealing with Shadow IT

When we compared practices across interviewees and their organizations, four

5 Silic, M. and Back, A. "Shadow IT—A View from Behind the Curtain," *Computers and Security* (45), September 2014, pp. 274-283.

6 Orr, D. "Perception Gaps in Cyber Resilience: Where Are Your Blind Spots? The Hidden Risks of Shadow IT, Cloud and Cyber Insurance," *Forbes Insights*, 2019, available at https://www.forbes.com/forbes-insights/our-work/perception-gaps-in-cyber-resilience/.

7 *Cost of a Data Breach Report* 2024, Ponemon Institute, available at https://www.ibm.com/reports/data-breach.

8 Koch, H. et al. "How a Low-Margin Business Cocreated Analytics Value through an Innovation Partnership," *MIS Quarterly Executive* (18:3), September 2019, pp. 157-73; Kranz, J. et al. "Unexpected Benefits from a Shadow Environmental Management Information System," *MIS Quarterly Executive* (20:3), September 2021, pp. 235-356.

9 Note that established frameworks for cybersecurity risk assessments advise that risks be evaluated along with the costs and benefits of measures taken to mitigate these risks. See, e.g., *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, April 2018, available at https://www.nist.gov/cyberframework/csf-11-archive.

archetypes emerged for how companies deal with shadow IT and how users perceive and respond to companies' behavior. We found that an organization's measures for managing cybersecurity risks—as well as how the organization manages the IT needs of internal users—have a substantial impact on employees' shadow IT use.

Below, we describe each of the four archetypes along two dimensions: 1) the management of cybersecurity, which includes technical and organizational measures and their enforcement, and 2) the management of user needs, focusing on communication with users and responsiveness to their suggestions. Table 1 summarizes the four archetypes, the managerial actions organizations performed to deal with shadow IT and their impact on employees' shadow IT use.

Archetype 1: MP1

Company MP1 operates in the media industry,[10] specializing in the production of digital content for movies, television installations and visual effects. MP1 has offices across the U.S., Canada, China and Germany and employs nearly 500 people. The local German office, which we analyzed, has close to 80 employees. As a small or medium-sized enterprise, MP1 values flat hierarchies. Cost efficiency is also a significant concern for MP1, underscoring the company's dedication to optimizing the value and effectiveness of its IT resources and operations. The firm's primary IT infrastructure and systems are mandated by its U.S. headquarters, though some local flexibility is allowed to ensure compatibility.

Actions to Manage Cybersecurity Risk

Due to the highly sensitive nature of the produced media data, managing cybersecurity is crucial for MP1. Therefore, the firm has implemented and enforced robust technical and organizational cybersecurity measures to prevent the use of shadow IT.

Technical and Organizational Measures: MP1 puts strict technical restrictions in place. For instance, access to certain websites such as Facebook is blocked, USB ports are locked and the use of smartphones at the workplace is limited. The firm's global core tool, its production database system, is deeply integrated into all operations and the tool mandates specific operational procedures and automatically prevents unintended or malicious user behaviors. These stringent cybersecurity and data-processing regulations are primarily driven by client requirements and are verified through audits. Meeting these standards is crucial for customer acquisition, while failure to comply can lead to customer loss—and, ultimately, put the company's survival at risk. A site manager at MP1 told us:

> *"It is digital data we work with. Through digital communication tools, they can quickly be taken somewhere else, which must not happen, and, of course, we are very sensitive about that. We also have regular audits from clients who come and check what our security standard looks like. At the workplace, things like Facebook are blocked. It didn't work to just tell people not to use it."*

The company's cybersecurity policies are specified in the firm's employment contracts and are thoroughly explained to employees during the hiring process. Users are also aware of the non-disclosure agreements (NDAs) that they have signed and recognize the NDAs as a media-industry standard that ensures high data protection and security for the company.

Enforcement: MP1 enforces strict and severe sanctions for the use of shadow IT—any incident could spell disaster for the organization, including reputational damage, financial losses due to customer and contract churn, and/or liability for damages. Sanctions range from warnings to immediate termination, particularly if customers demand it. The same site manager added:

> *"Data [leak] is a huge disaster because, in the case of a movie, nobody wants anything to be shown beforehand. Once, the client demanded that the person be fired immediately. The one who was fired exchanged data in an insecure manner with an employee on the client side, who was then also fired. They exchanged stuff among themselves over Facebook."*

10 The names of all the companies referenced in this article have been anonymized.

Table 1: The Four Archetypes

Characteristics		MP1	GK2	DB3	MF4
No. of employees		500	35,000	400,000	20,000
Industry		Media	Manufacturing	Automotive	Automation/ technical education
Values and culture		Security, innovation	Entrepreneurship, market orientation, flexibility, hands-on approach	Control, rules and compliance, hierarchy, mistrust	Flexibility, trust, security
Organizations' actions					
Cybersecurity risk management	**Technical and organizational measures**	Strict technical and organizational restrictions. Awareness raised with employment at MP1 and in media industry.	Technical restrictions that are open for discussion and adaptation.	Strict technical and organizational restrictions dictated by IT department. Compliance monitoring and controls.	Minimal technical restrictions. Regular employee cybersecurity and privacy training and awareness.
	Enforcement	Strict, severe and certain sanctions.	Case-by-case basis. No strict sanctions if shadow IT use is deemed to be in GK2's interest.	Sanctions inconsistent and mild. Consequences incomprehensible or ridiculous.	Trust and responsibility delegated to employees. Severe sanctions expected only for deliberate negligence.
User needs management	**Communication**	Constantly seeking feedback on user needs. Encouragement and promotion of new IT proposals with non-monetary rewards. Explanations of failed/not-implementable requests and required restrictions, discussion of alternative solutions.	Active encouragement of questioning cybersecurity policies, discussing adjustments, proposing novel IT.	Minimal communication and coordination with users and their needs. Lack of service mindset. Technically unskilled and disinterested leaders.	Company suggestion program for novel ideas with financial participation. IT support.
	Responsiveness	Swift, agile, efficient responses to compete with dynamic market requirements.	Slow adaptation of cybersecurity policies and introduction of new IT solutions, unless top management has a pressing need.	Lengthy and rare IT implementation of projects. Inaccessible, unhelpful IT support.	Responsive IT department and support.
Employees' responses					
Shadow IT use		Very little	Occasional	Very frequent	None possible/ necessary

Actions to Manage User Needs

Communication: While MP1 enforces strict cybersecurity measures that limit users' actions, the company also actively encourages users to regularly provide feedback on their IT needs. The company then reviews such feedback carefully. In cases where a user request cannot be implemented, the company provides a detailed explanation of the decision and may propose alternative solutions. This approach is feasible due to the relatively small office and its flat organizational structure, allowing for direct communication and swift responses to user needs. Users are also recognized for innovative IT proposals. The site manager continued: "Those out there know much better what can improve their process than I do here at my desk. So that means suggestions are always welcome—and they do come."

Responsiveness: In addition to requiring high cybersecurity standards, the media industry demands that MP1 operates swiftly, agilely and efficiently, while continually innovating to utilize state-of-the art technology. To balance these demands, MP1 ensures that its official IT channels can quickly provide the IT resources and capabilities necessary for customer projects. This leads to high satisfaction among employees. For example, the site manager said:

> *"We use more in the company than I even use privately, so, in terms of features, there really isn't a wish left unfulfilled. Because we are in the media industry, we also quickly adopt any innovations and changes, so it's unlikely that we work with stuff that's 10 years old. We must be very agile and flexible to accept new things and continuously improve our workflows, also to keep up the speed. It's not like in a normal industrial operation."*

Shadow IT Use

The cybersecurity structures created by MP1 explicitly ban shadow IT and also serve as a significant deterrent to using shadow IT. At the same time, MP1 is open to the needs of users and involves them in IT implementation and/or restriction decisions. By striking a balance between strong cybersecurity and good user experience, MP1 reduces the use of shadow IT within the company to a minimum. In fact, only a few known instances of shadow IT use have occurred in over a decade at MP1. Both MP1 and its customers take these incidents very seriously. As the site manager explained:

> *"Unfortunately, there are people who don't read their contracts or don't listen, even if you tell them multiple times. In the 12 years I've been at [MP1], it [a shadow IT incident] has happened 2 or 3 times. They [those incidents] were not well received at all."*

Archetype 2: GK2

GK2 is a multinational building-materials manufacturer with 35,000 employees and a turnover of €11 billion. Our analysis focused on the company's headquarters in Germany. Although cybersecurity also plays an important role in GK2's decision-making, values such as entrepreneurship, market orientation and the courage to take risks are especially appreciated by the firm.

Actions to Manage Cybersecurity Risk

Technical and Organizational Measures: The firm's IT department determines the company's cybersecurity policies and permitted technologies; users are not granted administrator rights. Subject to the IT department's approval, users may request certain IT devices. BYOD (bring your own device) is not allowed due to security concerns. But the use of mobile devices for private purposes is permitted. Storage on USB drives is only allowed when encrypted.

These restrictions, however, contrast with GK2's explicit promotion of entrepreneurship, market orientation and flexibility to "workarounds" that help solve problems. Employees are also informed that they are responsible for their actions: There is an analysis of mistakes when things go wrong and recognition of success when objectives are achieved. As a senior legal counsel and compliance officer at GK2 told us:

> *"We are a company that very much has a hands-on approach. Entrepreneurship and the courage to take risks are among the company values and are truly lived out.*

There is only one [IT] barrier and that's administrator rights."

Enforcement: Government labor laws protect employees at GK2 from harsh penalties for negligent use of IT (though deliberate actions to inflict harm through the misuse of IT can lead to termination). At GK2, each use of shadow IT that is detected by the IT department is reviewed on a case-by-case basis. To date, no cybersecurity incident resulting from shadow IT use at the company has been detected. The senior legal counsel and compliance officer observed:

"There is a fundamental openness [at GK2] to a workaround. With every workaround comes a responsibility that one assumes as an employee. When we look at the culture, the values and symbols, such 'war stories' are part of the story of successful employees [at GK2]."

Actions to Manage User Needs

Communication: GK2 expects its IT policies to create friction, which is why its IT leaders encourage such policies to be questioned, regularly reviewed and, if necessary, adjusted. The firm's IT leaders also aim to make it easy for users to report issues and solicit support by phone or email. The senior legal counsel and compliance officer explained how GK2 tries to balance the aforementioned friction:

"There are a multitude of different interests within a company. Ideally, these balance out, but usually not right from the start. This is really the entrepreneurial company culture here—not to be completely scared off by formal [IT] hurdles. The discussions [for adjustments to IT policies] take place; one just has to initiate them."

Responsiveness: While the IT team remains open to feedback, potential cybersecurity policy adjustments take time to evaluate. Likewise, new IT proposals require thorough examination and approval, resulting in a lengthy implementation process that makes ad hoc solutions to user needs challenging. The situation is aggravated by the fact that the IT department struggles with organizational restructuring challenges—especially by prioritizing large implementation projects (such as ERP and cloud) over users' experience. However, the more urgent the issue, the quicker the IT team's response. The process can also be sped up if one offers something in return (such as legal advice) or if one is higher in the organizational hierarchy. For example, the senior legal counsel and compliance officer said:

"If you need something ad hoc, then you have difficulties getting it ad hoc. Not everything takes a long time. It's just a question of where you stand in the hierarchy. My strategy is just that the IT [department] needs something from me [in return] and that's the quid pro quo."

Shadow IT Use

At GK2, shadow IT is used as a workaround to get business done until issues are resolved. This is especially true in urgent situations, where delays from the IT department could result in mishaps like missing out on merger and acquisition deals. Unofficially, notes the senior legal counsel and compliance officer, GK2's IT team supports the workaround approach too:

"There were workarounds [with the iPad]—whether it was AirDrop, or even worse, essentially sending the documents via email from the company account on the iPad to the private account on the iPad. These were occasionally the unofficial, official, tips that one received."

Archetype 3: DB3

DB3 is an automotive supplier with 400,000 employees worldwide. The division we studied has over 2,000 employees and develops innovative systems and functions for vehicle safety and assistance systems. DB3, which is marked by a traditional hierarchical environment, faces various cultural challenges. For example, though the enterprise is rooted in a strong tradition of production leadership—one marked by industrialization, standardization and mechanical engineering—the division we evaluated primarily focuses on software development, which demands agility and frequent iterations.

Actions to Manage Cybersecurity Risk

Technical and Organizational Measures: To manage cybersecurity threats posed by shadow IT use, DB3 established stringent technical restrictions. For instance, administrative rights and USB access require a specific request—and are only granted briefly, if at all. In addition, a configuration and administration tool installed on every user laptop specifies not only which tools users can install but also performs regular, automatic, audits to ensure the approval and security of those tools.

However, these security requirements are often not well integrated with the rest of the firm's IT infrastructure. Though Internet Explorer, for example, is blocked, DB3's HR software nevertheless often requires access to Explorer. Meanwhile, the firm's standard development tools do not perform well with a permitted browser, Mozilla Firefox. Nevertheless, other browsers, like Chrome, are only available with admin rights.

There are other inconsistencies. Mobile phones, for instance, are banned to protect prototypes at test tracks, but this protection is only half-heartedly implemented. DB3 performs physical device controls at worksite entrances, including prohibiting the removal of laptops, USB sticks and other IT equipment without permission. "We just regulate everything and then one must work around it with permission or not," a DB3 Scrum coach told us.

During the period of our study, DB3 intensified its security measures—a move that reflects both the firm's growing concern about cybersecurity attacks and its declining trust in its employees. A project manager and team leader at the company observed: "The fear of all kinds of external attacks and also mistrust toward employees is increasing. [The IT department] practically snatches the mouse cursor from your hand and resets you."

Enforcement: In case of suspicious IT activity on a user's laptop, an alert from the central IT department is issued, prompting the user to initiate a device reinstallation. According to the Scrum coach, if a user fails to respond to subsequent follow-up requests, the user faces disconnection from the DB3 network:

> *"Last year, this completely pointless automated email popped up on my tool, telling me that my computer regularly pings a server that's on some blacklist. I then wanted to find out what is actually being pinged and by which tool or process. But I never got that answer [from the IT department] and then I thought, 'just ignore the whole thing.' Then came another request and another request. Eventually, they disconnected me from the [DB3] network."*

When DB3 deals with the unauthorized use or removal of a device, the incident is reported to the IT department leader, who often shows indifference or tacit approval of the action because of the many outdated and sometimes nonsensical rules (such as a total ban on photography on company grounds, including harmless photos of flowers outside buildings). As a result of this indifference or tacit approval, the offender might, at the most, get scolded. There is thus a wide gap, notes the project manager and team leader, between DB3's cybersecurity policies on paper and how the company actually applies them:

> *"They're now doing increased gate checks. If you then have something [that you're not supposed to have], they write it down and report it back to your department head. And they [the department heads] think, man, leave me alone."*

Actions to Manage User Needs

Communication: The central IT department at DB3 is known for trying to flex its authority by dictating guidelines on IT acquisitions, operations and policies in a heavy-handed manner. The department is also known for poor communication and coordination with users, for failing to address users' needs and for not facilitating user feedback.

Although DB3 is customer-centric when dealing with external (paying) customers, the central IT department violates this principle when serving internal "customers" (i.e., users of its IT). For example, the department often implements updates and restarts PCs through configuration access without first coordinating with users—a practice that greatly disrupts users' work. Although users typically understand the need to close critical security vulnerabilities, the

department's unilateral decision-making process often fosters an antagonistic relationship with users. And when the department does solicit user feedback, poorly designed surveys frequently fail to accurately gauge employee sentiment.

Further, despite the existence of a user platform for submitting ideas, suggestions are seldom addressed by the department. Employees often criticize the department for its outdated IT knowledge, penny-pinching and low creativity. For instance, the Scrum coach said:

> *"What I find most annoying about the central IT department is their [arrogant] attitude toward people: 'We make the rules and everyone has to follow them.' When you come with a problem, they say: 'It's not possible because our technical implementation is different and we also don't want to think about a different one.' People who want to drive things forward find [the department's behavior] immensely frustrating."*

DB3's challenges extend to its leadership structure, where senior executives—who tend to have production knowledge but lack IT experience—are responsible for overseeing the development of products that are now largely digital. This disconnect results in user needs being frequently overlooked—a problem that is compounded by such leaders' reluctance to learn from mistakes.

As a result, business-driven IT changes or new IT implementations only occur when prompted by user-driven escalation. And over the three-year period that we conducted our interviews, executives at the company made no noticeable strides toward improving their IT competency. For example, the project manager and team leader said:

> *"We are a company that is becoming more and more IT-oriented, but currently still have executives in most areas who have very little [IT savvy]. When one reports [IT problems], one is not so well regarded because the gentlemen [executives] don't know what they should do about it."*

Responsiveness: DB3's IT department has, as noted, earned a reputation for being unhelpful. Typically, support staff are only able to resolve trivial issues; more complex problems either take a long time to resolve or go unaddressed. To get anywhere, personal connections are also vital: Users are much more likely to receive timely help if they know someone in the central IT department. The Scrum coach laments: "You call their hotline and then someone in India or Eastern Europe answers and it's like playing roulette. Sometimes you're lucky and the person knows the topic. But most of the time, you're not lucky." On the occasions when new IT solutions are adopted, the roll-out period can be endless. And once solutions are adopted, notes the Scrum coach, they outlast their usefulness:

> *"You finally get to the point where they offer a tool as a service and then there's a big deal made with documents about everything the tool can do. At some point, it's [finally] set up, but then it's also the solution for the next 10 years."*

Shadow IT Use

Given the failings of DB3's authorized IT systems, it is no surprise that employees widely use shadow IT to get their jobs done. Examples of shadow IT use include employees taking photos with personal smartphones to document their work; using personal email accounts or third-party cloud services for transferring photos, notes and documents from personal devices to the corporate network and business computers; and developing work-task automations or time-tracking apps.

There is also a lively exchange of shadow IT solutions among technically skilled colleagues from various departments. For example, software development teams who invested significant effort in creating their own suite of shadow IT shared their tools on DB3's internal social media platforms. At times, local IT teams even suggest shadow IT solutions. The Scrum coach explained:

> *"A lot of things happen under the table. Last year we had an event. There was someone there from [another subsidiary] with whom I got into a conversation; we know each other from architecture stuff. And he says: 'I'm having some trouble with the proxy.' And I say, 'Oh yes, I can show you.' It's kind*

of like the black market for [exchanging] IT tricks."

In the long run, however, DB3's reliance on shadow IT solutions to compensate for the deficiencies of its official IT infrastructure is inefficient and a cause of discontent for users—especially shadow IT users. Indeed, over time, the latter struggle with the added burden of maintaining their own IT solutions on top of their regular duties. The upshot for DB3, notes the project manager and team leader, is increased employee turnover and disengagement:

"I don't have the energy anymore. I want this stuff to just work. It's very clear that we're losing people. I'm being restricted by everything possible. I don't even have my own admin rights on my computer. I just can't work the way I want to."

Archetype 4: MF4

MF4 is a provider of automation technology and equipment. With headquarters in Europe, the company has about 20,000 employees. The subsidiary we studied specializes in technical education, employs 900 people and generates revenue of €150 million. (Because of a recent merger that directed available resources to process integrations, digital transformation was not a core focus of the company's operational strategy at the time of our interviews.)

Actions to Manage Cybersecurity Risk

Technical and Organizational Measures: MF4 has a quasi-open IT policy. Users can receive full admin rights on request and can install any software they need to effectively carry out their work. Standard security programs run in the background to check for viruses, malware and spam.

Despite such openness, cybersecurity and privacy are key goals at the company; both the management board and the works council are actively involved in promoting these goals. Employees are made aware of security risks through regular training. Because MF4 provides programming software for automation technology, ensuring the security of the company's products is a critical aspect of the development process. A product manager at MF4 told us:

"On the company computer, everything is possible. We have the possibility to request administrator rights for three days. One could install any software that one needs. Of course, I look with common sense to see if the source is trustworthy. And I also trust the company's security measures."

Enforcement: By balancing security with flexibility, MF4 places its trust in the hands of employees, who, in turn, are accountable for their IT practices. Severe sanctions are reserved for cases of deliberate carelessness. To date, there have been no reports of misuse stemming from this freedom.

Actions to Manage User Needs

Communication: MF4 has a centralized IT support team to assist users around the globe with daily IT challenges—from straightforward issues to more complex problems. In addition, MF4 has a suggestion program where employees can submit new IT ideas. When a suggestion is submitted, the corresponding division head is alerted to review it and then either endorses it, rejects it or begins a discussion. If the suggestion is implemented and it creates a positive financial impact for the company, the employee who submitted the suggestion receives a percentage of the financial benefits.

Responsiveness: IT admin rights at the company are approved within just a few hours. Thanks to the freedoms granted to users, IT support is seldom needed. Ordering new IT hardware or devices online only requires the approval of the user's supervisor. On the other hand, the time it takes to implement ideas for new IT products submitted through the company's suggestion program can vary. A challenge for MF4 lies in channeling and prioritizing the many useful ideas it receives (which come from users in departments across the firm, including employees in the IT department itself).

Shadow IT Use

Because users are given (almost complete) free reign to explore new IT solutions, there is, by definition, no use of shadow IT at MF4.

Lessons from the Four Archetypes

The four archetypes described above show how organizations can influence the level of shadow IT. Actions that *reduce* the use of shadow IT are actions that acknowledge and strive to meet users' needs without compromising the firm's cybersecurity. However, actions that promote shadow IT use are actions that are perceived by employees to hinder their ability to work effectively by, for example, failing to provide the opportunity to seek timely changes and/or explanations through open communication with decision makers. In such cases, shadow IT becomes an escape route for employees, especially when the likelihood of detection for bypassing cybersecurity restrictions—and the sanctions for doing so—are low.

GOAs vs. Followers

However, as our research shows, not all users of shadow IT fit the same profile. Shadow IT users typically fall into one of two groups. "GOAs" (goal-oriented actors), the first group, are tech-savvy and cybersecurity-savvy and deliberately use shadow IT to perform their job duties more effectively. Another characteristic of GOAs is that they take special care to minimize cybersecurity risks to their employer (including by distinguishing between sensitive and less sensitive data). GOAs also tend to be amenable to restrictions on their IT use when they are provided with a reasonable rationale for the rules. Another trait of GOAs is that they actively contribute to solving the company's IT challenges by proactively communicating with their organization's IT department.

"Followers," the second group, simply mimic the shadow IT use of GOAs. Because followers understand cybersecurity poorly, they often are unaware that certain data or actions are not suitable for shadow IT use. Followers, in other words, pose a higher risk to companies.

Dealing effectively with shadow IT thus requires IT leaders to differentiate between the main types of shadow IT users. To identify GOAs, IT leaders should:

- Analyze identified shadow IT cases within the organization.
- Ask employees whom they contact for IT problems.
- Review user comments on internal communication platforms.
- Post comments about critical IT challenges on such platforms and see who responds.
- Conduct personality tests and skill-based interviews of employees.

In addition to having lots of IT and cybersecurity knowledge, GOAs (unlike followers) frequently display personality traits such as being goal-oriented, extroverted and risk-taking. These traits, in turn, can be assessed using tools like the Personal Innovativeness in Information Technology Scale and the psychometric Big Five Personality Test.[11]

Recommendations for Dealing with Shadow IT

Drawing on our research and analysis, the following 10 recommendations are designed to help organizations boost their cybersecurity and improve the effectiveness of their IT solutions for employees.

1. **Accept Shadow IT:** Much as they may try to, IT leaders cannot entirely control or eliminate the use of shadow IT. As new digital technologies emerge, some employees will inevitably find ways to use them at work—even if their company's IT policies prohibit it and restrictive measures are in place. However, IT leaders can manage the level of shadow IT use more effectively by implementing our remaining recommendations.
2. **Assess whether Shadow IT Threatens Business Continuity:** IT leaders should assess the cybersecurity threat that shadow IT poses to their company. Here, frameworks like the one articulated by the National Institute of Standards and Technology (which evaluates risk based on the likelihood of it occurring as well as its potential business impact) may be useful. If potential security incidents resulting from shadow IT use pose a

11 See, e.g., Cubillos-Pinilla, L. and Emmerling, F. "Taking the Chance! Interindividual Differences in Rule-Breaking," *PLoS ONE* (17:10), October 2022; Agarwal, R. and Prasad, J. "A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology," *Information Systems Research* (9:2), June 1998, 204-15.

threat to business continuity, actions should be taken to reduce shadow IT to the necessary minimum. However, if the business is likely to withstand such incidents, a somewhat higher level of shadow IT use may be desirable because the firm and its employees can benefit from the use of shadow IT.

3. **Select, Enforce and Adjust Cybersecurity Policies with Care:** Based on their cybersecurity risk assessment of shadow IT use, IT leaders should carefully design technical and organizational cybersecurity measures to counteract shadow IT use, while also weighing potential opportunity costs, especially in terms of gains in effectiveness. Leaders should only support and enforce cybersecurity policies that are truly necessary; if a violation has beneficial outcomes and will not be sanctioned, the cybersecurity policy should be revised. Though warnings and dismissals can serve as particularly effective deterrents against shadow IT use, leaders should not forget that enforcing sanctions is time- and effort-intensive.[12]
4. **Educate Users About Cybersecurity:** IT leaders should provide training to employees to improve their understanding of the organization's cybersecurity policies—including by discussing threats, restrictions, sanctions and why such policies benefit not only the organization but also users.[13] Our research shows that even employees who use shadow IT tend to be more careful and otherwise act in ways that align with the organization's goals when the cybersecurity policies are well understood by everyone.
5. **Ensure That Users Do Not Feel Blocked:** It is crucial that IT allows users to complete their work efficiently and effectively. When this does not happen, employees often attempt to use shadow IT—or leave the company altogether. IT leaders should therefore consider how every new restriction they introduce affects employees' ability to get their work done. If users are hindered in their work by cybersecurity policies that are deemed by leaders to be essential, leaders should still discuss the restrictions with users, explain the rationale for the restrictions and look for ways to find solutions that are more agreeable to users. If the organization decides to sacrifice some level of performance in exchange for adhering to a given cybersecurity policy, that decision should also be clearly communicated to users.
6. **Create a User Experience Team:** To minimize employees' use of shadow IT, managers should continuously consult with users about their needs and respond to those needs promptly. Such consultations and responsiveness require IT leaders to allocate adequate resources to the task. The best way to do this is to create a user experience (UX) team that focuses entirely on managing employees' IT needs. While IT support should continue to serve as the first contact point for ad hoc IT challenges, the UX team should be users' first stop for strategic and operational needs, including offering new IT suggestions. By creating a UX team, the IT department can proactively work with users to jointly improve the functionality, effectiveness and experience of internal IT and discuss potential conflicts with the company's cybersecurity policies.
7. **Leverage Chatbots:** When organizational resources are extra tight, well-designed chatbots can be leveraged to support IT and UX teams. Chatbots can help in various ways, including offering real-time IT support, collecting user feedback to guide IT decisions and development, and providing advice on cybersecurity policies. Although the chatbot's implementation, operation and maintenance also require significant cost and effort, such investment can pay off in the long run.
8. **Reward Shadow IT Use:** To bring shadow IT use in the company out into the open, IT leaders should announce that any user who deploys shadow IT in a way

12 Cram, W. A. et al. "Maximizing Employee Compliance with Cybersecurity Policies," *MIS Quarterly Executive* (19:3), September 2020, 183-98.
13 Ibid.

Table 2: The 44 Interviewees

		%
Age (years)	20-29 30-39 40-49	34.1 54.5 11.4
Gender	Female Male	25.0 75.0
Education	Higher professional education Bachelor's Other master's degree MBA	2.3 29.5 40.9 27.3
IT experience compared to peers (self-assessed)	Above average Average Below average	68.2 27.3 4.5
Cybersecurity experience compared to peers (self-assessed)	Above average Average Below average	65.9 31.8 2.3
Firm size	Large Medium Small	65.9 29.6 4.5
Industry	Automotive Aviation Chemical Consultancy Construction Education Finance Logistics Manufacturing Media Packaging Retail Telecommunication/IT	20.5 2.3 6.8 6.8 4.5 2.3 15.9 4.5 2.3 2.3 2.3 13.6 15.9
Interview channel	Face to face Video conference Telephone	27.3 63.6 9.1
Interview site	Home Public University Workplace	29.6 6.8 15.9 47.7

that creates measurable value for the organization will receive a reward. The reward can be financial or non-monetary (such as public praise in front of the entire firm).

9. **Manage GOAs and Followers Differently:** IT leaders should harness GOAs' IT expertise and ingenuity to benefit the company. For example, GOAs could be tasked with generating ideas for more effective IT and identifying cybersecurity polices that need revision. IT leaders should also make it clear that 1) GOAs (but not followers) will, for the

aforementioned reasons, be permitted certain deviations from cybersecurity policies, and 2) GOAs will still be held accountable for cybersecurity incidents that result from not adhering to minimum standards, such as legal regulations (e.g., GDPR), or from reckless experimentation. IT leaders should also remind GOAs that their behavior should befit their status as role models for potential followers.

10. **Embrace and Lead GOAs Effectively:** Finally, IT leaders should embrace the support that users offer—especially GOAs' deep understanding of specific domain problems and tasks. Users represent valuable IT resources that can aid in the exploration and implementation of new IT solutions, allowing the organization to redirect its limited IT resources to other critical tasks. With this mindset, IT departments should collaborate with colleagues from other departments, viewing them as an extension of their IT team. IT leaders should also focus on enhancing their leadership skills (by, for example, attending workshops) to master participative, transformational leadership techniques that foster the best user and cybersecurity experiences for their company.

Concluding Comments

IT leaders often have a good understanding of the cybersecurity risks associated with shadow IT use and can generally impose restrictions on IT use within the organization that address many of those risks. However, IT leaders tend to struggle at creating and implementing restrictions in ways that do not harm the user experience for employees. A suboptimal user experience is, in turn, why employees typically pursue shadow IT.

Fortunately, our research also shows that it is possible to align cybersecurity and user needs—and reduce the use of shadow IT—by prioritizing both effective communication with employees *and* transparent cybersecurity policies. We identified four organizational archetypes that illustrate how different approaches to pursuing cybersecurity and users' IT needs can result in very different levels of shadow IT use. Finally, we offered 10 recommendations that can help IT leaders manage shadow IT more effectively.

Appendix: Research Method

To understand how IT leaders can better deal with shadow IT, we conducted 73 semi-structured interviews, averaging about 55 minutes each, with 44 users employed at 34 organizations across 13 industries (see Table 2 for interviewee demographics). We ran multiple interviews with some of the same users to test and refine our findings. We also conducted the interviews face-to-face or via video/audio conference. Our goal was to uncover when and why shadow IT is used.

By gathering data from IT users over a period of 3+ years, we were able to identify patterns in users' behavioral responses to different organizational actions. Our data analysis followed established guidelines[14] for conducting an explanatory search for the causal mechanisms of shadow IT use.

First, we used open coding in NVivo to identify 53 shadow IT instances reported by 25 interviewees, the key themes among the organizational actions and users' responses associated with these shadow IT uses. Next, using abductive reasoning, we abstracted and hypothesized several action mechanisms that could explain the observed shadow IT uses. We then examined the relationships between these actions and how they might link together to cause shadow IT use (or the lack thereof). Lastly, we compared organizations' actions that either contributed to shadow IT use or helped reduce it in order to identify the aforementioned archetypes.

About the Authors

Steffi Haag

Steffi Haag is a Professor of Digital Innovation and Entrepreneurship at the Institute of Computer Science at Heinrich Heine University Düsseldorf, Germany. Her research examines tensions between managing digital innovation and cybersecurity, focusing on the user

14 Danermark, B. et al. *Explaining Society: Critical Realism in the Social Sciences (second edition)*, Routledge, 2019; Wynn, D. and Williams, C. K. "Principles for Conducting Critical Realist Case Study Research in Information Systems," *MIS Quarterly* (36:3), September 2012, pp. 787-810

perspective. Her work is published in leading IS journals, such as *MIS Quarterly* and *MIS Quarterly Executive*, and in top IS conferences (e.g., ICIS). She has received several awards, including a Schöller Fellowship and the 2017 Research Award in Data Protection and Data Security. She currently serves as an Associate Editor for *Business & Information Systems Engineering*.

Andreas Eckhardt

Andreas Eckhardt is a Professor of Information Systems at the University of Innsbruck. He received his Ph.D. in Information Systems from Goethe University Frankfurt. His research on opinion polarization, cybersecurity, ethical design, and the virtualization of organizations has been published in two books, several book chapters, and over 100 papers, in conference proceedings and scientific journals (including *MISQ*, *JIT*, *ISJ*, *JSIS*, *EJIS*, and *MISQE*). Currently, he is a Senior Editor for the ISJ and a member of the editorial board of *AIS Transactions on HCI* and of the AIS Diversity & Inclusion Committee..