MITSloan
Management Review

WINTER 2015

The Dark Side of Information Technology

In recent years, digital technologies have been transforming workplaces and increasing economic productivity. But could overuse of information technology now be sapping your employees' — and your organization's — well-being?

Monideepa Tarafdar
John D'Arcy
Ofir Turel
Ashish Gupta

Vol. 56, No. 2 | Reprint #56221 | http://mitsmr.com/1wD3N7E

The Dark Side of Information Technology

In recent years, digital technologies have been transforming workplaces and increasing economic productivity. But could overuse of information technology now be sapping your employees' — and your organization's — well-being?

BY MONIDEEPA TARAFDAR, JOHN D'ARCY, OFIR TUREL AND ASHISH GUPTA

?

THE LEADING QUESTION

Is excessive use of digital technologies hurting your company?

FINDINGS

- **The more relentlessly organizations embrace IT, the more "techno-stress" their employees suffer.**
- **Many employees experience addiction-like symptoms related to mobile email use: They check email at home, on weekends and on vacation.**
- **There are steps executives can take to counter the negative effects of IT use.**

INFORMATION TECHNOLOGY has long been viewed as the power behind a new economic revolution — an evolving set of tools that has made workers much more productive than ever before, powering a step change as dramatic as steam or electricity. According to a report by the World Economic Forum, "digitization boosted world economic output by nearly US$200 billion and created 6 million jobs in 2011."[1] On a company-by-company basis, a number of studies have found that companies that use more IT have higher productivity than their competitors.[2] However, we may be entering an era in which human frailties begin to slow down progress from digital technologies. In a series of studies, we explored the implications of IT-induced technology stress, technology addiction and IT misuse in the workplace. (See "About the Research," p. 62.) One implication of our findings is that the very qualities that make IT useful — reliability, portability, user-friendliness and fast processing — may also be undermining employee productivity, innovation and well-being.

After observing a number of organizations, we found that this rapidly emerging "dark side" of IT hurts employees and their organizations and robs companies of some of the productivity gains they expect from their IT investments. In this article, we describe key negative effects of IT use in the workplace, explain the risks they pose, and suggest ways managers can mitigate their impact.

ABOUT THE RESEARCH

This article draws on 14 studies that one or more of the authors worked on, published from 2007 to 2014.[i] For simplicity's sake, we refer to these studies as "our" studies when one or more of us was involved, even when we had other coauthors. We collectively studied more than 3,100 organizational employees and IT users covering 28 organizations in the United States, from sectors such as health care, industrial sales, manufacturing, higher education and government services. Our studies are among the earliest to explore the workplace implications of IT-induced stress, technology addiction and deviant IT misuse behaviors. Interview/qualitative data were analyzed using qualitative content analysis. Multivariate statistical techniques to analyze the statistical data included confirmatory factor analysis to develop and validate the measurement scales for various constructs and structural equation modeling to analyze relationships among them.

The Effects of "Technostress"

Pervasive and near-continual use of organizational IT systems is now beginning to take a toll on some employees' health. Individuals experience "IT use-induced stress" or "technostress" for a number of reasons.[3] They feel forced to multitask rapidly on simultaneous streams of information from different devices simply because information feeds come at them in real time; remote work and flextime tether them round the clock to their devices and workplaces; and short technology cycles and pressures from IT vendors mean constantly changing interfaces, screens and functionalities, often without sufficient FAQs and help-desk support. We also found in a survey of about 600 computer-using professionals that 73% worried that refraining from constant connectivity and instantaneous information-feed response would place them at a disadvantage at work.[4]

Complex user interfaces that do not naturally fit with task workflows are an additional source of stress, because they create work overload when they are used. In studying the use of a health-care IT application in the context of care delivery processes in acute care facilities at two major hospitals, we found that physicians had to juggle between numerous different screens on their monitors to access patient data feeds, test results, clinical notes and treatment notes.[5] Most of the doctors complained that they had to do far more work using IT than they thought reasonable. Often, we find that the more enthusiastically and relentlessly organizations embrace IT, the more technostress their employees suffer.

Ironically, even as they dream of escaping from IT, many employees also confess to feeling "addicted"[6] to some of these stress-causing technologies. In a study of organizational mobile email users,[7] we found that 46% exhibited medium to high addiction-like symptoms. On the one hand, they take their work home: Employees spent time responding to work emails when at home (23 minutes on average per day), while commuting (12 minutes), each weekend day (42 minutes) and each vacation day (43 minutes). On the other hand, IT also allows employees to take their leisure-time activities to work (for example, using Facebook). Even when an organization blocks certain websites, the sites can still be accessed via personal mobile devices, especially now, as the bring-your-own-device-to-work trend continues to grow.

As with many addictions, the desire for stimulation becomes progressively harder to satisfy, and over time individuals often seek more ways to "up their dosage." A remarkable example of the effects of nonwork IT on the workplace is the popularity of the Candy Crush Saga online game. One survey found that 30% of its players called themselves "addicted" to the game, and 28% admitted to playing it at work.[8] One person confessed to "going to bed late, as I do 'just one more,' over and over. It seems everyone at work is also addicted. We need a Candy Crush anonymous group…"[9]

Employee Misuse of IT

Another aspect of the dark side of IT is the threat of employees misusing organizational IT resources and triggering "attacks" of different kinds. Firewalls and other network defenses can potentially stop attacks from the outside. However, no security technology can stop an employee who has authorized access to a computer system from, for example, obtaining confidential company information and selling it to competitors. A number of studies have found that attacks stemming from internal sources are greater in scope and severity and can result in about 10 times as many compromised records as those from external sources. Even more disturbingly, a sizeable percentage of such attacks turn out to be deliberate.[10] Other kinds of insider IT misuse range from truly malicious user behavior (such as stealing sensitive corporate data) to unsanctioned behavior (such as accessing unauthorized parts of a corporate network or knowingly using unlicensed software) to naive user actions such as opening an unknown email attachment. Unsanctioned and naive user behaviors make up the vast majority of IT misuses.

Perhaps the most common motivation for IT misuse by an employee, ironically, is a desire to be more effective. We presented respondents with the following scenario and asked them if they would engage in the same behavior under similar circumstances:

> *Jordan is given a personal computer (PC) at work. However, the new PC is missing a piece of software that Jordan believes would make her more efficient and effective on the job. Jordan requests that the company purchase the software, but her request is denied. To solve the problem, Jordan obtains a copy of the software from a friend outside of the company and installs the software on her PC at work.*

Of 269 professionals, 45% indicated at least a medium likelihood (those with a score of 4 or greater on a scale of 1 "strongly disagree" to 7 "strongly agree") that they would engage in the same behavior in their own companies given the same circumstances. The percentage jumped to 50% when respondents were asked how their coworkers would behave.[11]

A slightly weaker but still significant motivation for technology misuse is the desire to help others. Our research suggests that even as employees understand that such behavior violates organizational policy, they view it as innocuous. We presented this scenario to respondents:

> *Alex is an employee in the human resources department at your organization and thus has been authorized to view the salary information of all employees as part of his job functions. Recently, one of Alex's friends (who does not work for your organization) contacted Alex and asked for the salary information of all managers in your organization. The friend informed Alex that he was applying for a management position in your organization and wanted to use the information to determine what salary to ask for in case he is offered the position. Although Alex believes that providing the salary information is a violation of company policy, he looks it up and gives it to the friend.*

Thirty percent of professionals surveyed indicated at least a medium likelihood (those with a score of 4 or greater on a scale of 1 "strongly disagree" to 7 "strongly agree") that they might engage in similar behavior. The percentage jumped to 40% when respondents were asked whether their coworkers would do it. Unfortunately, such uses are difficult to combat: IT use requirements such as creating hard-to-guess passwords and blocking access to certain websites and cloud-based storage services such as Dropbox are seen as constraining and are *themselves* a form of stress that encourages IT misuse. In this same study, we found that respondents who felt that security policies in their organizations were complex, burdensome and stressful were significantly more likely to try to justify their misuse of IT.[12]

Why Senior Leaders Should Care

Why should senior executives care about these issues? First, they pose serious risks to productivity and innovation. The more time and effort employees spend keeping abreast of ever-changing applications, struggling through information gluts, trying to understand how best to navigate through and use IT, and making mistakes, the less time they have for the job their IT tools are intended to support. More ominously, the rush to respond to incoming information causes employees to process, hastily and ineffectively, only that information which is *immediately available*, rather than wait for the information they actually need to do the job. Such an approach can stymie innovation, which often requires unhurried and thoughtful processing of relevant, varied and, as far as possible, reasonably complete information. The distraction posed by IT use and its accompanying flow of incoming information also seems to interfere with relationship building — another potentially serious consequence, as many service-oriented jobs include both technology-enabled and relationship-oriented workflows. In a study of senior and middle managers in professional sales roles, we found that the effects of IT-induced stress are far-reaching enough to reduce innovation and productivity in *both* types of workflows.[13] In other words, the more IT employees used, the less effective they were. We often heard statements like "Those of us who achieve our sales quota use less IT and are less stressed."

Second, excessive IT use can harm employee well-being. We found instances where employees actually resigned because they found it too stressful to cope with and learn to use constantly changing workflows/applications. In two separate studies, one on stress from common workflow applications such as enterprise systems and email and another on addiction to mobile devices/email, we found that each correlated with higher employee desire to leave the job and reduced organizational commitment.[14] IT use-induced stress from work-related IT use was also associated with lower overall satisfaction with the job.

Third, there are monetary and reputational risks. IT misuse has financial ramifications for organizations. Employee IT misuse may in some cases provide grounds for litigation; an early example is the energy company Chevron Corporation, which was ordered in 1995 to pay female employees $2.2 million to settle a sexual harassment lawsuit stemming in part from inappropriate email circulated by employees.[15] Public disclosure of problems caused by employee or contractor IT use can also cause negative publicity and competitive disadvantage to a company. For example, the retailer Target Corp., based in Minneapolis, Minnesota, experienced a high-profile Thanksgiving season data breach in 2013, which has been attributed to a credentials theft that took place through a phishing email sent to a Target vendor.[16] The data breach led to the resignation of both Target's chief information officer and chief executive officer.[17]

A fourth risk is to the technical integrity and operational viability of the corporate IT system. Certain forms of addiction, such as visiting websites that host online gambling activities or pornography, are magnets for malware infections. Organizationally unsanctioned but seemingly mild IT misbehaviors such as using unlicensed software, downloading email attachments or sharing passwords with coworkers and sensitive information with nonemployees can put the organization's data and systems at risk. IT misuse also has operational costs. Unlicensed software usage can lead to significant user downtime, and sending or receiving email/phishing viruses can cause system downtime. Password-sharing practices undermine the effectiveness of technical access control measures while compromising audit trails and accountability. Employees who are addicted to social media sites may post sensitive company information that they are not permitted to share with outsiders. Seemingly innocuous actions such as sharing company news (for example, a new product or patent) on a social networking site such as LinkedIn can assist hackers or other unscrupulous individuals in stealing a company's intellectual property. And even when secrets aren't spilled, a lot of time is stolen: In our research, we found that employees who find it difficult to control their use of social networking websites such as Facebook may spend time on these sites at the expense of time on task. They may take longer breaks, miss deadlines, be reckless with confidential information and neglect organizational IT use policies.

Finally, there are legal risks. If certain legal conditions are met — such as clear breach of duty by the organization in, for example, not adequately disclosing the potential for IT addiction and the presence of potential damage for the employee — it may be possible for Internet-addicted employees to argue that employers are liable, leaving the organization vulnerable to employee lawsuits. Indeed, there has been some effort to establish Internet addiction as a disability, regardless of its origin and cause.[18] As the CIO of one major enterprise told us: "As society moves in a greater manner to technical intermediation, the impacts [of technology-related addictions] to employees are critical. ... [Employers] should be cautious regarding work-life balance. … It may turn to litigious issues." Organizations may also have to deal with the hassle of possible litigation on privacy violations and sexual harassment from rash and compulsive use of applications such as social media at work, but not for work, by technology-addicted employees.

Resisting the Dark Side

Organizations have traditionally taken primarily *technical* approaches to helping their employees use IT. These have consisted largely of routine, mostly one-time and one-size-fits-all technical training activities where employees go through material on how and when they can use features of particular systems. We find, however, that the interaction between employees and IT is beginning to increasingly consist of a continual stream of use of different types of IT (for example, applications on both mobile and fixed devices) in addition to specific periods of use of a particular application. This kind of multimodal use demands a multimodal response by senior executives, IT leaders and HR leaders to effectively combat impacts from IT's dark side. (See "Tackling the Dark Side of IT.") In particular, we suggest that managers go beyond technology-oriented solutions and encourage employees to step back and examine their personal *relationship* with IT.

What Senior Executives Can Do Our research on employee-initiated security breaches shows that top management attitudes are a critical element in promoting pro-security behaviors such as safe computing practices to coworkers.[19] "Top management should be committed to making security a function of business processes" was a recurrent theme in our interviews. As one respondent said, "The senior leadership provides the example of our security culture."

Second, company leaders should empower employees to be circumspect and mindful about how they use IT and about its potential good *and* bad impacts. This is perhaps a departure from and certainly a complement to typical current leadership mindsets that focus singularly on the benefits of IT use. Senior leadership should encourage employees to reflect on not only how they use IT *from* or at work, but *for* work, from *anywhere*. More than 65% of

TACKLING THE DARK SIDE OF IT

Taking on the dark side of IT requires a three-pronged approach that involves not only a company's IT leaders but also its senior executives and HR leaders.

THREE-PRONGED APPROACH FOR TAKING ON IT'S DARK SIDE	
Senior leadership should make mindful use of IT an organizational priority.	•Make the organization aware of the negative impacts of IT's "dark side." •Develop strategic plans (relating to IT-use policies, employee development and electronic countermeasures) for identifying and mitigating dark-side risks associated with the use of IT. •Commit resources for campaigns/events such as email-free weekday afternoons or IT addiction-awareness days. •Incentivize employees to find out how best they can use IT by experimenting with features and use strategies. •Lead by example by showing, for instance, how senior leaders limit unnecessary and less urgent use of IT beyond working hours or adhere to IT security policies, procedures and guidelines themselves.
IT leaders should build and maintain vigilance against IT's dark side.	•Drive formal and informal learning about IT. Conduct forums and brown-bag events for people to share stories about how they actually use IT — in both positive and negative ways. •Provide ongoing technical and general support (rather than one-time training) to employees for applications they use. •Build dark-side resistant technical features into IT applications and infrastructure, such as blocking potentially addictive applications. •Design and implement IT-use policies that help people self-regulate their use of IT, such as email management and dashboard-based self-tracking. •Engage users in the design and implementation of IT-use policies that foster awareness and action regarding the dark side of IT. •Design and implement "persuasive" IT systems that guide users to effectively use IT.
HR leaders should monitor and enhance employees' well- being.	•Implement HR programs that monitor and measure whether employees experience dark-side IT-use effects. •Implement initiatives that foster positive job-related attitudes, recognizing that they can help thwart addiction, stress and IT misuse. •Design and implement employee development programs that encourage responsible IT use. •Encourage and provide training resources for employees to maintain work-life-technology balance. •Create depositories of external and internal resources (programs and centers that help with IT addiction, overload and stress) that employees can draw upon.

employees we asked reported feeling stressed from the work-home blurring and invasive effects of work IT. However, the rather common idea that older employees feel stressed from "technology insecurity" because they cannot keep up with the constant waves of new digital technologies that organizations introduce appears to something of a myth. Indeed, we found older employees to be on average 15% to 20% less stressed than younger employees, possibly because they are able to marshal experience and knowledge of their work and organizational context in order to engage in more *informed* use of IT — such as, for example, not allowing themselves to be interrupted by their cellphones unless the message concerns a higher priority. Leaders should organize and promote "mindful technology use" events and practices such as "email-free" weekday afternoons. If they don't, it's possible that the labor lobby will start demanding such practices. Interestingly, a major labor agreement in France recently moved to outlaw certain employees' responding to email message outside of normal work hours, and there are some similar efforts being considered in Germany.[20] While that may not be something that all organizations want or should ask for, it does suggest rising concern among union leaders and policy makers about the potentially harmful effects of excessive IT usage on employee well-being.

Third, leaders should create a climate that encourages employees to *really* understand the IT they use at work. When faced with IT applications having more functionality than is needed, many respondents said they either "switch off" or "use the bare minimum information to look good," both of which they thought hindered the effectiveness of their IT use. We find that this mastery of IT is often best achieved by giving employees the resources to "mess around" and experiment with the devices and applications. Users need to learn in less formal and more enriching ways, outside the structured and often limited training paradigm. Once they "speak" the language of the application, employees tend to be less overwhelmed by excessive features or distracted by glitzy ones.

What IT Leaders Can Do Given their natural domains of expertise, IT leaders have a special responsibility to instruct the organization about pertinent aspects of IT systems and applications that could either exacerbate or mitigate their darker effects. One of our studies showed that a simple educational video on the risks of Internet overuse significantly increased the motivation of users to control and reduce Internet use.[21] IT leaders should provide forums, such as brown-bag meetings, for employees to discuss and share their IT-related experiences, challenges and remedies with colleagues. Users of enterprise systems, for instance, in spite of training on how to navigate screens for standard workflows, often find it a stressful experience to extract information and build the custom reports they actually need. Sharing stories with others who have been able to do so reduces some of that stress: Employees whose companies encouraged them to share experiences and learning with new applications reported 20% lower stress levels than those in organizations that did not. In studying the use of electronic health record systems by doctors and medical staff, we found that those who continued to learn about IT features informally from one another were better able to counter the effects of stress. Employees' propensity to misuse IT resources was about 40% lower in organizations where IT leaders made an effort to deliver ongoing security education and training.[22] Efforts to inform and educate users on the potential risks of IT can likewise reduce the incidence of naive misuse behaviors such as opening an unknown email attachment or accidental data entry. The key is to inject information that alerts employees to the negative effects of IT usage and encourages them to explore these topics on their own and with others if necessary.

Traditional IT training programs, which are mostly one-time exercises (unless employees specifically request otherwise) delivered face-to-face or electronically and focusing largely on how to use common application features, are able to address only part of employees' training needs. For most applications, employees need to understand how to combine and use features and functions in nonstandard ways to fit their particular tasks and activities. Learning to use the system for nonstandard uses typically entails a process of tinkering to find features, workarounds and shortcuts that work, which may be different for different people.

“One of our studies showed that a simple educational video on the risks of Internet overuse significantly increased the motivation of users to control and reduce Internet use. IT leaders should provide forums, such as brown-bag meetings, for employees to discuss and share their IT-related experiences.”

In one of our studies, we found hospital physicians and staff felt stressed when patient charts became accessible on their mobile devices because they felt pressured to respond whenever they heard the device alert from a new or changed chart. The physicians and staff then worked through the application and learned how to create their own work practices; some turned to the IT department to help them turn off the immediate alarm notification and create one at a different time more conducive to their schedules, which helped ease the stress. Rather than keep installing systems and tossing them over to users, IT leaders need to remain engaged with users for significantly longer periods after implementing a system. They especially need to let employees know about features such as email archiving that can potentially counter or offset impacts such as information overload. We found that employees who felt informed and involved reported 10% to 15% lower stress while using IT.

Of course, technical guardrails must still play a role in curbing IT misuse. IT leaders can create an environment that keeps the organization vigilant to and, to some extent, safe from the dark-side effects on a day-to-day basis. We found that the more employees know about specific security-related countermeasures, the more they are inclined to abide by security policies and procedures.[23] Such countermeasures include, for instance, blocking technologies to address workplace addiction to IT and technical controls for tackling IT misuse, such as multiple levels of authentication and disabling access to USB ports where necessary. Engaging employees in the design and implementation of such countermeasures can help increase compliance and reduce misuse. Another way to improve productivity is to streamline systems to mirror workflows of key groups of IT users. We asked 169 physicians in one of our studies to use a simpler interface with fewer screens over a period of 40 weeks that covered about 1,300 patients. By the end of the trial, all of them reported less time spent using the IT application.[24]

IT leaders can also develop what are called “persuasive” systems[25] that “nudge” users towards more effective IT use. Giving users different prebuilt options regarding how they should process interruptions from, for instance, work-related email or social media information could guide them in addressing interruptions meaningfully. We found in further studies that designing simple prioritizing heuristics into IT applications based on importance and source of interruption messages led to a 39% reduction in the time that physicians spent in handling simultaneous information from multiple sources. We find that such real-time feedback also helps employees to reduce errors from IT-related overload,[26] as the persuasion can be directed towards corrective suggestions *in the moment of use* — provided, of course, that the feedback itself is not intrusive and does not cause information overload.[27] IT leaders could also commission the design and rollout of simple dashboard applications that track the timing, extent and type of IT-use activities during and after working hours. Employees can use this sort of information to help decide for themselves when their IT use is becoming a problem.

Finally, IT leaders can develop and implement IT-use policies that clearly define appropriate use and forbid the misuse of the company’s IT resources. It is important, however, that these policies be understandable and not a significant hindrance to employees’ normal job duties, or else they risk becoming an additional source of stress. For example, such policies should clearly explain technical requirements of IT use for nontechnical employees. Most technology-use policies are limited to specifying how employees may use specific IT resources such as shared printing and scanning equipment and services. These use policies should also alert employees to — and deter them from — the risks posed by technology addiction. Such policies also provide legal protection for organizations, because by developing and implementing them, organizations can demonstrate that they did not breach their duty to their employees.

What HR Leaders Can Do HR leaders have perhaps the most significant role to play in combating the dark-side effects of IT. The first issue that HR leaders face is assessing the extent of the dark-side effects of technostress or technology addiction that their organization may be facing. The difficulty here is that these sorts of phenomena are not easily quantified. For instance, a number of our study respondents mentioned that they were "stressed" by or "fed up" with constant upgrades to software in their workplaces, but they were not able to pinpoint what made them stressed and how their performance or well-being at work suffered as a result. HR leaders should work together with IT leaders to create programs and audit exercises to regularly measure and monitor the extent to which employees are plagued by these effects and are less productive, innovative or effective as a result. (See "Signs of IT's Dark Side.")

A second issue for HR executives is improving employees' sense of well-being at work. Stress and addiction diminish indicators of well-being such as job satisfaction, clarity of work expectations and work-life balance. Our findings imply that internal company policies such as limiting IT use after working hours, monitoring use and providing warning signs when improper/excessive use is detected, and training employees regarding the various risks associated with the improper/excessive use of technologies at the workplace and beyond can help reduce stress and addiction. Circulating information on external help and resources can also have a positive impact. At the same time, our research indicates that being unhappy at work leads to more improper security-related behaviors. Research on organizational behavior also suggests that general moods on a particular day influence whether or not employees comply with security policies, as does a higher level of job satisfaction.[28] HR initiatives such as job

SIGNS OF IT'S DARK SIDE

Productivity and well-being problems from IT use tend to increase under the following conditions.

Conditions that create stress from IT use ("technostress")	•Employees are forced by IT to work to tight schedules. •IT forces employees to be in touch with work around the clock. •Employees face constant IT changes and upgrades. •Employees' personal life is invaded by organizational IT. •Employees spend undue time and effort to understand and use IT. •Employees feel a constant need to update their IT skills for job security. •Employees must change their work practices and task workflows to adapt to new IT. •Employees must work with a multitude of IT systems to complete their job duties. •Employees find it mentally taxing to use IT systems.
Conditions that indicate IT misuse	•Employees share or write down passwords. •Employees use unapproved devices, such as personal USB sticks. •Employees fail to lock/log off their computers when not using them. •Employees share sensitive information with nonemployees. •Employees download and/or install untrusted programs. •Employees access unauthorized parts of the corporate network. •Employees intentionally circumvent technical controls, such as those that block access to certain websites and cloud-based services.
Conditions that indicate addiction to IT (for example, excessive use of mobile devices, Internet browsing)	•Employee performance suffers because of constant and needless IT use. •Employees are consistently preoccupied with using IT. •Employees find it difficult to stop using IT, whether or not it is required. •Employees neglect daily job duties because of being on the Internet. •Employees become restless, frustrated, irritated or agitated when unable to access and use IT.

enrichment programs that contribute to job satisfaction should positively influence security behavior. Mood-management strategies, such as fostering a positive work environment, helping employees find meaning in their work and offering a pleasant physical work environment, among others, should also help reduce IT misuse.

Third, HR leaders need to consider tailoring organizational policies regarding IT use to individual-specific traits. *Why does A take so long to answer email while B does not?* was an oft-repeated sentiment we came across. We found in a study with 129 professionals[29] that those more naturally inclined toward multitasking[30] respond relatively closer to real time to interruptions from different devices they carry. HR leaders should make employees aware of these sorts of differences and their implications for how they might expect colleagues to use IT, such as how quickly they answer email. Such actions can help employees develop a healthy understanding and tolerance for the different kinds of IT use their colleagues might engage in. We also found that certain personality traits such as neuroticism make employees more prone toward deviant IT misuse behaviors.[31] Although these characteristics are not readily observable, they can become apparent over time, and HR leaders might need to consider whether specific kinds of individual characteristics should be taken into account when matching employees to positions that involve sensitive data.

Lastly, in extreme cases, HR leaders will increasingly face the prospect of having to decide on alternate and complex courses of action (organizational, legal and medical) to deal with deviant IT use, stress and addiction. They may need to weigh the cost of terminating employees who are repeatedly caught in misuse or addictive use of their company's IT systems versus possibly helping them with rehabilitation. There are a number of treatment centers for Internet addiction, and given the potential legal issues that might arise from a dismissal, companies in some cases may be better off funding rehabilitation than pursuing organizational and/or legal sanctions.

Organizations invest in IT because they expect to boost their efficiency. The dark-side phenomena that we address in this article instead diminish productivity and innovation. Fortunately, a holistic and integrated approach by senior executives, IT leaders and HR leaders can help mitigate the most damaging consequences.

Monideepa Tarafdar *is a professor of information systems and a codirector of the HighWire Doctoral Training Centre at Lancaster University in Lancaster, United Kingdom.* ***John D'Arcy*** *is an assistant professor of management information systems at the Alfred Lerner College of Business and Economics at the University of Delaware in Newark, Delaware.* ***Ofir Turel*** *is a professor of information systems and decision sciences at the College of Business and Economics at California State University, Fullerton as well as a scholar in residence in the department of psychology at the University of Southern California in Los Angeles.* ***Ashish Gupta*** *is an associate professor of analytics and information systems in the College of Business and director of the Big Data and Analytics Research Center at the University of Tennessee Chattanooga. Comment on this article at http://sloanreview.mit.edu/x/56221, or contact the authors at smrfeedback@mit.edu.*

REFERENCES

1. B. Bilbao-Osorio, S. Dutta and B. Lanvin, eds., "The Global Information Technology Report 2013" (Geneva, Switzerland: World Economic Forum, 2013), vii.

2. E. Brynjolfsson and L.M. Hitt, "Computing Productivity: Firm-Level Evidence," Review of Economics and Statistics 85, no. 4 (November 2003): 793-808; and E. Brynjolfsson and A. McAfee, "The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies" (New York: W.W. Norton & Co., 2014), 98-106.

3. While stress due to IT use in the workplace is an emerging phenomenon, workplace stress due to organizational roles and tasks is well-known; see, for example, R. Kahn and P. Byosiere, "Stress in Organizations" in "Handbook of Industrial and Organizational Psychology," vol. 3, 2nd ed., ed. M.D. Dunnette and L.M. Hough (Palo Alto, California: Consulting Psychologists Press, 1992), 571-650.

4. T.S. Ragu-Nathan, M. Tarafdar, B.S. Ragu-Nathan and Q. Tu, "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation," Information Systems Research 19, no. 4 (December 2008): 417-433.

5. A. Gupta, R. Sharda, Y. Dong, R. Sharda, D. Asamoah and B. Pickering, "Improving Rounding in Critical Care Environments Through Management of Interruptions," Decision Support Systems 55, no. 2 (May 2013): 516-527.

6. Addiction to "thrill-producing" technologies such as social networking sites and mobile email is a growing problem for which the workplace implications are just beginning to be understood. It is different from substance addiction, about which, for example, see T.E. Robinson and K.C. Berridge, "Addiction," Annual Review of Psychology 54, no. 1 (2003): 25-53.

[7] O. Turel, A. Serenko and N. Bontis, "Family and Work-Related Consequences of Addiction to Organizational Pervasive Technologies," Information & Management 48, no. 2-3 (March 2011): 88-95.

[8] E. Dockterman, "Candy Crush Saga: The Science Behind Our Addiction," Nov. 15, 2013, www.time.com.

[9] Saint, comment on L.J. Williamson, "'Candy Crush Saga' Gives Addicted Mobile-Game Players a Sugar Rush," May 25, 2013, http://herocomplex.latimes.com.

[10] For example, see Verizon, "2008 Data Breach Investigations Report," 2008, http://verizonenterprise.com, 11.

[11] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research 20, no. 1 (March 2009): 79-98.

[12] J. D'Arcy, T. Herath and M.K. Shoss, "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," Journal of Management Information Systems 31, no. 2 (fall 2014): 285-318.

[13] M. Tarafdar, E.B. Pullins and T.S. Ragu-Nathan, "Technostress: Negative Effect on Performance and Possible Mitigations," Information Systems Journal, in press, published electronically July 24, 2014.

[14] Ragu-Nathan et al., "The Consequences of Technostress"; and Turel, Serenko and Bontis, "Family and Work-Related Consequences."

[15] T. Lewin, "Chevron Settles Sexual Harassment Charges," New York Times, Feb. 22, 1995.

[16] G. Laasby, "Target Data Breach Started With Phishing Malware Email at Contractor," Milwaukee Wisconsin Journal Sentinel, Feb. 12, 2014, www.jsonline.com.

[17] M. Riley and D. Lawrence, "As Data Breach Woes Continue, Target's CEO Resigns," May 5, 2014, www.businessweek.com.

[18] See N. Kakabadse, G. Porter and D. Vance, "Addicted to Technology," Business Strategy Review 18, no. 4 (winter 2007): 81-85; and J. Fitzgerald, "Lawsuit Claims Addiction to Internet Is a Disability," Seattle Times, Feb. 19, 2007.

[19] J. D'Arcy and G. Greene, "Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance," Information Management & Computer Security 22, no. 5 (2014): 474-489.

[20] K. Stuart, "German Minister Calls for Anti-Stress Law Ban on Emails Out of Office Hours," August 29, 2014, www.theguardian.com; P. Oltermann, "Germany Ponders Ground-Breaking Law to Combat Work-Related Stress," September 18, 2014, www.theguardian.com; T. de Castella, "Could Work Emails Be Banned After 6 p.m.?," April 10, 2014, www.bbc.com; and "Volkswagen Turns Off Blackberry Emails After Work Hours," December 23, 2011, www.bbc.com.

[21] Turel, Serenko and Bontis, "Family and Work-Related Consequences."

[22] D'Arcy, Hovav and Galletta, "User Awareness of Security Countermeasures."

[23] Ibid.

[24] Gupta et al., "Improving Rounding in Critical Care Environments."

[25] B.J. Fogg, "Persuasive Technology: Using Computers to Change What We Think and Do" (San Francisco, California: Morgan Kaufmann, 2002).

[26] Gupta et al., "Improving Rounding in Critical Care Environments."

[27] P. Khanal, A, Vankipuram, A. Ashby, M. Vankipuram, A. Gupta, D. Drumm-Gurnee, K. Josey, L. Tinker and M. Smith, "Collaborative Virtual Reality Based Advanced Cardiac Life Support Training Simulator Using Virtual Reality Principles," Journal of Biomedical Informatics 51 (October 2014): 49-59.

[28] See, for example, D'Arcy and Greene, "Security Culture and the Employment Relationship."

[29] H. Li, A. Gupta, X. Lou and M. Warkentin, "Exploring the Impact of Instant Messaging on Subjective Task Complexity and User Satisfaction," European Journal of Information Systems 20, no. 2 (March 2011): 139-155.

[30] Such individuals have "polychronous" personalities; see J.M. Conte and J.N. Gintoft, "Polychronicity, Big Five Personality Dimensions and Sales Performance," Human Performance 18, no. 4 (2005): 427-444.

[31] M. Kajzer, J. D'Arcy, C. Crowell, A. Striegel and D. Van Bruggen, "An Exploratory Investigation of Message-Person Congruence in Information Security Awareness Campaigns," Computers & Security 43, (June 2014): 64-76.

[i] The 14 studies are: Ragu-Nathan et al., "The Consequences of Technostress"; M. Tarafdar, Q. Tu, B.S. Ragu-Nathan and T.S. Ragu-Nathan, "The Impact of Technostress on Role Stress and Productivity," Journal of Management Information Systems 24, no. 1 (summer 2007): 301-328; M. Tarafdar, Q. Tu and T.S. Ragu-Nathan, "Impact of Technostress on End-User Satisfaction and Performance," Journal of Management Information Systems 27, no. 3 (winter 2010-11): 303-334; Tarafdar, Pullins and Ragu-Nathan, "Technostress: Negative Effect on Performance and Possible Mitigations"; O. Turel, M. Mouttapa and E. Donato, "Preventing Problematic Internet Use Through Video-Based Interventions: A Theoretical Model and Empirical Test," Behaviour & Information Technology, in press, published electronically July 7, 2014; Turel, Serenko and Bontis, "Family and Work-Related Consequences"; O. Turel, A. Serenko and P. Giles, "Integrating Technology Addiction and Use: An Empirical Investigation of Online Auction Users," MIS Quarterly 35, no. 4 (December 2011): 1043-1061; D'Arcy, Hovav and Galletta, "User Awareness of Security Countermeasures"; D'Arcy, Herath and Shoss, "Understanding Employee Responses to Stressful Information Security Requirements"; D'Arcy and Greene, "Security Culture and the Employment Relationship"; Kajzer et al., "An Exploratory Investigation of Message-Person Congruence"; Gupta et al., "Improving Rounding in Critical Care Environments"; Li et al., "Exploring the Impact of Instant Messaging"; and Khanal et al., "Collaborative Virtual Reality Based Advanced Cardiac Life Support Training Simulator Using Virtual Reality Principles."

Reprint 56221.