2018

Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences

Gabriela Mallmann
Universidade Federal do Rio Grande do Sul, gabilmallmann@gmail.com

Aline de Vargas Pinto
UFRGS, alinevargas01@hotmail.com

Antonio Carlos Gastaud Maçada
UFRGS, acgmacada@ea.ufrgs.br

Lançando luz sobre Shadow IT: Definição, Conceitos relacionados e Consequências.

Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences.

Gabriela Labres Mallmann, UFRGS, Brasil, gabilmallmann@gmail.com

Aline de Vargas Pinto, UFRGS, Brasil, alinevargas01@hotmail.com

Antônio Carlos Gastaud Maçada, UFRGS, Brasil, acgmacada@ea.ufrgs.br

Resumo

O uso de Tecnologias de Informação (TI) sem aprovação e suporte do departamento de TI, denominadas shadow IT, tem desafiado as organizações a repensarem as formas de gerenciar os recursos de TI com o objetivo de lidar com o uso de tecnologias não autorizadas nas organizações. Este trabalho revisou a literatura sobre shadow IT com o propósito de lançar luz sobre o fenômeno, apresentando e discutindo sua definição conceitual e tipos, conceitos relacionados e consequências do seu uso. O presente estudo é, assim, um esforço de melhor compreender o fenômeno com base na literatura existente, contribuindo para o desenvolvimento conceitual do tema, bem como sugerindo lacunas de pesquisa para avançar no conhecimento sobre uso de tecnologias não autorizadas nas organizações.

Palavras-chave: Shadow IT; Workarounds; Cosumerização de TI; BYOD; Revisão de Literatura.

Abstract

The use of Information Technology (IT) without the approval and support of the IT department, called shadow IT, has challenged organizations to rethink ways to manage IT resources to cope with the use of unauthorized technologies within organizations. We review the literature on shadow IT to shed light on this phenomenon, discussing the conceptual definition and types, the related concepts, and its consequences. This study, then, is an effort to better understand the phenomenon based on the extant literature. We provide contributions by enhancing the emerging body of knowledge on shadow IT, as well as by suggesting research gaps to be addressed in future research in order to advance on the topic.

Keywords: *Shadow IT; Workarounds; IT consumerization; BYOD; Literature Review.*

1. INTRODUÇÃO

O departamento de TI deixou de ser o único fornecedor de tecnologia da informação (TI) utilizada nos processos de negócios. Muitos indivíduos e grupos de trabalho tem implementado, de forma autônoma, soluções tecnológicas não disponibilizadas pelo departamento de TI para realizar as tarefas de trabalho. Esta tecnologia de informação não autorizada ou desconhecida pelo

ISSN 2183-489X

departamento de TI utilizada pelos funcionários para realizar suas tarefas de trabalho vem sendo chamada de shadow IT (e.g., Haag & Eckhardt, 2017).

A magnitude do fenômeno shadow IT é crescente uma vez que o usuário está mais familiarizado com as tecnologias que estão facilmente acessíveis, facilitando ao funcionário a adoção e uso de TI além das fornecidas pela organização. Consequentemente, torna-se cada vez mais difícil para os gerentes de TI governar a crescente variedade de sistemas e os riscos provenientes dela (Fürstenau & Rothe, 2014). O Instituto Ponemon afirma que a violação média de dados, em 2015, custou às empresas uma média de US $4 milhões, sendo que 70% do acesso não autorizado aos dados são cometidos pelos próprios funcionários da organização (Globalscape, 2016). Contudo, quando a ação de um funcionário coloca a organização em risco pode não haver uma intenção maliciosa, e sim uma necessidade de ser produtivo (e.g., Zimmermann et al., 2017; Mallmann et al., 2018). Em alguns casos os funcionários não estão cientes ou não entendem as políticas de segurança da informação da sua organização (e.g., Haag & Eckhardt, 2014; Silic et al., 2017).

Shadow IT é, assim, um fenômeno que está ganhando relevância na prática e também recebendo maior atenção acadêmica. Sistemas shadow e conceitos relacionados têm recebido ampla atenção de pesquisadores e gestores devido a popularização da computação em nuvem (Müller et al., 2015), da política bring your own device (BOYD) (Miller et al., 2012), workarounds relacionadas à TI (Alter, 2014), e outras tendências importantes no cenário de consumerização de TI (Harris, Ives & Junglas, 2012). Motivado por este contexto, este estudo tem como objetivo lançar luz sobre o fenômeno shadow IT, apresentando e discutindo sua definição e tipos, conceitos relacionados e consequências de uso. Desta forma, este trabalho contribui ao responder, por meio de uma revisão de literatura, as seguintes questões de pesquisa: RQ1: Qual a definição conceitual de shadow IT e como os diferentes tipos de shadow IT citados na literatura podem ser classificados? RQ2: Quais conceitos são relevantes ao investigar shadow IT e como esses conceitos estão relacionados? RQ3: Quais são os consequentes do uso da shadow IT para os indivíduos e para a organização?

Embora não seja um fenômeno novo e esteja cada vez mais em voga, este tópico é relativamente inexplorado e o conhecimento atual ainda é limitado e escasso (e.g., Silic et al., 2017; Haag & Eckhartd, 2017). A literatura acadêmica sobre shadow IT está focada em estudos exploratórios, os quais discutem, principalmente, os benefícios e malefícios destas tecnologias para as empresas (e.g., Fuerstenau & Rothe, 2014; Silic & Back, 2014), bem como sobre os mecanismos de governança para controle destas tecnologias (e.g., Györy et al., 2012; Zimmermann et al., 2014). Assim, a necessidade de uma revisão de literatura sobre shadow IT deve-se a escassez de abordagens teórico-conceituais ao estudar o tema (e.g., Haag & Eckhartd, 2017).

Reunir os achados sobre shadow IT contribui para a compreensão do fenômeno, o que é fundamental para avançar no conhecimento do tema (Webster & Watson, 2002). Outra contribuição desta

pesquisa é apresentar a relação da shadow IT com conceitos similares. Haag e Eckhardt (2017) afirmam que alguns conceitos estudados na área de SI compartilham atributos com shadow IT, como BYOD, consumerização de TI e workaround, sendo importante reconhecer quais são os aspectos que os diferenciam, possibilitando a caracterização da shadow IT como um conceito único e relevante. Por fim, este estudo também contribui discutindo as consequências individuais e organizacionais do uso da shadow IT, pois conhecer as tecnologias não autorizada e suas possíveis consequências pode ajudar a mitigar os riscos através do redesenho efetivo de fluxos de trabalho e / ou sistemas tecnológicos existentes (Vogus & Hilligoss, 2016).

Este artigo está organizado em seções. Na seção 2 é apresentada a revisão de literatura sobre o tema. Na seção 3 descreve-se o método. A análise dos resultados é apresentada na seção 4. Na sequência, os resultados da pesquisa são discutidos, identificando lacunas de pesquisa, bem como as implicações teóricas e práticas.

2. REVISÃO DE LITERATURA

A literatura sobre shadow IT vem ganhando relevância ao longo dos últimos anos. Desde 2012, o número de trabalhos acadêmicos publicados sobre o tema têm aumentado consideravelmente, porém a grande maioria dos estudos sobre shadow IT é recente, sendo mais de 70 por cento das publicações datadas dos últimos quatro anos (2014 a 2017). Dessa maneira, o tema pode ser considerado pouco explorado, embora também esteja ganhando notoriedade na academia ao longo dos anos. Os primeiros artigos sobre a temática discutem o surgimento da shadow IT após a adoção de ERPs (Enterprise Resource Planning), por exemplo, a criação e uso de planilhas do Excel para executar as tarefas de trabalho ao invés da utilização do sistema ERP oficial implementado pela organização (e.g., Jones et al., 2004; Behrens & Sedara, 2004; Raden, 2005).

A partir de 2012, destacam-se os estudos que abordam a shadow IT ao nível organizacional, com foco em mecanismos de governança de TI para lidar com o uso de shadow IT nas organizações, minimizando os riscos de segurança (e.g., Györy et al., 2012; Zimmermann & Rentrop, 2014; Furstenau et al., 2017; Zimmermann et al., 2017). A partir de 2014, alguns estudos preocuparam-se em investigar shadow IT enquanto um comportamento de uso de TI que desvia das políticas da empresa, por exemplo, investigando as motivações ou antecedentes que levam ao uso de shadow IT da perspectiva dos funcionários, bem como a relação entre o uso de shadow IT e o desempenho individual (e.g., Haag & Eckhardt, 2014; Haag et al., 2015).

O termo shadow IT, apesar de não ser recente, ainda carece de um conceito largamente aceito e um entendimento do que é o fenômeno e de como ele se apresenta nas organizações. O tópico pode ser considerado, então, relativamente inexplorado e o conhecimento atual ainda é limitado (e.g., Silic et al., 2017; Haag & Eckhartd, 2017). Ademais, estudos prévios (e.g., Silic & Back, 2014; Huber et

al., 2017; Zimmermann et al., 2017) sugerem que shadow IT pode se apresentar de diversas maneiras dentro das organizações, através de um hardware, software ou qualquer outra solução, como uma planilha, serviços em nuvem ou um aplicativo desenvolvido pelo funcionário. Dessa forma, o tema carece de uma discussão conceitual, fazendo-se necessário também esclarecer a diferença entre os conceitos relacionados e as consequências do seu uso (Haag & Eckhardt, 2017).

2.1. Conceitos relacionados

2.1.1 Consumerização de TI

Consumerização de TI (CTI) diz respeito ao impacto exercido pelas tecnologias oriundas do mercado consumidor nas organizações. Harris et al. (2012) argumentam que a chegada de dispositivos e aplicações com origem no setor de consumo está dando origem a uma segunda revolução de TI orientada pelo funcionário. As inovações que se originam no setor de consumo vêm cada vez mais se infiltrando no ambiente corporativo e essa tendência, chamada de consumerização, vem impactando a gestão da informação e trazendo, continuamente, novos desafios para os gestores de TI (Weisß & Leimeister, 2012).

Weisß e Leimeister (2012) apresentam um modelo de mudanças de expectativas para explicar a origem da tendência da Consumerização. Segundo estes autores, o que leva os empregados a adotarem tecnologias de mercado é a expectativa de alto nível de experiência do usuário e a sua expectativa de oferta de novas aplicações por parte da TI da empresa. Contudo, aos olhos dos funcionários, a tecnologia oferecida pela área de TI não está conseguindo atender a estas expectativas, levando as organizações (pressionadas pelos funcionários) a adotar tecnologias do mercado consumidor. Esta necessidade de adotar tecnologias do mercado consumidor é mais proeminente na alta gestão (Weisß & Leimeister, 2012) e na nova geração de usuários de tecnologia, chamados na literatura de tech savvy ou nativos digitais (Harris et al., 2012; Silic & Back, 2014; Weiß & Leimeister, 2012).

Conforme Harris et al. (2012), a CTI pode ter diferentes definições dependendo do stakeholder: (1) da perspectiva do funcionário, a CTI está relacionada ao uso individual e a familiaridade com dispositivos e aplicações da vida pessoal do usuário, as quais são vistas como úteis ao serem utilizadas no trabalho; (2) da perspectiva do departamento de TI da empresa, a CTI é uma vasta quantidade de dispositivos e aplicações utilizados dentro da organização que podem não fazer parte da lista sancionada pela empresa ou que não foram formalmente aprovadas pela área de TI, podendo ser vistas, assim, ou como uma ameaça ou como uma oportunidade; (3) da perspectiva do mercado, a CTI pode ser considerada como todo dispositivo ou aplicação que se origina no mercado consumidor e que, ao menos originalmente, não é alvo da organização para ser usado em conjunto ou substituir a tecnologia da informação utilizada pela empresa.

2.1.2. Workaround

Workaround é conceituado por Alter (2014) como adaptações dos sistemas e recursos disponíveis pela empresa, possibilitando superar anomalias e restrições encontradas que impossibilita que as tarefas de trabalho sejam realizadas de forma completa e efetiva (Alter, 2014; Malaurent & Avison, 2015). Workaround pode ser uma estratégia de usar um sistema de forma que não foi projetado para ser usado ou usando métodos alternativos, sendo útil para resolver um problema imediato e urgente (Azad & King, 2008). Exemplos comuns de workaround são o ajuste ou a manipulação de dados para chegar ao resultado desejado (Alojairi, 2017).

Muitas organizações afirmam que workaround é composto por práticas temporárias implementadas para lidar com as incertezas no período imediatamente posterior à implementação do sistema, com o entendimento de que estas devem diminuir ao longo do tempo. Contudo, evidências crescentes sugerem que essas práticas, de fato, evoluem ao longo do tempo ao invés de desaparecerem podendo levar ao uso de tecnologias alternativas (Azad & King, 2012). Muitas soluções alternativas ocorrem porque a tecnologia não se encaixa nas necessidades do trabalho (Alter, 2014), podendo ser necessárias para os usuários no sentido de apoiar suas atividades diárias (Azad & King, 2012) e facilitar a interação do usuário no caso de um SI mal planejado (Ferneley & Sobreperez, 2006).

2.1.3. BYOx

O conceito de Bring Yor Own Anything (BYOx) vem ao encontro dos conceitos até aqui discutidos, uma vez que diz respeito a adoção e uso de tecnologias trazidas pelo funcionário no ambiente de trabalho. BYOx é um termo que engloba várias tendências de BYO nas organizações, tais como Bring your onw device (BYOD) e Bring Your Own Cloud (BYOC), etc. (e.g., French et al., 2014; Haag, 2015).

O termo BYOD é o mais antigo e conhecido de todos e, portanto, o mais discutido na literatura acadêmica. BYOD é uma política de gestão que permite que os usuários acessem recursos e aplicações de trabalho de seus dispositivos móveis pessoais (Dang-pham & Pittayachawan, 2015). BYOD permite que os funcionários tragam seus próprios dispositivos de computação para trabalhar e incorporá-los a rede da organização, em vez de utilizar dispositivos de propriedade da empresa (French et al., 2014). Trata-se, então, de políticas e estratégias de gestão elaboradas pelas organizações para lidar com a tendência criada pelos funcionários de adotar e usar as suas próprias soluções no ambiente de trabalho.

2.1.4. Computação em nuvem

A computação em nuvem é um modelo que permite acesso onipresente e conveniente, através da internet, a um conjunto compartilhado de recursos computacionais configuráveis que podem ser rapidamente provisionados e liberados com esforço mínimo de gerenciamento ou interação com

prestadores de serviço (Mell & Grance, 2011). A principal tarefa da computação em nuvem é a capacidade de adquirir e gerenciar dados sempre que o usuário requisitar (Lis & Paula, 2015). Entre os fatores impulsionadores do uso da computação em nuvem está a possibilidade de acesso a softwares sem a necessidade de qualquer conhecimento detalhado ou específico da infraestrutura usada para fornecer os recursos, além da independência de plataformas e dispositivo. Como os aplicativos são baseados na web, eles podem ser acessados virtualmente de qualquer lugar e de praticamente qualquer dispositivo (Shin, 2015), permitindo que os usuários compartilhem informações e conhecimentos mais facilmente (Park & Ryoo, 2013). Esses novos serviços em nuvem geram mudanças revolucionárias no modo como as soluções são projetadas, construídas, entregues e gerenciadas. Portanto, devido a facilidade de acesso e uso, a computação em nuvem propicia um cenário favorável para os usuários utilizarem os serviços em nuvem sem a aprovação ou supervisão necessária da organização (Khalil et al., 2017).

3. MÉTODO DE PESQUISA

O método de pesquisa deste trabalho é uma revisão de literatura com base nas diretrizes propostas por Webster e Watson (2002). Como shadow IT é ainda pouco explorado, uma revisão de literatura pode corroborar criando uma base sólida para o avanço do conhecimento (Webster & Watson, 2002). Desta maneira, reunir o conhecimento dos estudos existentes sobre o tema é de fundamental importância para a evolução das pesquisas.

A busca dos artigos foi realizada com base em um protocolo de pesquisa. Primeiramente, foi realizada uma pesquisa nas principais revistas da área de SI ('basket eight'). Na sequência, buscou-se em base de dados científicas como ScienceDirect, Web of Knowledge, Google Scholar e EBSCO. Utilizou-se as bases de dados da Association for Information System - AIS Electronic Library (AISeL), que contém artigos dos maiores congressos de Sistemas de Informação. Essa expansão nas bases de dados pesquisadas justifica-se, pois, grande parte da literatura em shadow IT advém de congressos internacionais, podendo ser considerada uma literatura emergente e que vem crescendo em publicações ao longo dos anos.

As seguintes palavras-chave foram utilizadas na busca dos artigos: shadow IT e shadow systems, as quais deveriam estar contidas no título, no resumo ou nas palavras-chave. As seguintes palavras serviram como critérios de exclusão: workrounds, end-user-computing e bring your own device (BYOD), porquanto, embora possuam similaridades, são conceitos diferentes do termo shadow IT (Rentrop & Zimmermann, 2012; French et al., 2014; Haag & Eckhardt, 2017).

Considerando os critérios do protocolo de pesquisa, foram encontrados 50 artigos relevantes. A busca foi realizada entre os meses de março e maio de 2018. A Tabela 1 apresenta os artigos selecionados segundo os critérios de inclusão e exclusão de artigos.

FONTE		NÚMERO DE ARTIGOS
Revista	Network Security	2
	Computer & Security	1
	Information & Management	1
	Outros (Computer Fraud & Security, CAIS, Journal of Information Systems, etc.)	9
	Total	13
Conferência	AMCIS	8
	ECIS	7
	ICIS	5
	PACIS	5
	Outros (ACIS, ICDS, BLED, ECKM, Conf-irm …)	12
	Total	37
Total de Artigos		50

Tabela 1 – Artigos Selecionados

4. RESULTADOS

4.1. Definição conceitual de shadow IT

Shadow IT é definida como qualquer hardware, software ou serviços criados, introduzidos e usados pelos funcionários sem aprovação explícita ou mesmo sem o conhecimento da organização (Haag & Eckhardt, 2017). Estes sistemas são implementados de forma autônoma dentro das unidades de negócio pelos usuários, portanto estas tecnologias não possuem relação técnica nem estratégica com a gestão de serviços de TI da organização (Zimmermann et al., 2014).

Outro fator importante na definição da shadow IT é a intenção do usuário ao adotar uma tecnologia shadow, definida por Györy et al (2012) como bem intencionada apesar da não conformidade com as políticas da empresa. O termo "shadow"' implica em um comportamento ilícito e mal intencionado, entretanto, a maioria dos casos de shadow IT são ocasionados por conveniência (Walters, 2013). Shadow IT é, assim, implementada pelo usuário intencionalmente para ajudar na realização de suas tarefas, como apoio ao processo de negócio, e não com intenções maliciosas, como causar danos econômicos à organização (e.g., Györy et al., 2012, Silic & Back, 2014, Haag & Eckhardt, 2014).

Pesquisas recentes (e.g., Haag et al., 2015; Mallmann et al., 2018) tem abordado shadow IT como comportamento de uso, diferenciando-se dos estudos anteriores. Estes estudos têm como base o conceito de uso individual da shadow IT (individual shadow IT usage) proposto por Haag e Eckhardt (2014) que definem uso de shadow IT como o uso voluntário de qualquer recurso de TI que viola as normas do local de trabalho como reação às restrições situacionais percebidas com a intenção de melhorar o desempenho no trabalho sem, no entanto, prejudicar a organização. Esta definição alega que os usuários de shadow IT agem por conta própria com o principal objetivo de finalizar de forma eficaz e produtiva as suas tarefas de trabalho, as quais são prejudicadas, por exemplo, devido ao mau funcionamento dos sistemas de TI da organização ou instruções inadequadas, fazendo com que o usuário desvie deliberadamente das políticas e aceite possíveis riscos à segurança e danos aos ativos de TI da organização (Haag & Eckhardt, 2014).

4.1.1. Tipos de shadow IT

Os primeiros estudos sobre shadow IT discutem o surgimento de sistemas shadow após a implementação de Enterprise Resource Planing (ERP) (e.g., Jones et al, 2004; Behrens & Sedara, 2004), principalmente, com relação ao uso de planilhas de Excel em substituição às ferramentas de ERP implementadas pela empresa. Contudo, em virtude dos avanços tecnológicos, os estudos mais recentes (e.g., Silic & Back, 2014, Mallmann et al., 2018) apresentam outras ocorrências de shadow IT, como uso de mídias sociais e serviços baseados em nuvem (e.g., Dropbox e Google Apps).

Silic e Back (2014), por exemplo, dividem os tipos de Softwares de shadow IT encontrados no seu estudo de caso em dois grupos: internos e externos. Softwares shadow internos são softwares instalados nos computadores de trabalho, enquanto softwares shadow externos são providos por serviços externos, como serviços de Computação em Nuvem. A literatura existente sugere, então, que as ocorrências de shadow IT podem ser aplicações, planilhas, serviços de nuvem, dispositivos móveis, hardware, ou uma combinação destes fatores (e.g., Silic & Back, 2014; Huber et al., 2016; Zimmermann et al., 2017). Dessa forma, buscou-se na literatura como essas tecnologias se apresentam na prática em um esforço de esclarecer como os indivíduos usam a shadow IT no local de trabalho. A Tabela 2 resume os quatro tipos de shadow IT com base na literatura.

SHADOW IT	DESCRIÇÃO	AUTORES
Serviços providos via internet (***internet based services***)	*Softwares* de mídia social para comunicação e troca de informação ou outros serviços providos pela internet como serviços de nuvem. Ex: Whatsapp, Facebook, Dropbox, Google Apps, etc.	Gyory et al. (2012); Fürstenau and Rothe (2014); Silic and Back (2014); Haag and Eckhardt (2014); Haag (2015); Walters (2013);

		Walterbusch et al. (2017), Mallmann at el. (2018).
Soluções desenvolvidas pelo usuário (***self-made solutions***)	Soluções desenvolvidas pelos funcionários das unidades de negócios para realizar as tarefas de trabalho. Ex: *software* desenvolvido pelos próprios funcionários para realizar suas tarefas de trabalho.	Jones et al. (2004); Rentrop and Zimmermann (2012); Fürstenau and Rothe (2014); Zimmermann et al. (2014); Huber et al. (2016).
Softwares* instalados pelo usuário** (self-installed applications***)	Aplicações de software instaladas pelos funcionários das unidades de negócios nos dispositivos da empresa (estações de trabalho). Ex: *software* disponível para download na internet de forma gratuita que, de alguma forma, auxilia nas atividades do trabalho.	Jones et al. (2004); Rentrop and Zimmermann (2012); Fürstenau and Rothe (2014); Zimmermann et al. (2014); Silic and Back (2014).
Dispositivos adquiridos pelo usuário (***self-acquired devices***)	Em termos de *hardware*, *shadow IT* pode ser dispositivos ou outros periféricos adquiridos pelos funcionários. Esses dispositivos são comprados diretamente do varejo pelo usuário ao invés de serem requisitados através do catálogo oficial da TI da empresa. Inclui o uso das aplicações dos dispositivos pessoais na rede da empresa. Ex: smartphones, notebooks, tablets, etc.	Rentrop and Zimmermann (2012); Silic and Back, (2014); Zimmermann et al. (2014); Gozman and Willcocks (2015), Huber et al. (2016).

Tabela 2 – Tipos da *Shadow IT*

Quatro tipos de shadow IT surgiram da literatura. O primeiro, chamado de serviços providos via internet, representa os softwares não autorizados acessados pela Internet (e.g., Furstenau & Rothe, 2014; Haag, 2015; Walterbusch et al., 2017) e, portanto, para ser usado, não precisa ser instalado em qualquer dispositivo. Por exemplo, uso do Dropbox para compartilhamento de conteúdo ou uso de Skype via web para comunicação com colegas e clientes para realizar tarefas de trabalho sem autorização do departamento de TI. O segundo tipo são as soluções desenvolvidas e utilizadas pelos funcionários sem autorização nos computadores da empresa para executar suas tarefas de trabalho (e.g., Zimmermann et al., 2014; Zimmermann et al., 2017), que podem variar de uma simples planilha Excel a uma aplicação mais complexa desenvolvida pelos funcionários para ser utilizada por toda a unidade de negócios. Por exemplo, a utilização de uma planilha de Excel desenvolvida para controle, ao invés de utilizar o sistema oficial da empresa.

O terceiro tipo, chamado de softwares instalados pelo usuário, são aquelas aplicações instaladas e utilizadas pelos funcionários nos dispositivos da empresa, por exemplo, nos computadores, smartphones ou tablets fornecidos pela organização (e.g., Jones et al., 2004; Silic & Back, 2014). Esse tipo de uso de TI envolve soluções que geralmente estão disponíveis gratuitamente na Web e precisam ser baixadas e instaladas antes do uso, ao invés de serem acessadas pela Internet.

Finalmente, o quarto tipo diz respeito aos dispositivos auto adquiridos pelos funcionários e representam a camada de hardware da shadow IT. São os dispositivos adquiridos e de propriedade dos funcionários em vez dos dispositivos da empresa, incluindo o uso de aplicativos nestes dispositivos pessoais (e.g., Rentrop & Zimmermann, 2012; Zimmermann et al., 2017).

4.2. Relação da shadow IT com conceitos similares

Haag e Eckhardt (2017) destacam que shadow IT se distingue conceitualmente de outros termos relacionados, como bring-your-own-device (BYOD) e consumerização de TI. Embora esses conceitos compartilhem semelhanças, existem diferenças cruciais entre eles. Na sequência os conceitos relacionados ao tema são discutidos segundo a literatura de SI.

Consumerização de TI é um conceito amplo que engloba diferentes fenômenos relacionados ao uso de tecnologias do mercado consumidor no local de trabalho (Harris et al., 2012). A relação da consumerização de TI com a shadow IT, dá-se, pois a consumerização engloba tanto as tecnologias advindas do mercado consumidor contempladas nas políticas da empresa, quanto tecnologias que ainda não constam nestas políticas, ou seja, que não foram aprovadas pela área de TI da empresa, configurando, assim, uma shadow IT.

Também sob o guarda-chuva da consumerização de TI, o termo workaround refere-se, de maneira ampla, às adaptações conscientes de atividades de trabalho que não são esperadas ou especificadas para serem alteradas dessa maneira (Laumer et al. 2017). Haag e Eckhardt, 2017 apontam três exemplos de soluções alternativas: 1) workarounds não baseados em TI, por exemplo, uso de papel para coletar e processar informações; 2) adaptação da solução de TI obrigatória e/ou a TI pessoal aprovada e usá-las de maneiras diferentes e inesperada, por exemplo, usando o MS Word para converter e reeditar o conteúdo de documentos PDF; e 3) shadow IT, ou seja, uso de TI não aprovada e/ou alteração da TI aprovada de formas não aprovadas, por exemplo, criando macros do MS Excel sem aprovação para automatizar tarefas de trabalho repetitivas.

Shadow IT, assim, é um tipo de workaround, embora nem todo workaround seja necessariamente uma shadow IT, pois workaround engloba características adicionais que vão além da shadow IT. Shadow IT está relacionada à tecnologia, enquanto workaround também pode estar relacionado a dispositivos que não são de TI (e.g., papel). Dessa maneira, workaround é um conceito mais amplo que engloba outras instâncias, incluindo shadow IT, e ambos os termos podem ser classificados como comportamento de trabalho que desviam das políticas da organização. Outra diferença, segundo Lund-Jensen et al. (2016), se caracteriza no aspecto temporal, já que workarounds tendem a ser práticas temporárias e a shadow IT práticas a longo prazo (Haag & Eckhardt, 2017).

Por sua vez, BYOx é um conceito frequentemente confundido com shadow IT. A diferença entre os dois conceitos é crucial pois refere-se ao desvio ou não das políticas de TI. No contexto do BYOx,

a tecnologia trazida pelo funcionário para uso nas suas tarefas de trabalho é permitida pela organização por meio de políticas elaboradas em conjunto com a área de TI (e.g., Dang-pham & Pittayachawan, 2015). Por exemplo, a política de BYOD permite que o usuário use seu próprio laptop no local de trabalho. No contexto de shadow IT, porém, a solução utilizada pelo usuário, geralmente, não é se quer conhecida pela área de TI, não sendo, assim, nem aprovada e nem apoiada pelo departamento de TI da empresa (e.g., Rentrop & Zimmermann, 2012).

Silic e Back (2014) argumentam que, no contexto tecnológico atual, no qual smartphones estão sendo cada vez mais utilizados no ambiente de trabalho, como nas políticas de BYOD, shadow IT está se tornando ainda mais importante em diferentes níveis organizacionais, motivada também pelo fato dos usuários acreditarem que não estão fazendo nada errado de fato. Portanto, o papel do BYOx no contexto de shadow IT é de facilitar o surgimento destas tecnologias shadow uma vez que a adoção de políticas de permissão ao uso de tecnologias próprias, representadas pelos BYOx, aumenta a complexidade da área de TI em gerenciar o crescente número de dispositivos e aplicações utilizadas pelos funcionários, possibilitando o maior surgimento de uma shadow IT.

Por fim, a Computação em Nuvem (CN) surge como um conceito relevante no contexto de shadow IT. Haag e Eckhardt (2015) argumentam que além dos equipamentos advindos do mercado consumidor, como os smartphones, os serviços de computação em nuvem tornaram a shadow IT acessível também para as pessoas sem muito conhecimento em TI, pois os serviços são entregues sem custo via web browers e são bastante simples e intuitivos de utilizar. Por esse motivo, muitos estudos (e.g., Silic & Back, 2014; Mallmann et al., 2018) apresentam os serviços de nuvem como a principal ocorrência de shadow IT, sendo frequentemente utilizada pelos funcionários no local de trabalho sem autorização do departamento de TI.

4.3. Consequências do uso de shadow IT para os indivíduos e organização

Apensar do termo "shadow"' implicar um comportamento ilícito e mal-intencionado que põe em risco a segurança de TI da organização, a maioria dos casos de shadow IT são ocasionados por conveniência (Walters, 2013). Estudos sugerem que funcionários utilizam shadow IT para auxiliar na realização de suas tarefas, não com intenções maliciosas (e.g., Györy et al., 2012; Haag & Eckhardt, 2014). Emerge, assim, uma vasta discussão sobre as consequências positivas e negativas do uso de shadow IT para indivíduos e organização.

No nível individual, consequentes como produtividade e desempenho se destacam em pesquisas recentes como benefícios do uso de shadow IT (e.g., Silic & Back, 2014; Haag & Eckhardt, 2014; Haag, 2015; Haag et al., 2015; Furstenau et al., 2017). Estudos empíricos, como o estudo de Haag et al. (2015), sugerem que shadow IT alavanca a produtividade individual, melhorando o desempenho no trabalho dos funcionários. Também relacionado ao desempenho do usuário, pesquisas identificam que os funcionários frequentemente utilizam shadow IT para se comunicar e

colaborar no trabalho (e.g., Shumarova & Swatman, 2008; Silic & Back, 2014), bem como para compartilhar informações e conhecimento entre colegas, clientes e parceiros externos (e.g, Mallmann et al., 2018; Steinhueser et al., 2017). Dessa maneira, a melhoria na comunicação e na colaboração é um dos requisitos que pode levar a um aumento da produtividade e do desempenho individual dos usuários de TI.

Shadow IT também é frequentemente relacionado com inovação, sendo considerada um driver legítimo de inovação de soluções de TI (Fürstenau & Rothe, 2014). Haag et al. (2015) argumentam que a existência do uso de shadow IT desafia a importância da autonomia dos usuários para o surgimento de comportamentos inovadores, uma vez que o uso de sistemas shadow parece ser uma manifestação da criatividade e inovação pessoal dos usuários. Assim, a literatura também aponta um caráter inovador das soluções shadow conduzidas pelos usuários (Fürstenau & Rothe, 2014; György et al., 2012; Fürstenau et al., 2016; Zimmermann et al., 2016; Singh, 2015).

A melhoria no desempenho individual, por sua vez, pode ter impactos na organização como um todo. Singh (2015) argumenta que os gerentes de TI que gerenciam shadow IT, ao invés de apenas tentar evitar o seu uso, podem ver melhorias no desempenho de suas organizações, devido à introdução de inovações dos funcionários, que estão mais satisfeitos com as ferramentas que usam para executar tarefas de trabalho. Similarmente, os resultados empíricos de Haag et al. (2015) mostram que, ao nível individual, os usuários de shadow IT podem ser muito valiosos para as organizações porque são mais orientados para objetivos, eficazes e tentam encontrar soluções de longo prazo. Assim, os gerentes podem analisar os resultados construtivos do uso de shadow IT, como melhorias no trabalho dos funcionários e, consequentemente, no desempenho da empresa (Haag & Eckhardt, 2015).

O lado negativo da shadow IT, contudo, persiste apesar dos potenciais benefícios. Muitos funcionários não estão cientes de que a shadow IT está violando as políticas de TI da empresa e colocando em risco a segurança da informação organizacional (Walter, 2013; Silic & Back, 2014; Silic et al., 2017). O risco a segurança, assim, figura entre as principais preocupações citadas na literatura (e.g., Haag & Eckhardt, 2015; Silic & Back, 2014). Ao utilizar shadow IT como, por exemplo, aplicativos baseados em nuvem e uploading de dados sem o conhecimento da empresa, vários problemas de segurança podem ocorrer, tais como vazamento e perda de informações, risco à privacidade dos dados e compliance, representando, assim, um sério problema à segurança da informação organizacional.

5. DISCUSSÃO E CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo fazer uma revisão de literatura sobre shadow IT com a finalidade de lançar luz sobre o fenômeno, apresentando e discutindo sua definição, conceitos relacionados e

consequências do uso por meio de uma revisão de literatura. Esta seção discute os resultados, visando apontar lacunas de pesquisa sobre o tema, bem como discutir as implicações teóricas e práticas do estudo.

Os artigos que trazem como tema central a shadow IT tem objetivado entender quais são as shadow IT mais utilizadas e como identificá-las (e.g., Silic & Back, 2014), além de entender o que motiva os funcionários a adotar estas tecnologias (e.g., Haag & Eckhardt, 2015) e as formas de controle da shadow IT (e.g., Fürstenau & Rothe, 2014). Estes estudos corroboraram, especialmente, para a definição dos tipos e consequentes da shadow IT. Baseando-se nas pesquisas existentes, o presente estudo explorou a definição conceitual de shadow IT, bem como apresentou como ela se apresenta na prática, chamado aqui de tipos de shadow IT. Adicionalmente, o estudo discutiu a relação com conceitos similares para esclarecer as características da shadow IT e como ela se diferencia dos conceitos relacionados, conforme sugerido por Haag e Eckhardt (2017).

Os resultados sugerem que quando uma tecnologia é trazida do mercado consumidor pelo funcionário para uso no trabalho e não esta conforme com as políticas de TI da empresa, ela então é caracterizada como shadow IT, sendo diferente, assim, das políticas de BYOx. Estas políticas permitem que os funcionários utilizem suas próprias soluções - dentro de um leque de opções pré-definidas pelo departamento de TI - para realizar as suas tarefas de trabalho. Em suma, BYOD não pode ser considerado um comportamento desviante, uma vez que é uma política que permite aos funcionários trazer e usar dispositivos pessoais no trabalho (e.g., French et al. 2014). Workaround, por sua vez, é um comportamento que desvia das normas de TI, porém é mais amplo que shadow IT, pois inclui também soluções não baseadas em tecnologia. Por fim, serviços baseados em nuvem não são necessariamente shadow IT, mas se relaciona, pois muitas shadow IT utilizadas pelo funcionário são serviços de nuvem pela facilidade em acessar e utilizar estes recursos.

Com relação aos consequentes, os resultados sugerem que ainda há divergência na literatura sobre os resultados positivos e negativos do uso de shadow IT. Riscos à segurança da informação, vazamento e perda de dados, risco à privacidade e compliance figuram entre as principais preocupações citadas na literatura (e.g., Haag & Eckhardt, 2015; Silic & Back, 2014). Neste sentido, estudos prévios (e.g., Haag & Eckhardt, 2015) apontam a necessidade de equilibrar os prós e contras da shadow IT. Assim, pesquisas sobre os impactos do uso de shadow IT, como desempenho organizacional, caráter inovador e questões de segurança, ajudaria a esclarecer os consequentes da shadow IT nas organizações de forma a mitigar os riscos provenientes do seu uso, bem como potencializar os seus benefícios.

5.1. Lacunas de pesquisa segundo níveis de análise

Estudos anteriores sugerem que shadow IT surge no nível do funcionário (e.g, Györy et al., 2012; Furstenau et al., 2017) e pode ser usado por um indivíduo ou um grupo de indivíduos, ou seja, uso

individual e/ou coletivo da Shadow IT. No entanto, esta perspectiva de diferentes níveis precisa de investigação adicional, incluindo uma abordagem em nível de grupo, além do nível individual, para entender como os grupos de trabalho apoiam coletivamente o uso de shadow IT e quais são as consequências para o grupo (Haag & Eckhardt, 2017). Estudos a nível individual sobre shadow IT vêm sendo desenvolvidos desde 2014 (e.g., Haag & Eckhardt, 2014; Haag et al., 2015), os quais tem analisando shadow IT enquanto um comportamento (shadow IT usage), buscando entender o que leva o indivíduo a desviar das políticas de TI e utilizar shadow IT no trabalho. Sugere-se, então, que estudos futuros abordem investigações em nível de grupo para entender o uso de shadow IT no nível coletivo de análise, por exemplo, a difusão do uso de shadow IT entre os funcionários no local de trabalho.

A literatura também fornece evidências para uma relação entre o uso de shadow IT e a idade ou geração. A dependência da tecnologia, principalmente para interação social, está aumentando, especialmente entre os nativos digitais (Turkle, 2011). Isto está mudando a maneira como interagimos socialmente e trazendo várias consequências. Estudos anteriores sugerem que o uso de tecnologias do mercado consumidor é mais proeminente entre as gerações mais jovens, chamadas de tech-savvy, millennials ou geração Y (e.g., Weiß e Leimeister, 2012; Turner, 2015). Assim, a idade pode ser um fator potencial para entender o comportamento do usuário de TI. Um estudo geracional sobre o uso de shadow IT pode acrescentar informações valiosas sobre o comportamento individual em uma sociedade pós-moderna.

Ao nível organizacional, temas como Governança de TI e da Informação devem ser associados à shadow IT. Estudos neste nível podem buscar práticas de gestão para lidar com o uso de tecnologias não autorizadas no ambiente de trabalho através de abordagens de governança de TI, por exemplo, visando reduzir as falhas na segurança da informação e também reduzir os riscos de sobrecarga na infraestrutura de TI da empresa por parte dos usuários (e.g., György et al., 2012).

5.2. Implicações teóricas e práticas

Este estudo fornece implicações teóricas e práticas para o conhecimento emergente sobre shadow IT. Apesar de não ser recente, shadow IT ainda é um fenômeno pouco estudado na literatura de SI. Este estudo contribui, nesse sentido, ampliando o conhecimento conceitual sobre shadow IT e seu uso. O artigo também fornece contribuição conceitual ao discutir as semelhanças e diferenças entre shadow IT e conceitos relacionados. Ademais, este artigo fornecendo uma discussão sobre as consequências do uso da shadow IT que ainda são poucas exploradas e desconhecidas.

Este estudo também fornece contribuições práticas. Os gerentes devem prestar atenção ao fato de que a principal razão para o surgimento da shadow IT é a ausência completa ou parcial de soluções adequadas de TI que atendam aos requisitos dos funcionários (Walterbusch et al., 2017). Portanto, conhecer os tipos de shadow IT e suas consequências é também uma boa oportunidade para os

gerentes de TI entenderem as expectativas dos usuários e suas necessidades relacionadas à tecnologia, fornecendo a tecnologia adequada para executar suas tarefas. Ademais, a literatura sobre shadow IT discute uma ampla gama de consequências, desde melhorias de desempenho e soluções inovadoras até riscos de segurança e conformidade. Neste sentido, as organizações devem encontrar maneiras de equilibrar os resultados positivos e negativos da shadow IT de acordo com o contexto de cada organização.

Assim, este estudo é um esforço de melhor compreender o fenômeno por meio da revisão de literatura e sugerir lacunas de pesquisa para avançar no conhecimento do tema. Como limitações desta pesquisa, aponta-se o limitado número de artigos em periódicos que traga como tema central a shadow IT. A maioria dos trabalhos sobre o tema são de conferências, mostrando a necessidade, assim, de avanços teóricos e conceituais sobre o fenômeno.

REFERÊNCIAS

Alter, S. (2014). Theory of workarounds.Communications of the Association for Information Systems: Vol. 34, Article 55, pp. 1041=1066

Alojairi, A. (2017). The Dynamics of IT Workaround Practices A Theoretical Concept and an Empirical Assessment. International Journal of Advanced Computer Science and Applications, 8(7), 527-534.

Azad, B., & King, N. (2008). Enacting computer workaround practices within a medication dispensing system. European Journal of Information Systems, 17(3), 264-278.

Azad, B., & King, N. (2012). Institutionalized computer workaround practices in a Mediterranean country: an examination of two organizations. European Journal of Information Systems, 21(4), 358-372.

Behrens, S., & Sedera, W. (2004). Why do shadow systems exist after an ERP implementation? Lessons from a case study. Pacific Asia Conference on Information Systems (PACIS).

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. Computers & Security, 48, 281-297.

Ferneley, E. H., & Sobreperez, P. (2006). Resist, comply or workaround? An examination of different facets of user engagement with information systems. European Journal of Information Systems, 15(4), 345-356.

French, A. M., Guo, C., & Shim, J. P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). CAIS, 35, 10.Communications of the Association for Information Systems, Volume 35, Article 10, pp. 191-197, November 2014.

Furstenau, D., & Rothe, H. (2014). Shadow IT systems: discerning the good and the evil. Twenty Second European Conference on Information Systems, Tel Aviv.

Furstenau, D., Rothe, H., & Sandner, M. (2017). Shadow Systems, Risk, and Shifting Power Relations in Organizations. Communications of the Association for Information Systems, 41, 43-61.

Globalscape. Be afraid of your shadow: What is "shadow IT" and how to reduce it, 2016. Disponível em: https://www.globalscape.com/resources/whitepapers/shadow-it-guide. Acesso em: 05 março. 2018.

Gozman, D., & Willcocks, L. (2015). Crocodiles in the Regulatory Swamp: Navigating The Dangers of Outsourcing, SaaS and Shadow IT. In the Proceedings of the Thirty-Sixth International Conference on Information Systems, Fort Worth.

Györy, A. A. B., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. Proceedings of European Conference on Information Systems. Paper 222.

Haag, S., & Eckhardt, A. (2014). Normalizing the Shadows–The Role of Symbolic Models for Individuals' Shadow IT Usage. In the Proceedings of the Thirty-Fifth International Conference on Information Systems, Auckland.

Haag, S. (2015). Appearance of Dark Clouds?-An Empirical Analysis of Users' Shadow Sourcing of Cloud Services. In Wirtschaftsinformatik (pp. 1438-1452).

Haag, S., & Eckhardt, A. (2015). Justifying Shadow IT Usage. In Proceedings of the 19th Pacific Asia Conference on Information Systems, Singapore.

Haag, S., Eckhardt, A., & Bozoyan, C. (2015). Are Shadow System Users the Better IS Users?–Insights of a Lab Experiment. In the Proceedings of the Thirty-Sixth International Conference on Information Systems, Fort Worth.

Haag, S., & Eckhardt, A. (2017). Shadow IT. Business & Information Systems Engineering, 1-5.

Harris, J., Ives, B., & Junglas, I. (2012). IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. MIS Quarterly Executive, 11(3).

Huber, M., Zimmermann, S., Rentrop, C. & Felden, C. (2016). The Relation of Shadow Systems and ERP Systems—Insights from a Multiple-Case Study. Systems, 4, (1), 11. doi:10.3390/systems4010011

Huber, M.; Zimmermann, S.; Rentrop, C.; & Felden, C. (2017). Integration of Shadow IT Systems with Enterprise Systems - A Literature Review. In Proceedings of the Twenty-First Pacific Asia Conference on Information Systems, Langkawi.

Jones, D., Behrens, S., Jamieson, K., & Tansley, E. (2004). The rise and fall of a shadow system: Lessons for enterprise system implementation. ACIS 2004 Proceedings, 96.

Khalil, S., Winkler, T. J., & Xiao, X. (2017). Two Tales of Technology: Business and IT Managers' Technological Frames Related to Cloud Computing.

Laumer, S., Maier, C., & Weitzel, T. (2017). Information quality, user satisfaction, and the manifestation of workarounds: a qualitative and quantitative study of enterprise content management system users. European Journal of Information Systems, 26(4), 333-360.

Lis, T., & Paula, B. (2015). The Use of Cloud Computing by Students from Technical University–The Current State and Perspectives. Procedia Computer Science, 65, 1075-1084.

Lund-Jensen, R., Azaria, C., Permien, F. H., Sawari, J., & Bækgaard, L. (2016). Feral Information Systems, Shadow Systems, and Workarounds–A Drift in IS Terminology. Procedia Computer Science, 100, 1056-1063.

Mallmann, G. L., Maçada, A. C. G., & Oliveira, M. (2018). The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users. Business Information Review, 35(1), 17-28.

Mallmann, G. L., Maçada, A. C. G., Eckhardt, A. (2018). We are Social: a social influence perspective to investigate shadow IT usage. In Proceedings of European Conference on Information Systems, Portsmouth, UK.

Malaurent, J., & Avison, D. (2015). From an apparent failure to a success story: ERP in China—Post implementation. International Journal of Information Management, 35(5), 643-646.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. Disponível em http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. It Professional, 14(5), 53-55.

Müller, S. D., Holm, S. R., & Søndergaard, J. (2015). Benefits of Cloud Computing: Literature Review in a Maturity Model Perspective. CAIS, 37, 42.

Park, S. C., & Ryoo, S. Y. (2013). An empirical investigation of end-users' switching toward cloud computing: A two factor theory perspective. Computers in Human Behavior, 29(1), 160-170

Raden, N. (2005). Shedding light on shadow IT: Is Excel running your business. DSSResources. com, 26.

Rentrop, C., & Zimmermann, S. (2012). Shadow IT-Management and control of unofficial IT. In Proceedings of the 6th International Conference on Digital Society (pp. 98-102).

Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. Computers & Security, 45, 274-283.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. Information & management, (in press), 1-15. http://dx.doi.org/10.1016/j.im.2017.02.007

Singh, H. (2015). Emergence and consequences of drift in organizational information systems. In Proceedings of the Asia Conference on Information Systems (PACIS). Paper 202.

Shin, D. (2015). Beyond user experience of cloud service: Implication for value sensitive approach. Telematics and Informatics, 32(1), 33-44.

Shumarova, E., & Swatman, P. A. (2008). Informal ecollaboration channels: Shedding light on "shadow cit". In the Proceedings of LED 2008, Bled, Slovenia.

Steinhüser, M., Waizenegger, L., Vodanovich, V. & Richter, A. (2017). Knowledge Management without Management – Shadow IT in Knowledge-intense Manufacturing Practices. In Proceedings of the 25th European Conference on Information Systems, Guimarães, Portugal.

Turner, A. (2015). Generation Z: Technology and social interest. The Journal of Individual Psychology, 71(2), 103-113.

Turkle, S. (2011). Alone together: Why we expect more from technology and less from each other. Basic Books, New York.

Vogus, T. J., & Hilligoss, B. (2016). The underappreciated role of habit in highly reliable healthcare. BMJ Qual Saf, 25(3), 141-146.

Walterbusch, M., Fietz, A., & Teuteberg, F. (2017). Missing cloud security awareness: investigating risk exposure in shadow IT. Journal of Enterprise Information Management, 30(4), 644-665.

Walters, R. (2013). Bringing IT out of the shadows. Network Security, 2013(4), 5-11.

Webster, J. & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26, xiii-xxiii.

Weiß, F.; Leimeister, J. M. (2012). IT Innovations from the Consumer Market as a Challenge for Corporate IT. Business & Information Systems Engineering.

Zimmermann, S., Rentrop, C., & Felden, C. (2014). Managing shadow IT instances–a method to control autonomous IT solutions in the business departments.

Zimmermann, S., & Rentrop, C. (2014). On the emergence of shadow IT-a transaction cost-based approach. European Conference on Information Systems (ECIS).

Zimmermann, S., Rentrop, C., & Felden, C. (2017). A Multiple Case Study on the Nature and Management of Shadow Information Technology. Journal of Information Systems, 31(1), 79-101.