Machine Translated by Google

Revista Internacional de Gestão da Informação 40 (2018) 54–66

Listas de conteúdo disponíveis no ScienceDirect

Revista Internacional de Gestão da Informação

página inicial do periódico: www.elsevier.com/locate/ijinfomgt

O impacto da liderança relacional e do alinhamento social na eficácia do sistema de segurança da informação em organizações governamentais coreanas

Yun Ji Moona,1, Myeonggil Choib,1, Deborah J. Armstrongc,ÿ

aDepartamento de Sistemas de Informação Gerencial, Universidade Católica de Pusan, #57 Oryundae-ro, Geumjeong-gu, Busan, Coreia do Sul bDepartamento de Administração de Empresas, Universidade Chung-Ang, 84 Heukseok-ro, Dongjak-gu, Seul 06974, Coreia do Sul

[c] Departamento de Análise de Negócios, Sistemas de Informação e Cadeia de Suprimentos, Universidade Estadual da Flórida, Tallahassee, FL 32306, EUA

INFORMAÇÕES DO ARTIGO

Palavras-chave:
Diretor de segurança
Eficácia do sistema de segurança da informação (ISS)
Liderança relacional
Alinhamento social
Desempenho organizacional

RESUMO

Embora a tecnologia da informação tenha criado cada vez mais diversas oportunidades de inovação nas organizações, essas oportunidades têm causado sérios riscos associados à informação. Devido a esses riscos potenciais, a segurança da informação tornou-se uma grande preocupação nas organizações, e o papel do diretor de segurança começou a atrair a atenção de pesquisadores. Utilizando a perspectiva da teoria do capital social, este estudo visa explorar como o nível de liderança relacional do diretor de segurança impulsiona o alinhamento social entre executivos de negócios e de TI. Especificamente, estudamos como o alinhamento social influencia o conhecimento integrado, a eficácia do sistema de segurança da informação (SIS) e o desempenho organizacional. Dados empíricos de 102 organizações governamentais na República da Coreia confirmam o impacto da liderança relacional, do alinhamento social e da eficácia do ISS no desempenho organizacional.

1. Introdução

Segurança da informação é a prática de defender informações contra acesso, uso, divulgação, interrupção ou destruição não autorizados (Sen & Samanta, 2014). A dependência das tecnologias da informação e comunicação (TICs) dentro das organizações fez com que questões relacionadas às TICs se tornassem uma preocupação organizacional central (Knapp, Marshall, Rainer & Morrow, 2006). As perdas financeiras e/ou de reputação potencialmente em larga escala decorrentes de violações de segurança da informação levam as organizações a proteger vigorosamente seus ativos de informação. Por exemplo, uma pesquisa realizada pela PricewaterhouseCoopers (PwC, 2015) mostra que houve um aumento no número de organizações, tanto grandes quanto pequenas, que sofreram violações de segurança, com 90% das grandes organizações tendo sofrido uma violação de segurança. O Identity Theft Resource Center (ITRC, 2015) descobriu que o número de violações de dados nos Estados Unidos (EUA) aumentou 8,1% de 2014 a 2015, e o custo do crime cibernético somente nos EUA é de aproximadamente US$ 100 bilhões por ano (Forbes, 2016a,b).

Embora as violações de segurança sejam uma preocupação para as organizações, elas são especialmente críticas para órgãos governamentais, onde a violação de informações e ativos pode causar problemas sociais generalizados. Por exemplo, a Coreia do Norte lançou um ataque cibernético contra a Coreia do Sul em 2016, e uma violação massiva de dados expôs dados pertencentes a uma rede de internet. Shopping center (CNN Tech, 2017). De acordo com a BBC (2014), os números de identificação e dados pessoais de cerca de 80% dos 50 milhões de sul-coreanos foram roubados de bancos e outros alvos. Portanto, o governo está considerando emitir novos números de identificação para todos os cidadãos com mais de 17 anos, o que custará bilhões de dólares.

Assim, a segurança da informação tornou-se um foco estratégico e um desafio para organizações governamentais. No entanto, permanece a questão sobre qual é a abordagem mais eficaz para a gestão da segurança da informação, especialmente em uma organização governamental.

As principais contramedidas de gerenciamento de segurança da informação exploradas na literatura são principalmente de natureza técnica (por exemplo, Goodhue & Straub, 1991; Nance & Straub, 1988; Straub, 1990; Straub & Welke, 1998) e priorizam tecnologias sofisticadas.

Como a segurança é percebida como uma questão técnica, a equipe de segurança da informação tende a ser posicionada em funções técnicas de baixo nível que se concentram na implementação de tecnologias (Kayworth & Whitten, 2010).

No entanto, uma visão mais recente sugere uma estratégia sociotécnica, que enfatiza a importância de integrar a segurança aos aspectos principais do negócio e incorporar o elemento humano na concepção de programas de segurança eficazes (Goles, White e Dietrich, 2005; Kayworth e Whitten, 2010). Uma estratégia de segurança sociotécnica incorpora competência técnica, bem como elementos sociais e organizacionais. A segurança da informação é entendida como um conceito que

Autor correspondente em: 821 Academic Way, Tallahassee, FL 32312, EUA.
Endereços de e-mail: yjmoon@cup.ac.kr (YJ Moon), mgchoi@cau.ac.kr (M. Choi), djarmstrong@business.fsu.edu (DJ Armstrong).
[1] Co-primeiros autores.

https://doi.org/10.1016/j.ijinfomgt.2018.01.001
Recebido em 25 de agosto de 2017; Recebido em formato revisado em 19 de dezembro de 2017; Aceito em 4 de janeiro de 2018
Disponível online em 03 de fevereiro de 2018
0268-4012/ © 2018 Elsevier Ltd. Todos os direitos reservados.

Machine Translated by Google

abrange fatores como tecnologias de segurança, relações sociais entre os membros da organização, estratégia e políticas de segurança. Portanto, este estudo identifica um Sistema de Segurança da Informação (SIS) como um conjunto de fatores interdependentes que interagem regularmente para proteger as informações dentro de uma organização.

Um grande desafio enfrentado pelos executivos de segurança é a necessidade de equilibrar as necessidades de informação do negócio com a necessidade de proteger os ativos de informação. Um ISS eficaz deve ser orientado para o negócio, mas também segura, portanto, o alinhamento entre as funções de negócios e de TI é fundamental (Kayworth & Whitten, 2010). Kayworth e Whitten (2010) sugerem que a falta de alinhamento entre as tarefas de negócios e as tecnologias disponíveis para realizá-las frequentemente resulta em segurança da informação ineficaz. A literatura discute a ideia de alinhamento entre negócios e TI[2] para a otimização do ISS (por exemplo, Bergeron, Raymond & Rivard, 2004; Chan, Huff, Barclay & Copeland, 1997; Reich & Benbasat, 1996) e a ideia de que a alta gerência desempenha um papel fundamental na obtenção da eficácia do ISS. Portanto, este artigo discute o alinhamento entre negócios e TI entre os executivos de ambas as unidades.

De acordo com Wagner, Beimborn e Weitzel (2014), existem três visões principais sobre o alinhamento entre negócios e TI: alinhamento estrutural, alinhamento estratégico e alinhamento social. O alinhamento estrutural enfatiza a importância de mecanismos formais de coordenação para alcançar resultados, como a codificação dos direitos de tomada de decisão da unidade de TI (p. ex., Chan & Reich, 2007). Alinhamento estratégico significa que o plano estratégico de TI está alinhado com o plano estratégico organizacional, e esse alinhamento pode ser encontrado nos artefatos organizacionais/departamentais, como a declaração de missão (p. ex., Bergeron et al., 2004; Chan et al., 1997; Reich & Benbasat, 1996). O alinhamento social tradicionalmente enfatiza a interconexão entre os domínios entre os executivos de negócios e de TI, o que permite a criação de conhecimento integrado (p. ex., Chan, 2002; Wagner et al., 2014). Recentemente, o foco da pesquisa sobre alinhamento entre negócios e TI mudou para estudar os aspectos sociais do alinhamento, destacando a importância de estruturas informais baseadas em relacionamentos (Chan, 2002).

Wagner et al. (2014) consideram o alinhamento social como o capital social existente entre as unidades de negócio e de TI, cujo resultado é a integração do conhecimento de negócio e de TI. Capital social é “a boa vontade disponível para indivíduos ou grupos. Sua fonte reside na estrutura e no conteúdo das relações sociais do ator. Seus efeitos decorrem da informação, influência e solidariedade que disponibiliza ao ator” (Adler & Kwon, 2002, p. 23). Consistente com essa visão está o conceito de liderança relacional, que se baseia em relacionamentos interpessoais e é tradicionalmente visto como o padrão de interações recíprocas entre líderes e liderados (Gittell & Douglass, 2012). O conceito de liderança relacional foi expandido mais recentemente para incluir relacionamentos que ocorrem em uma rede social organizacional mais ampla e é considerado um importante facilitador para o aprimoramento do capital social, bem como do conhecimento integrado em uma organização (Uhl-Bien, 2006). Conhecimento integrado é definido como “a capacidade de uma empresa de executar repetidamente uma tarefa produtiva que se relaciona direta ou indiretamente com sua capacidade de criar valor por meio da transformação de insumos em produtos” (Grant, 1996, p. 377). O conhecimento integrado é desenvolvido em etapas (Clark & Fujimoto, 1991), começando com o foco em capacidades que abordam tarefas especializadas e, em seguida, movendo o foco para a integração das capacidades específicas da tarefa em capacidades multifuncionais mais amplas.

Neste estudo, vemos o alinhamento social como o capital social que existe entre os executivos de negócios e de TI, em que o resultado é
Conhecimento integrado. Dentro da unidade de TI, o diretor de segurança (CSO) é um executivo sênior responsável pelo desenvolvimento e supervisão de todas as políticas e programas relacionados à segurança. O CSO é cada vez mais solicitado a colaborar com os executivos de negócios e a buscar proativamente criar oportunidades para que a TI atenda às necessidades dos negócios.
Este estudo utiliza a teoria do capital social para considerar o alinhamento de um ponto de vista social.
perspectiva, e vê isso como as ligações sociais entre executivos em
as unidades de negócios e o CSO na unidade de TI.

Embora pesquisas anteriores argumentem que o alinhamento entre negócios e TI facilita o desempenho organizacional, Kearns e Sabherwal (2006–2007); Sabherwal e Chan (2001) apontam que não houve pesquisas teóricas e empíricas suficientes conduzidas sobre as relações entre os facilitadores e os resultados do alinhamento entre negócios e TI. Embora pesquisas tenham estabelecido a influência do alinhamento entre negócios e TI no desempenho organizacional (Reich & Benbasat, 2000; Sabherwal & Chan, 2001), o que está ausente é uma exploração dos prováveis fatores impulsionadores e intervenientes. O presente estudo tenta preencher essa lacuna identificando como o alinhamento entre negócios e TI afeta o desempenho organizacional por meio de relacionamentos sociais informais. Especificamente, este artigo sugere um modelo de pesquisa integrado fundamentado na teoria do capital social que inclui os facilitadores do alinhamento social, os mecanismos de alinhamento social e os resultados do alinhamento. Em resumo, o presente artigo persegue as três questões de pesquisa a seguir: (1) Como a liderança relacional de CSOs em organizações governamentais coreanas afeta o alinhamento social entre negócios e TI?; (2) Como o conhecimento integrado de negócios e TI medeia a relação entre alinhamento social e eficácia do ISS?; e (3) Como o conhecimento integrado influencia o desempenho organizacional?

2. Fundamentação teórica e revisão bibliográfica

Este artigo propõe um modelo da influência da liderança relacional de CSOs no alinhamento social entre executivos de negócios e de TI, e os resultados do alinhamento social. Este modelo utiliza a liderança relacional (Tsai, Dionne, Wang e Spain, 2017; Uhl-Bien, 2006) e o alinhamento social (Chan, 2002; Kayworth e Whitten, 2010; Karahanna e Preston, 2013; Wagner et al., 2014) para prever a eficácia do ISS e o desempenho organizacional. Revisamos os principais constructos do nosso modelo conceitual e descrevemos os fundamentos teóricos que sustentam os relacionamentos nele contidos.

2.1. Liderança relacional

A liderança relacional é exercida em relacionamentos interpessoais (Hiller, Day & Vance, 2006) e é definida como um padrão de interações recíprocas entre líderes e liderados, no qual os indivíduos dão sentido às situações, determinam o que deve ser feito e como fazê-lo (Gittell & Douglass, 2012). Liderança relacional refere-se à liderança que oferece suporte e se concentra no desenvolvimento de relacionamentos de trabalho de alta qualidade e confiança dentro da organização (Brower, Schoorman & Tan, 2000; Uhl-Bien, Graen & Scandura, 2000). A díade relacional (líder e liderado) cria conhecimento interpessoal que pode ser usado para processar informações sociais e demonstrar comportamentos sociais (Baldwin, 1997).

Recentemente, pesquisas expandiram a conceituação de líder, passando de um indivíduo em uma posição formalizada de influência dentro da organização (por exemplo, supervisor) para indivíduos que desenvolveram influência social dentro da organização (por exemplo, usuário líder). Uhl-Bien (2006, p. 655) refere-se à liderança relacional como "um processo de influência social por meio do qual a coordenação emergente (isto é, a ordem social em evolução) e a mudança (por exemplo, novos valores, atitudes, abordagens, comportamentos e ideologias) são construídas e produzidas". Assim, a liderança relacional pode envolver indivíduos que transcendem as fronteiras organizacionais tradicionais.

2.2. Alinhamento social e conhecimento integrado

Na era do conhecimento, a importância de ativos e recursos intangíveis, como relacionamentos sociais e conhecimento coletivo, nas organizações está se tornando cada vez mais relevante (Nahapiet & Ghoshal, 1998). A teoria do capital social propõe que uma organização seja entendida como "uma comunidade social especializada na velocidade e eficiência na criação e transferência de conhecimento" (Kogut & Zander, 1996, p. 503).

[2] Por "negócio" estamos nos referindo a áreas funcionais dentro de uma organização fora da função de TI, como finanças ou manufatura.

Machine Translated by Google

As relações sociais entre os membros de uma organização são vistas como capital social, que pode ser definido como a soma dos recursos incorporados, disponíveis por meio e derivados da rede de relacionamentos de um indivíduo (Nahapiet & Ghoshal, 1998), e são considerados um recurso para ação e transferência de conhecimento (Burt, 1997). Nahapiet e Ghoshal (1998) argumentam que o capital social é um conceito multidimensional composto por dimensões estruturais, cognitivas e relacionais. De acordo com Nahapiet e Ghoshal (1998), a dimensão estrutural se refere ao padrão geral de conexões entre os indivíduos – em outras palavras, quem você alcança e como você os alcança. Se houver colegas (ou seja, laços de rede) que fornecem acesso a recursos em uma organização, esses colegas podem fornecer canais de troca social para transmissão de conhecimento. A dimensão cognitiva se refere aos recursos que fornecem representações, interpretações e sistemas de significado compartilhados entre os indivíduos. Uma parte essencial de uma troca social é que pelo menos algum nível de contexto compartilhado seja desenvolvido (Boisot, 1995). A dimensão relacional concentra-se nas facetas dos relacionamentos específicos que as pessoas mantêm, como confiança, confiabilidade e normas. Se os indivíduos não estão dispostos a confiar nos outros para participar de uma troca social, o conhecimento integrado não pode ser facilmente acumulado.

Em consonância com a teoria do capital social, o alinhamento social enfatiza a interconexão entre áreas de negócio e executivos de TI, o que facilita a criação de conhecimento integrado (p. ex., Chan, 2002; Kayworth & Whitten, 2010; Wagner et al., 2014). O alinhamento social também pode ser considerado como composto por três dimensões focadas em relacionamentos – estrutural, cognitiva e relacional (Karahanna & Preston, 2013; Wagner et al., 2014), denominadas conexões.

A ligação estrutural entre executivos de negócios e de TI indica a estrutura de rede encontrada em reuniões e conferências de projetos, que se beneficia do contato direto frequente e de equipes de projeto multifuncionais (Chan, 2002; Chan & Reich, 2007) para desenvolver o entendimento mútuo (Lind & Zmud, 1991). A ligação cognitiva refere-se ao grau em que executivos de negócios e de TI conhecem os códigos, a linguagem e as perspectivas uns dos outros (Nahapiet & Ghoshal, 1998). Por meio da linguagem e do vocabulário compartilhados e do desenvolvimento de narrativas coletivas, executivos de negócios e de TI podem se entender em um nível mais profundo (Reich & Benbasat, 2000). A ligação relacional indica as facetas específicas dos relacionamentos, como confiança e confiabilidade (Nahapiet & Ghoshal, 1998). A confiança entre indivíduos em unidades de negócios e de TI aumenta a cooperação, e a cooperação gera mais confiança (Chong, Ooi, Chan & Darmawan, 2011; Jones & George, 1998). A integração bem-sucedida do conhecimento exige que os indivíduos sejam motivados a participar do processo de integração (Nahapiet & Ghoshal, 1998). Consequentemente, a confiança e a cooperação fomentam a confiança coletiva ao longo do tempo, o que pode gerar participação e, por fim, produzir conhecimento integrado.

2.3. Eficácia do sistema de segurança da informação (ISS)

Em termos empresariais, a eficácia nas organizações pode ser vista no contexto da realização de objetivos ou da obtenção de resultados. Da mesma forma, a eficácia do ISS refere-se à extensão em que as metas do programa de ISS são alcançadas e as informações organizacionais são suficientemente protegidas (Hwang & Choi, 2017). A eficácia do ISS é o grau em que a organização estabelece controles que previnem danos causados por ameaças externas e internas. Três tipos de fatores têm sido utilizados para mensurar a eficácia do ISS: fatores organizacionais, como treinamento de usuários e aplicação de políticas de segurança (Chen, Ramamurthy e Wen, 2012; Son, 2011; Straub, 1990; Warkentin e Willison, 2009), fatores tecnológicos, como ferramentas de hardware e software (D'arcy e Herath, 2011; Herath e Rao, 2009; Kankanhalli, Teo, Tan e Wei, 2003; Straub, 1990), e fatores híbridos, como o número de horas semanais dedicadas à prevenção e dissuasão de ameaças ao ISS e a dedicação da alta administração à segurança de dados (Kankanhalli et al., 2003; Straub, 1990). Pesquisas anteriores sobre a eficácia do ISS tenderam a se concentrar em um aspecto da abordagem. O presente estudo utiliza a perspectiva de que a eficácia do ISS é alcançada por meio dos efeitos combinados de fatores tecnológicos.

fatores baseados na organização e outros fatores projetados para reduzir ameaças de fontes internas e externas (Hwang & Choi, 2017).

3. Modelo de pesquisa e hipóteses

3.1. Liderança relacional e alinhamento social

Como mencionado anteriormente, a liderança relacional concentra-se no desenvolvimento de relacionamentos de trabalho de alta qualidade e confiança (Brower et al., 2000; Uhl-Bien et al., 2000) por meio de interações frequentes para modelar o comportamento e, assim, capacitar os funcionários a trabalharem como parceiros. Embora as tarefas específicas do CSO possam diferir entre as organizações, um CSO não é simplesmente um especialista técnico que introduz, desenvolve e implementa tecnologia, mas também é responsável pela operação e controle do ISS em nível empresarial. Um CSO é responsável por proteger os ativos intelectuais de uma organização e desempenha o papel de um especialista técnico, bem como de um estrategista gerencial. Além disso, os CSOs são frequentemente solicitados a gerenciar recursos humanos nas organizações (Soomro, Shah & Ahmed, 2016). Como a maioria das violações de dados e vulnerabilidades do ISS ocorrem devido aos funcionários (Sarkar, 2010; Vance, Lowry e Eggett, 2013), os humanos se tornam um dos elementos mais críticos na eficácia do ISS.

Para melhorar o ISS e o alinhamento entre negócios e TI, os CSOs comunicam a importância da gestão do ISS e veem as questões de segurança tanto de uma perspectiva de negócios quanto tecnológica. Constatou-se que os CSOs que adotam liderança relacional apresentam melhor alinhamento entre os executivos de negócios e de TI e maior sucesso organizacional (Kayworth & Whitten, 2010; Soomro et al., 2016). Por meio do compartilhamento de conhecimento em interações individuais, reuniões ou conferências de projeto, o CSO e os executivos de negócios conseguem conversar sobre questões de negócios, bem como sobre questões relacionadas à tecnologia. Ter capital social disponível em um grupo pode aumentar a eficácia do grupo quando baseado em fortes relacionamentos de confiança que se desenvolvem dentro e além das fronteiras do grupo (Oh, Labianca & Chung, 2006). Constatou-se que a liderança relacional influencia positivamente o capital social (Uhl-Bien, 2006), e o alinhamento social ocorre quando o capital social é desenvolvido no contexto de um ambiente de trabalho (Wagner et al., 2014). Assim, hipotetizamos que esses mecanismos ocorrerão no contexto CSO-executivo empresarial da seguinte forma:

Hipótese 1. O nível de liderança relacional exercido pelo CSO influenciará positivamente o nível de alinhamento social entre o CSO e os executivos da empresa.

H1a. O nível de liderança relacional exercido pelo CSO influenciará positivamente o nível de vínculo estrutural entre o CSO e os executivos da empresa.

H1b. O nível de liderança relacional exercido pelo CSO influenciará positivamente o nível de ligação cognitiva entre o CSO e executivos de negócios.

H1c. O nível de liderança relacional exercido pelo CSO influenciará positivamente o nível de vínculo relacional entre o CSO e os executivos da empresa.

3.2. Alinhamento social e conhecimento integrado

O alinhamento social entre executivos de negócios e de TI é um processo contínuo e inclui o compartilhamento de conhecimento de domínio de negócios e de TI, bem como a integração de conhecimento (Kearns & Sabherwal, 2006; Wagner et al., 2014). O conhecimento de domínio compartilhado permite que “executivos de TI e de negócios possam participar dos processos-chave uns dos outros e respeitar as contribuições e os desafios únicos uns dos outros” (Reich & Benbasat, 2000, p. 86); e o conhecimento integrado resulta quando as pessoas interagem e combinam suas informações para criar novos conhecimentos (Grant, 1996; Okhuysen & Eisenhardt, 2002; Wagner et al., 2014). O alinhamento social deve ajudar a estabelecer uma linguagem comum, melhorando

Machine Translated by Google

comunicação e potencialmente atuar como um impulsionador do conhecimento integrado. As estratégias de negócios mudam com as situações de mercado e as incertezas ambientais, e as estratégias de ISS refletem as necessidades do negócio. Se uma unidade funcional muda, mas a unidade de TI não se ajusta à mudança, pode ocorrer falta de alinhamento. A falta de alinhamento pode levar à escassez de conhecimento integrado entre os executivos de negócios e de TI, o que pode prejudicar o sucesso organizacional (Chen, Sun, Helms & Jih, 2008). Assim, esta pesquisa propõe as seguintes hipóteses relacionadas ao conhecimento integrado:

Hipótese 2. O nível de alinhamento social entre o CSO e os executivos de negócios influenciará positivamente o nível de conhecimento integrado.

H2a. O nível de ligação estrutural entre o CSO e os executivos da empresa influenciará positivamente o nível de conhecimento integrado.

H2b. O nível de vínculo cognitivo entre o CSO e os executivos da empresa influenciará positivamente o nível de conhecimento integrado.

H2c. O nível de vínculo relacional entre o CSO e os executivos da empresa influenciará positivamente o nível de conhecimento integrado.

3.3. Eficácia do sistema integrado de segurança do conhecimento e da informação (ISS)

Lembre-se de que a eficácia do ISS refere-se à capacidade do ISS de proteger contra o uso não autorizado ou o uso indevido deliberado de ativos de informação por pessoas (Straub, 1990). Uma estratégia eficaz de ISS precisa enfatizar a importância de considerar tanto o contexto tecnológico quanto o socioorganizacional (Kayworth & Whitten, 2010; Soomro et al., 2016; Wagner et al., 2014). Por exemplo, o uso de estruturas organizacionais formais (ou seja, arranjo hierárquico de relacionamentos entre funções dentro de uma organização; Meyer & Rowan, 1977) para definir direitos e responsabilidades na tomada de decisões pode ajudar a alcançar a eficácia do ISS. Essa rede formal de relacionamentos entre executivos de negócios e de TI em uma organização pode incentivar a interação entre os membros da rede e facilitar a troca de conhecimento, pois os indivíduos sabem com quem se comunicar para "fazer as coisas" (Karahanna & Preston, 2013). Os processos de coordenação alcançados por meio da comunicação e da troca de conhecimento podem facilitar a gestão eficaz do ISS (Kayworth & Whitten, 2010). Assim, quanto mais integrado o conhecimento estiver dentro da organização, maiores serão as oportunidades de explorar mecanismos para prevenir violações de segurança. Assim, esta pesquisa propõe a seguinte hipótese:

Hipótese 3. O nível de conhecimento integrado entre o CSO e os executivos de negócios influenciará positivamente a eficácia do ISS.

3.4. Eficácia do ISS e desempenho organizacional

Conforme mencionado anteriormente, constatou-se que o uso eficaz de ISS por meio de abordagens tecnológicas e organizacionais influencia positivamente o desempenho geral das organizações (Gupta, 2011; Moffat & Nzulwa, 2016); e o uso ineficaz de ISS causou danos financeiros e reputacionais às organizações, o que, por sua vez, afetou severamente o desempenho organizacional e a avaliação de mercado (Gupta, 2011; Kraemer, Carayon & Clem, 2009). Com base em descobertas anteriores, levantamos a hipótese de que existe uma relação positiva entre a eficácia do ISS e o desempenho organizacional no contexto de organizações governamentais na República da Coreia.

Hipótese 4. A eficácia do ISS influenciará positivamente o desempenho organizacional.

3.5. O efeito moderador do conhecimento técnico

O CSO frequentemente gerencia uma infinidade de funções de segurança administrativa, políticas, sistemas, pessoal, até segurança física, como instalações e controle de acesso (Soomro et al., 2016).
Portanto, as OSCs devem ter não apenas uma ampla compreensão dos aspectos técnicos de TI (por exemplo, infraestrutura e aplicativos), mas também uma ampla gama de conhecimentos de domínio empresarial, jurídicos e gerenciais para se prepararem para discussões, questões, problemas e conflitos com várias partes interessadas.

No entanto, em muitas organizações governamentais na República da Coreia, o departamento de segurança é organizado em torno de uma equipe de TI altamente técnica, cuja função é instalar uma ferramenta de ISS. Em contraste, um gerente geral, geralmente sem conhecimento técnico ou com conhecimento limitado, é frequentemente nomeado CSO. Há vários casos documentados em que um gerente desconhecedor de vários aspectos de TI se torna CSO e, como resultado, limita o estabelecimento de uma estratégia de ISS eficaz (Hankook Newpaper, 2015; Yonhap Newspaper, 2015). CSOs com maior nível de expertise técnica estarão mais aptos a preencher a lacuna entre a funcionalidade das tecnologias de segurança e as questões de negócios (Whitten, 2008). Um CSO com sólido conhecimento técnico está em melhor posição para entender como as estratégias de ISS podem ser integradas às estratégias de negócios e como elas podem ser implementadas ou aprimoradas com a tecnologia. Os CSOs devem ser capazes de compreender os vários aspectos da proposta de valor das iniciativas de segurança e comunicá-los efetivamente a outros executivos. Assim, esta pesquisa propõe a seguinte hipótese:

Hipótese 5. O conhecimento técnico do CSO moderará a relação entre o conhecimento integrado e a eficácia do ISS, de modo que o nível de conhecimento técnico do CSO aumentará a força da relação entre o conhecimento integrado e a eficácia do ISS.

A Fig. 1 resume as relações exploradas neste estudo.

4. Metodologia de pesquisa

Neste estudo, utilizamos uma abordagem quantitativa para testar o modelo proposto. Começamos fornecendo detalhes sobre as medidas, a coleta de dados e os procedimentos de análise. Em seguida, apresentamos os resultados do estudo.

4.1. Mensuração de constructos

Mensuramos cada construto utilizando escalas previamente validadas e adaptamos alguns dos itens para o contexto deste estudo. O Apêndice A apresenta os construtos, definições, itens e fontes das medidas utilizadas neste estudo. Todas as medidas são reflexivas e utilizam uma escala Likert de cinco pontos. Diversos fatores que não estão incluídos no modelo de pesquisa, mas que foram sugeridos na literatura como influenciadores da eficácia do ISS, são incluídos como variáveis de controle. Essas variáveis incluem:
Inclui gênero, nível educacional, número de certificações e tempo de serviço como CSO. Estudos anteriores indicaram que o número de anos de trabalho como diretor de segurança da informação, bem como treinamento e educação, podem influenciar a eficácia do ISS (Choi, 2016); portanto, incluímos esses fatores em nosso estudo. Em vez de focar apenas no desempenho financeiro, medimos o desempenho organizacional como composto pelo desempenho financeiro e pelo desempenho dos processos de negócios (por exemplo, utilização de informações na execução de tarefas).

4.2. Coleta de dados

Questionários em papel foram distribuídos por agentes de segurança da informação de nível médio do governo central sul-coreano e preenchidos pelas OSCs de cada departamento. O cargo de OSC é obrigatório em organizações governamentais e é nomeado pelo governo central e por funcionários públicos na Coreia do Sul (Kim, 2012). Os questionários foram enviados a 43 departamentos e conselhos do governo central sul-coreano e a 78 instituições públicas (por exemplo, o Serviço de Compensação e Bem-Estar do Trabalhador da Coreia) na Coreia do Sul. Dos 121

Machine Translated by Google

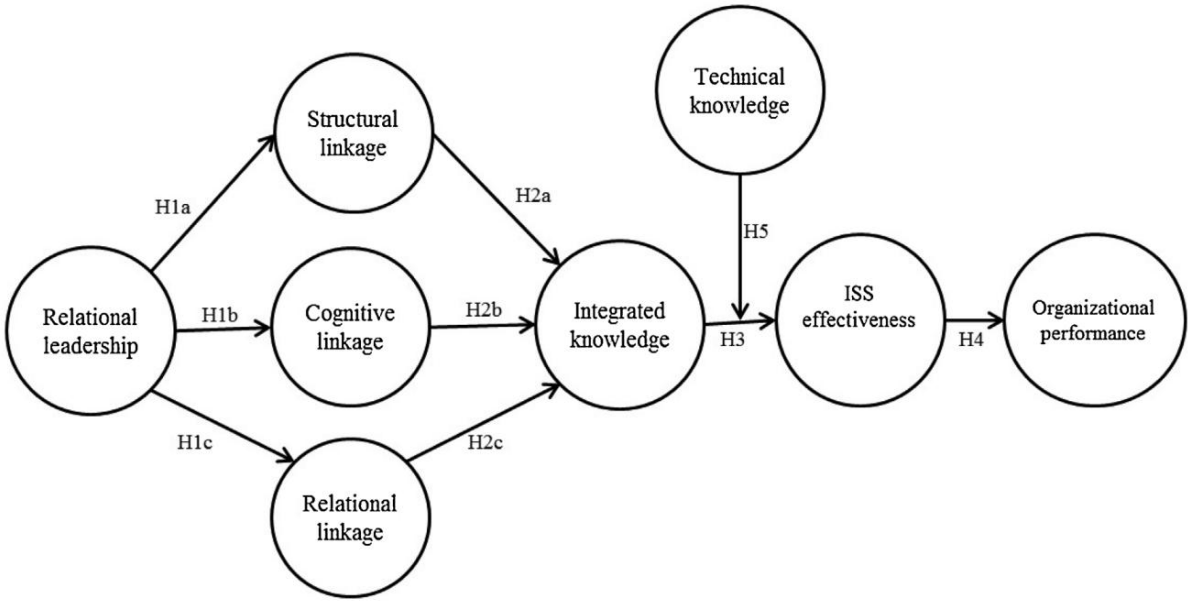


Fig. 1. Modelo conceitual.

Tabela 1
Perfis dos entrevistados.

Item	Variável	Freqüência	Percentagem(%)
Gênero	Macho	99	97,1
	Fêmea	3	2.9
Idade	Menos de 45 anos	2	2.0
	46–50 anos	13	12,7
	51–55 anos	34	33,4
	56–60 anos	46	45.1
	Acima de 61 anos	7	6.8
Experiência de trabalho	Menos de 10 anos 11–	30	29,4
	20 anos 21–30	13	12,7
	anos 31–40	42	41.2
	anos	16	15,7
	Mais de 40 anos	1	1.0
Permanência do CSO	Menos de 1 ano 1–3	22	21,6
	anos 3–5	66	64,7
	anos 5–10	7	6.9
	anos	1	1.0
	Mais de 10 anos	6	5.9
Posse de TI	Menos de 1 ano 1–10	28	27,4
	anos 10–20	59	57,7
	anos 20–30	2	2
	anos	10	9,9
	Mais de 30 anos	3	3.0
Educação	Diploma do ensino médio	1	1.0
	Faculdade Júnior	2	2.0
	Bacharel	22	21,6
	Mestrado ou superior	77	75,5
Número de Certificações	0	73	71,6
	1	12	11.8
	2	7	6.9
	3	5	4.9
	4	4	3.9
	Mais de 5	1	1.0

questionários em papel enviados, 108 foram devolvidos e os questionários foram coletados de maio de 2015 a novembro de 2015. Após a remoção de seis questionários com respostas incompletas ou não confiáveis, 102 válidos questionários permaneceram, para uma taxa de resposta efetiva de 84,3%. A Tabela 1 apresenta as características dos entrevistados. Conforme demonstrado em Tabela 1, a maioria dos entrevistados era do sexo masculino (97,1%) e estava entre 51 e 60 anos (78,6%). Cerca de metade (41,2%) dos entrevistados tinham trabalharam por 21 a 30 anos e 64,7% trabalharam como CSO por 1 a 3 anos. A maioria dos entrevistados (71,6%) não possuía nenhuma certificação relacionada à TI, mas eram bem educados (75,5% tinham obtido um mestrado ou acima).

5. Análise de dados e resultados

Utilizamos um processo multietapas para avaliar o modelo de pesquisa. SPSS versão 21 e SmartPLS versão 2.0 (Ringle, Wende, & Will, 2005) foram usados na abordagem multiestágio. Na primeira etapa, examinamos o modelo de medição para propriedades psicométricas adequadas (ou seja, modelo de medição), enquanto na segunda etapa nos concentramos em testar o modelo de pesquisa e as hipóteses (ou seja, modelo estrutural). Tabela 2 mostra as estatísticas descritivas.

Antes da análise dos dados, foi realizada uma análise fatorial exploratória utilizando a análise de componentes principais. Foi realizada a rotação fatorial ortogonal-varimax. A Tabela 3 apresenta os resultados da análise fatorial exploratória. análise fatorial.

Os mínimos quadrados parciais (PLS) foram usados para avaliar empiricamente a modelo teórico (Gefen & Straub, 2005; Thatcher & Perrewe, 2002). O Smart PLS 2.0 (Ringle et al., 2005) foi usado para análise de dados e 1500 amostras bootstrap foram usadas para calcular empiricamente erros padrão e avaliar significância estatística (Gefen, Rigdon, & Straub, 2011).

5.1. Modelo de medição

O PLS consiste em duas seções principais. Na primeira seção, o modelo de mensuração e sua validade (convergente e discriminante) são avaliados (Gefen & Straub, 2005). Utilizamos o procedimento descrito por Chin

Tabela 2
Estatística descritiva.

	Significar	DST	MÍNIMO	MÁXIMO
Ligação estrutural	3.163	1.254	1	5
Ligação relacional	4.754	0,403	3	5
Ligação cognitiva	4.277	0,457	3	5
Conhecimento integrado	4.585	0,543	3	5
Desempenho organizacional	4.111	0,716	2	5
Eficácia da ISS	4.557	0,453	3	5
Liderança relacional	4.608	0,404	3	5
Conhecimento técnico	4.585	0,054	2	5

Machine Translated by Google

Tabela 3
Cargas fatoriais.

		Factor						
		1	2	3	4	5	6	7
Organizational Performance	ORG_PRM4	.940	.115	.112	.033	.026	.104	.037
	ORG_PRM2	.870	.238	.100	-.137	.032	.056	.114
	ORG_PRM3	.868	.290	.131	.008	.065	.022	.114
	ORG_PRM1	.845	-.018	.086	.189	.095	.093	.049
	ORG_PRM7	.701	.186	.184	.381	.217	.151	.013
	ORG_PRM5	.614	.260	.184	.375	.182	.153	.117
Relational leadership	REL_LED6	.157	.833	.276	.119	.066	.210	.088
	REL_LED7	.260	.713	.257	.157	.126	.206	.176
	REL_LED4	.332	.629	.013	-.180	.121	.339	.141
	REL_LED1	.171	.600	.208	.429	.025	.034	.065
	REL_LED5	.266	.588	.292	.262	.037	.382	.012
	REL_LED9	.187	.540	.207	.349	-.022	.362	.203
ISS Effectiveness	EFFCT4	.182	.105	.829	.208	.144	.060	.083
	EFFCT5	.313	.135	.742	.037	-.020	.346	.231
	EFFCT3	.141	.433	.720	.221	.193	.010	-.027
	EFFCT6	.271	.206	.707	.047	-.006	.386	.252
	EFFCT2	-.009	.147	.703	.041	.068	.078	.030
Relational linkage	LIN_REL2	.100	.088	.167	.801	.044	.207	.237
	LIN_REL3	.104	.099	.067	.728	.000	.269	.176
	LIN_REL1	.073	.485	.116	.599	-.032	.105	.175
Structural linkage	LIN_STR3	.099	.061	.115	.017	.940	-.010	.021
	LIN_STR1	.036	.103	.093	.047	.932	.123	-.051
	LIN_STR2	.180	.018	.053	-.010	.888	.016	.114
Integrated knowledge	INT_KNO1	.064	.256	.124	.365	.007	.716	.008
	INT_KNO3	.254	.324	.255	.256	.117	.700	.160
	INT_KNO2	.128	.352	.318	.230	.118	.640	.220
Cognitive linkage	LIN_COG2	.107	.188	.237	.231	.029	.047	.801
	LIN_COG1	.169	.134	.065	.302	.059	.210	.790

Tabela 4
Validade e confiabilidade dos constructos reflexivos.

	Composto AVE confiabilidade	R quadrado de Cronbach	alfa
Liderança relacional	0,650 0,917		0,891
Ligação cognitiva	0,817 0,899	0,234	0,776
Ligação relacional	0,703 0,876	0,378	0,789
Ligação estrutural	0,875 0,955	0,041	0,929
Conhecimento integrado	0,789 0,912	0,419	0,866
Eficácia da ISS	0,694 0,918	0,368	0,887
Organizacional desempenho	0,749 0,947	0,237	0,933

(1998) para medidas reflexivas para avaliar a confiabilidade dos construtos e a validade convergente e discriminante do modelo. O valor do confiabilidade do indicador, confiabilidade composta e variância média extraída (AVE) avaliam a validade convergente (Fornell & Larcker, 1981). A Tabela 4 mostra que os AVEs estavam acima do limite de 0,5 (Chin 1998; Fornell & Larcker 1981; Thatcher & Perrewe, 2002), o composto as confiabilidades (CR) foram todas maiores que 0,7 (Thatcher & Perrewe, 2002), e os valores do alfa de Cronbach foram maiores que 0,7, indicando que os dados eram confiáveis (Bagozzi & Yi, 1988).

Para avaliar a validade discriminante dos constructos, utilizamos o procedimento recomendado por Fornell & Larcker (1981). O critério de Fornell-Larcker sugere que a validade discriminante é demonstrada quando a raiz quadrada de cada AVE é maior que a correlação dos construtos com qualquer outro constructo latente (Fornell & Larcker, 1981). Tabela 5 mostra a raiz quadrada da variância média extraída (AVE) e a correlações entre construtos reflexivos. Todos os construtos correlacionados mais fortemente com suas próprias medidas do que com qualquer um dos outros construções. Isso indica validade convergente e discriminante. Finalmente, As cargas cruzadas foram calculadas e todos os indicadores apresentaram cargas mais altas com seus respectivos construtos do que com qualquer outro indicador reflexivo. construir (Chin, 1998).

Além disso, analisamos os dados em busca de indicações de doenças comuns viés do método. Utilizamos o método baseado em Podsakoff, MacKenzie, Lee, e Podsakoff (2003) e análise PLS por Liang, Saraf, Hu e Xue (2007). Os indicadores de todos os construtos foram associados reflexivamente ao fator método. A variância de cada indicador foi explicada pelo construções principais e pelo método o fator foi calculado (Chin, Thatcher e Wright, 2012). A Tabela 6 mostra que a maioria dos carregamentos do método não foram significativos. Além disso, enquanto a variância média explicada substantiva para um indicador foi de 0,709, o método comum baseado a variância foi de apenas 0,038. Com base nos resultados deste teste, acreditamos o viés do método comum não foi uma ameaça significativa neste estudo.

Em conjunto, os resultados dos testes demonstram que o modelo de medição atende aos padrões rigorosos esperados (Straub, Boudreau, & Gefen, 2004), e apresentamos a seguir a avaliação do modelo estrutural.

Machine Translated by Google

Tabela 5
Correlação dos escores das variáveis latentes.

	Integrado conhecimento	Eficácia do ISS Cognitiva	ligação	Relacional ligação	Estrutural ligação	Organizacional Desempenho	Relacional liderança
Conhecimento integrado	0,888						
Eficácia da ISS	0,606**	0,833					
Ligação cognitiva	0,495**	0,432**	0,903				
Ligação relacional	0,599**	0,430**	0,543**	0,838			
Ligação estrutural	0,209*	0,224*	0,119	0,092	0,935		
Organizacional desempenho	0,463**	0,486**	0,366**	0,374**	0,259**	0,865	
Liderança relacional	0,742**	0,640**	0,483**	0,615**	0,203**	0,571**	0,806

A raiz quadrada da variância média extraída (AVE) está na diagonal em negrito.
***p < 0,001.
** p < 0,01.
* p < 0,05.

5.2. Avaliação do modelo estrutural

A segunda seção do PLS apresenta os resultados da análise estrutural modelo e a importância relativa de cada variável independente (Gefen & Straub, 2005; Gefen et al., 2011). O modelo estrutural foi testado usando as cargas, significância dos coeficientes do caminho e valores t. O modelo explicou 36,8% da variância total na eficácia do ISS. A Fig. 2 mostra os resultados da avaliação do modelo estrutural.

A primeira hipótese (H1) analisou a influência positiva da liderança relacional em três tipos de alinhamento social e foi apoiada (ÿ = 0,204, p < 0,05; ÿ = 0,483, p < 0,001; ÿ = 0,615, p < 0,001). O a segunda hipótese (H2) analisou a relação entre o social alinhamento e conhecimento integrado, e foi apoiado (ÿ = 0,139, p < 0,05; ÿ = 0,228, p < 0,01; ÿ = 0,462, p < 0,001), indicando que As ligações estabelecidas entre as OSCs e os executivos de negócios influenciaram positivamente o nível de conhecimento integrado. A terceira hipótese (H3) analisou a influência positiva do conhecimento integrado sobre Eficácia do ISS e foi apoiada (ÿ = 0,607, p < 0,001). O quarto hipótese (H4), analisou a influência positiva da eficácia do ISS sobre desempenho organizacional e foi apoiado (ÿ = 0,487, p < 0,001).

Além disso, as variáveis de controle não influenciaram a eficácia do ISS neste estudo. Ao contrário de estudos anteriores que constataram que a experiência profissional, a educação e o treinamento poderiam influenciar a eficácia do ISS em organizações (Choi, 2016), experiência de trabalho e nível de educação de Uma OSC não influenciou a eficácia do ISS. Uma explicação para esse resultado pode ser a natureza homogênea das OSCs na Coreia do Sul. contexto governamental.

5.3. O efeito moderador do conhecimento técnico

A quinta hipótese (H5) afirmava que o conhecimento técnico de a OSC moderaria positivamente a relação entre as organizações integradas conhecimento e eficácia do ISS. Essa influência foi significativa, mas em na direção oposta à hipótese. O nível de conhecimento técnico da OSC influenciou negativamente a relação entre o conhecimento integrado e a eficácia do ISS (ÿ = ÿ2,203, p < 0,001). mostrado na Tabela 7, analisamos o impacto das variáveis individuais sobre a variável endógena no modelo para determinar o tamanho do efeito. o tamanho do efeito da moderação é moderado (Cohen, 1988). Um resumo de os resultados dos testes de hipóteses são apresentados na Tabela 8.

6. Discussão e implicações

Os resultados do estudo mostram que a liderança relacional da A OSC afeta positivamente o alinhamento social, o que influencia a integração conhecimento desenvolvido entre o CSO e os executivos de negócios. Isso o conhecimento integrado resultou num maior nível de eficácia do ISS e maior desempenho organizacional. Esses resultados sugerem diversas implicações para a pesquisa e a prática. Começamos detalhando as implicações para a pesquisa e, em seguida, abordamos as implicações que podem ser úteis para os profissionais. Em primeiro lugar, este estudo é significativo porque considera a alinhamento entre TI e negócios sob um novo ponto de vista – o de alinhamento social. Para facilitar o alinhamento social entre as OSCs e executivos de negócios, as OSCs devem se esforçar para explorar oportunidades para construir relacionamentos fortes (ou seja, laços de rede) em uma organização. Nas organizações governamentais sul-coreanas, existem laços de rede informais, como laços com a alma mater (ou seja, laços escolares) e regionalismo. Os laços informais de rede (por exemplo, regionalismo) podem ter uma influência maior do que a autoridade formal em uma organização governamental. Embora

Tabela 6
Análise do efeito da moderação na variável dependente.

	Efeito direto (caminho)		Efeito indireto (caminho)		Efeito total R2	Tamanho do efeito (f2)
Modelo Básico	LED ÿ POR	0,579	LED ÿ STR ÿ INT ÿ ISS ÿ POR LED ÿ COG ÿ INT ÿ ISS ÿ POR LED ÿ REL ÿ INT ÿ ISS ÿ POR	0,132	0,711	0,238
	LED ÿ ISS	0,684	LED ÿ STR ÿ INT ÿ ISS LED ÿ COG ÿ INT ÿ ISS LED ÿ REL ÿ INT ÿ ISS	0,256	0,940	0,368
Modelo de Moderação (conhecimento técnico) LED ÿ PER		0,579	LED ÿ STR ÿ INT ÿ KNO ÿ ISS ÿ POR LED ÿ COG ÿ INT ÿ KNO ÿ ISS ÿ POR LED ÿ REL ÿ INT ÿ KNO ÿ ISS ÿ POR	ÿ0,454 0,124		0,238 (ÿ0)
	LED ÿ ISS	0,684	LED ÿ STR ÿ INT ÿ KNO ÿ ISS LED ÿ COG ÿ INT ÿ KNO ÿ ISS LED ÿ REL ÿ INT ÿ KNO ÿ ISS	ÿ0,931 ÿ0,247		0,476 (ÿ.108) 0,206

a. LED (liderança relacional), PER (desempenho), STR (ligação estrutural), COG (ligação cognitiva), REL (ligação relacional), INT (conhecimento integrado), ISS (eficácia do ISS), KNO (conhecimento técnico).

Machine Translated by Google

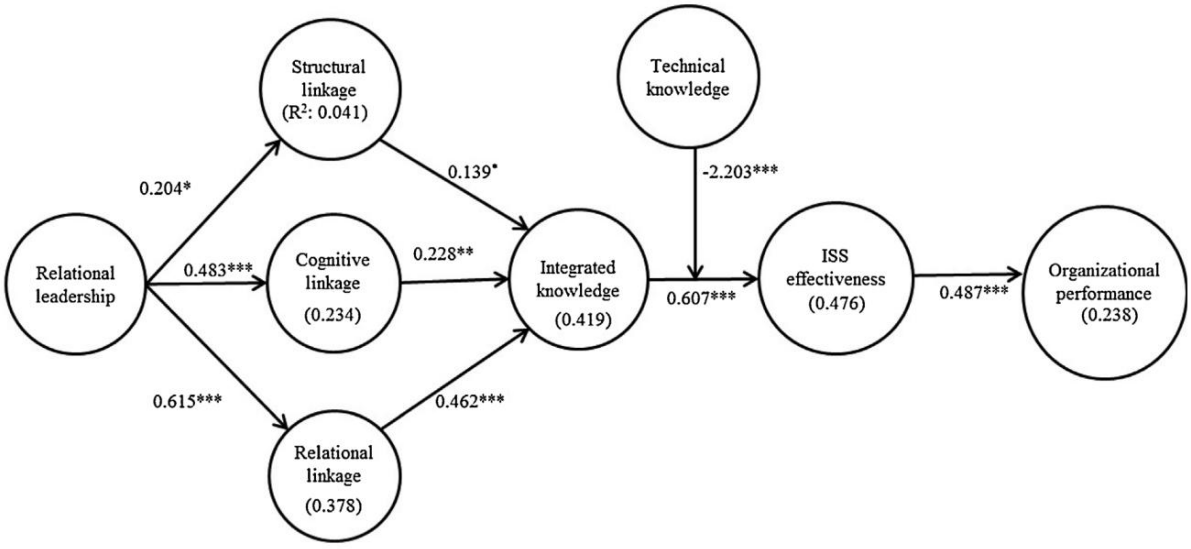


Fig. 2. Resultados do modelo de avaliação estrutural.

Tabela 7

Análise do viés do método comum.

Construir	Indicador	Substantivo Fator Carregando	Variância Explicado	Método Fator Carregando	Variância Explicado
Relacional liderança	REL_LED1	0,741***	0,5487	ý0,014	0,000
	REL_LED4	0,690***	0,476	0,015	0,000
	REL_LED5	0,744***	0,554	0,106	0,011
	REL_LED6	1,080***	1.167	ý0,202*	0,0406
	REL_LED7	0,771***	0,595	0,110	0,012
	REL_LED9	0,340	0,115	0,428*	0,183
Relação ligação	LIN_REL1	0,717***	0,514	0,120	0,014
	LIN_REL2	0,892***	0,795	-0,031	0,000
	LIN_REL3	0,908***	0,824	ý0,088	0,008
Estrutural ligação	LIN_STR1	0,945***	0,894	0,009	0,000
	LIN_STR2	0,896***	0,802	0,016	0,000
	LIN_STR3	0,967***	0,936	ý0,025	0,001
Cognição ligação	LIN_COG1	0,904***	0,817	0,002	0,000
	LIN_COG2	0,904***	0,817	ý0,002	0,000
Integrado conhecimento	INI1	1,036***	1.073	ý0,253**	0,063
	INT2	0,891***	0,794	0,037	0,001
	INT3	0,760***	0,578	0,186**	0,035
eficaz- ness	EFEITO2	0,844***	0,719	ý0,231*	0,053
	EFEITO3	0,708***	0,501	0,148	0,022
	EFEITO4	0,980***	0,959	ý0,135	0,018
	EFEITO5	0,853***	0,727	0,049	0,002
	EFEITO6	0,811***	0,657	0,108	0,012
Organizacional executar- mance	ORG_PRM1	0,832***	0,692	0,028	0,000
	ORG_PRM2	0,983***	0,965	-0,071	0,005
	ORG_PRM3	0,903***	0,816	0,064	0,004
	ORG_PRM4	0,974***	0,948	-0,021	0,000
	ORG_PRM5	0,225*	0,051	0,613***	0,376
	ORG_PRM7	0,364***	0,132	0,507***	0,257
Técnico conhecimento	TEC_KNO1	0,910***	0,829	0,047	0,002
	TEC_KNO2	0,7952***	0,631	0,161*	0,026
	TEC_KNO3	1,028***	1.057	ý0,235*	0,055
		Média	0,709	Média	0,038

* p < 0,05.
** p < 0,01.
*** p < 0,001.

os membros estão situados dentro de uma rede formal, seus relacionamentos podem facilitam pouca comunicação. Relacionamentos formais baseados em autoridade não nem sempre refletem a estrutura social informal dentro das organizações. Quando a estrutura social informal não coincide com a formal estrutura de autoridade, o desempenho organizacional muitas vezes sofre (Gulati & Puranam, 2009). Portanto, a liderança relacional de uma OSC pode beneficia o desempenho organizacional porque reforça as informações, os comportamentos e as orientações normativas para os membros da organização (Soda & Zaheer, 2012), resultando em um alinhamento mais eficaz entre negócios e TI. Isso sugere que relacionamentos, em vez de estruturas hierárquicas de autoridade, podem ser a chave para novas formas de liderança eficaz. (Drath, 2001) que deve ser explorado.

Em segundo lugar, os preditores diretos da eficácia do ISS neste estudo foram o nível de ligações cognitivas, estruturais e relacionais entre os CSO e executivos de negócios. Chan e Reich (2007) afirmaram que mais investigações focadas no alinhamento são necessárias para ir além do 'alinhamento afirmações 'é bom' e explorar sutilezas sobre como, quando, e onde o alinhamento realmente importa. Consistente com Wagner et al. (2014) proposições conceituais, este estudo constatou que o alinhamento social (consistindo em ligações estruturais, cognitivas e relacionais) permite Compartilhamento de conhecimento e desenvolvimento de conhecimento integrado. Pesquisas futuras devem incorporar aspectos do capital social em modelos de alinhamento entre negócios e TI, a fim de explorar de forma mais abrangente o alinhamento dentro das organizações.

Em terceiro lugar, este estudo é significativo por ter testado empiricamente as relações entre alinhamento social, eficácia do ISS e desempenho organizacional. Pesquisas anteriores na área de TI têm comumente viu os problemas de segurança da informação através das lentes da dissuasão teoria (por exemplo, D'arcy & Herath, 2011; Siponen & Vance, 2010). Isto a teoria propõe que as pessoas tomem decisões racionais para se comprometer ou abster-se de atividades ilícitas baseadas na maximização de benefícios e minimização de custos. Se sanções formais (ou seja, legais) para um ato ilícito forem percebidos como certos e severos, os indivíduos geralmente são dissuadidos de envolvendo-se nesse ato (Gibbs, 1975). Da mesma forma, grande parte do comportamento IS A pesquisa de segurança postula que quanto mais os funcionários percebem os riscos e custos das sanções formais, maior a probabilidade de cumprirem o EI políticas de segurança (D'arcy & Herath, 2011).

No entanto, o estudo atual mostra que a eficácia do ISS pode ser obtidos por meio de alinhamento social informal e integração de conhecimento. O papel do CSO inclui a gestão de pessoas e processos bem como a segurança da informação, uma vez que o CSO é responsável por desenvolver, supervisionar e coordenar todas as facetas dos esforços de segurança em toda a organização. Essa ampla gama de funções de trabalho geralmente leva tomadores de decisão a procurar indivíduos com mais competências relacionadas com a gestão origens. Olhando para a origem das OSCs, geralmente cerca de 26% atualmente possuem MBA e esse número está aumentando (CSO Online, 2009). Em muitas organizações, o CSO é um dos membros funcionais seniores

Machine Translated by Google

Tabela 8
Resumo da Hipótese.

Hipótese	Peso de regressão padrão	Nível Sig	Suportado
H1 CSO A liderança relacional influencia positivamente o alinhamento social.			
H1-a A liderança relacional da CSO influencia positivamente a ligação estrutural.	0,204	0,05	Sim
A liderança relacional do CSO H1-b influencia positivamente a vinculação cognitiva.	0,483	0,001	Sim
H1-c A liderança relacional do CSO influencia positivamente o vínculo relacional.	0,615	0,001	Sim
H2 O alinhamento social influencia positivamente o conhecimento integrado.			
H2-a A ligação estrutural influencia positivamente o conhecimento integrado.	0,139	0,05	Sim
H2-b A ligação cognitiva influencia positivamente o conhecimento integrado.	0,228	0,01	Sim
H2-c A ligação relacional influencia positivamente o conhecimento integrado.	0,462	0,001	Sim
H3 O conhecimento integrado influencia positivamente a eficácia do sistema de segurança da informação.	0,607	0,001	Sim
H4 A eficácia do sistema de segurança da informação influencia positivamente o desempenho organizacional.	0,487	0,001	Sim
H5 O conhecimento técnico modera positivamente o conhecimento integrado – eficácia do sistema de segurança da informação	-2,203	0,01	Não*

* Direção oposta à hipótese.

executivos com status semelhante ao de um CFO ou CIO, e a Forbes relatou que, por Em 2018, 75% das OSCs se reportarão diretamente ao CEO (Forbes, 2016a,b). Assim, esta pesquisa destaca o papel do CSO em termos de liderança relacional e a capacidade de gerir o alinhamento social entre negócios e TI. como um mecanismo para a eficácia do ISS.

Em quarto lugar, embora o nosso modelo de investigação tenha tido sucesso na previsão de muitos relacionamentos, uma das hipóteses não foi suportada (H5). Ao contrário conforme nossa expectativa, o nível de conhecimento técnico do CSO moderou negativamente a relação entre conhecimento integrado e Eficácia do ISS. Nos EUA, profissionais de SI com experiência significativa em tecnologia são promovidos a cargos executivos seniores. de OSC. Mas nas organizações governamentais coreanas, a maioria das organizações centrais e organizações governamentais locais nomeiam o CSO como um oficial de nível superior que é funcionário público. Após executivos com longa gestão carreira adquirir algum conhecimento técnico, é provável que sejam nomeados CSO. Além disso, as informações do governo coreano O departamento de segurança faz parte da divisão de gestão geral em responsável pela gestão de recursos humanos e orçamento, e o alto funcionário da divisão de gestão geral é frequentemente nomeado para o cargo de CSO. Portanto, um CSO em uma organização governamental coreana pode não ser um profissional técnico com experiência significativa no departamento de segurança da informação, mas um gerente geral.

Os entrevistados neste estudo refletem esta característica em relação a 58% das OSCs tinham mais de 30 anos de experiência em atividades governamentais organizações, e 86,3% delas atuavam em TI e CSOs há menos de três anos. Além disso, 71,6% dos entrevistados não possuíam nenhum conhecimento de TI certificações. Especulamos que a hipótese rejeitada pode refletir a distinção cultural das organizações governamentais coreanas nesse sentido o nível geral relativamente baixo de experiência em TI das OSCs em nosso estudo afetou a moderação da relação entre os integrados conhecimento e eficácia do ISS. Especificamente, quanto mais técnico conhecimento que a OSC possuía, mais fraca era a relação entre conhecimento integrado e eficácia do ISS. Assim, em vez de aumentar a influência do entendimento compartilhado na eficácia do ISS, as OSCs com mais conhecimento técnico talvez não fossem capazes de efetivamente comunicar os vários aspectos da proposta de valor da segurança iniciativas para outros executivos, desestabilizando assim a influência do conhecimento integrado na eficácia do ISS. Pesquisas futuras devem testar a validade da moderação dentro de uma organização governamental coreana contexto, bem como outros contextos, como organizações privadas dentro Coreia do Sul e organizações públicas/privadas fora da Coreia do Sul.

Do ponto de vista do praticante, a primeira implicação diz respeito à CSOs mais técnicos. Os CSOs com uma carreira mais técnica solo em organizações governamentais coreanas podem experimentar alguns dificuldades em desenvolver alinhamento social entre negócios e TI porque podem ter redes sociais mais fracas dentro de sua organização. A implementação do CISO (Chief Information Security Officer) portaria do Ministério da Ciência e Informação da Coreia A Tecnologia da Comunicação em 2014 forçou as organizações a designar OSCs. Esta portaria de execução contribuiu para um aumento da número de OSCs, mas há grande variação nas tarefas e atividades de um CSO em cada organização. Embora os CSOs devam se destacar em habilidades de liderança e pensamento estratégico, eles ainda são profissionais e supervisores técnicos em organizações governamentais. Em caso de incidente de segurança uma resposta imediata e sistemática por parte de uma OSC pode ser difícil porque a ISS requer competências de gestão geral e técnicas conhecimento. A falta de uma rede informal pode impedir o desenvolvimento de competências mais técnicas participantes demonstrando liderança relacional visando promover o alinhamento social e acumular conhecimento integrado. por outro lado, a falta de conhecimento técnico pode impedir menos conhecimento técnico os participantes compreendam a extensão do incidente de segurança e pode comprometer a eficácia da ISS. Se a ISS for um ativo importante, a Coreia as organizações governamentais precisam ter uma compreensão adequada da toda a extensão do papel estratégico do CSO dentro da organização. Por mais articulando e padronizando claramente as qualificações exigidas para uma OSC e organizações governamentais coreanas podem aumentar significativamente o ISS eficácia.

Relativamente a esta questão, na altura da nomeação do CSO, a decisão os fabricantes precisam considerar a experiência técnica do indivíduo dentro do departamento de TIC, bem como a formação educacional e profissional do indivíduo. Os tomadores de decisão seriam aconselhados a examinar a conhecimento, experiência e antecedentes relevantes do indivíduo em relação as qualificações necessárias de uma OSC e, então, contratar apenas pessoal totalmente qualificado. O governo também deve considerar a contratação de "outsiders" para uma posição de OSC dentro de organizações governamentais coreanas. O público O sistema de pessoal de oficiais é um sistema de pessoal fechado e, portanto, não é fácil recrutar uma OSC. Portanto, pode ser necessário recrutar fora especialistas com qualificações adequadas do setor privado para Cargos de OSC e, em seguida, socializá-los na cultura organizacional do governo após a contratação. Mesmo após a nomeação, seja um insider ou um estranho, o CSO deve envolver-se continuamente em projetos de curto e longo prazo cursos de formação de longa duração sobre as mais recentes tecnologias técnicas e de gestão conhecimento necessário para permanecer eficaz como uma OSC.

7. Limitações e pesquisas futuras

Além das implicações, este estudo apresenta algumas limitações. Primeiro, o efeito moderador do conhecimento técnico do CSO hipotetizado em Este estudo foi contra as expectativas. Propusemos uma moderação positiva devido ao papel único das OSCs como uma posição executiva e posição de supervisor/técnico. Devido à natureza da nossa exemplo, parece que o conhecimento técnico das OSCs pode ser uma obstáculo ao alinhamento entre negócios e TI. Portanto, pesquisas futuras devem segmentar ainda mais a amostra com base na trajetória profissional do CSOs e explore o impacto do alinhamento entre negócios e TI.

Em segundo lugar, ao analisar a relação entre liderança relacional e alinhamento social (H1), é importante notar que a liderança de uma OSC O estilo de liderança também pode ser afetado por suas habilidades, comportamentos e

Machine Translated by Google

traços de liderança, visto que a liderança eficaz é uma combinação de traços, habilidades e comportamentos (Strang, 2007). O estudo atual concentrou-se na liderança relacional, mas estudos futuros podem considerar outros traços, comportamentos e habilidades de liderança, como eficácia pessoal, influência no alinhamento social e capacidade cognitiva de integrar conhecimento (Katz & Kahn, 1978; Schermerhorn, Hunt & Osborn, 2003; Strang, 2007).

Terceiro, pesquisas anteriores descobriram que as ligações estruturais (interações formais e informais) entre CIOs e equipes de alta gerência não influenciaram a integração do conhecimento no setor privado (Karahanna & Preston, 2013; Smaltz, Sambamurthy & Agarwal, 2006).

O presente estudo representou a vinculação estrutural apenas como uma interação informal entre OSCs e executivos de empresas, utilizando apenas o contexto do setor público na Coreia do Sul. Pesquisas futuras podem explorar as relações que emergem das vinculações formais e informais e da integração de conhecimento nos setores público e privado.

Em quarto lugar, com relação à relação entre o conhecimento integrado e a eficácia do ISS (H3), este estudo investigou a integração do conhecimento apenas no nível executivo. Pesquisas constataram que, para desenvolver um alto nível de eficácia do ISS, a conformidade dos funcionários é necessária (Siponen & Vance, 2010). Pesquisas futuras poderiam examinar a relação entre a integração do conhecimento e a conformidade entre agentes de segurança e funcionários nos diferentes níveis hierárquicos da organização, bem como expandir o modelo para OSCs corporativas na República da Coreia e em outros lugares.

Em quinto lugar, como visto na Tabela 5, existem algumas variáveis altamente correlacionadas (por exemplo, liderança relacional e conhecimento integrado). As OSCs em organizações governamentais coreanas tendem a avaliar muito bem seu nível de habilidade e conhecimento de liderança, bem como o nível de desempenho de sua organização. Este resultado é consistente com, e pode ser interpretado por meio de pesquisas anteriores que constataram que o conceito de "salvar a face" influencia o comportamento em organizações sediadas na Ásia (Kim & Nam, 1998; Park, Dai Hwang & Harrison, 1996). Embora as correlações sejam elevadas, todos os construtos correlacionaram-se mais fortemente com suas próprias medidas do que com qualquer um dos outros construtos, indicando validade discriminante suficiente. Pesquisas futuras devem testar esses resultados em outros contextos para confirmar ou refutar os achados.

Por fim, este estudo indica um efeito significativo do alinhamento social na eficácia do ISS e no desempenho organizacional. O conhecimento integrado pode atuar como um antecedente para o desempenho organizacional e a eficácia do ISS, e pesquisas futuras podem explorar como o alinhamento social entre OSCs e executivos de negócios pode ser desenvolvido.

Afirmamos que estudos futuros sobre esta questão seriam mais bem atendidos por meio de observação longitudinal. Pesquisas futuras poderiam comparar o desenvolvimento e/ou o efeito do alinhamento estratégico e social ao longo do tempo para obter um quadro mais completo do fenômeno.

8. Conclusão

Este estudo explorou, a partir de uma perspectiva de capital social, como o nível de liderança relacional do CSO impulsiona o alinhamento social entre o CSO e o executivo de negócios, o que por sua vez influencia o conhecimento integrado, a eficácia do ISS e o desempenho organizacional.

Curiosamente, e em contraste com o previsto, o nível de conhecimento técnico do CSO atenuou a relação entre o conhecimento integrado e a eficácia do ISS, talvez indicando um efeito de substituição. Por fim, os resultados mostraram que o nível de eficácia do ISS influenciou positivamente o desempenho organizacional, incluindo o desempenho focado em processos financeiros e de negócios.

Apêndice A

Construir	Fonte	Definição	Itema
Relacional Liderança	Carmeli e Gittel (2009), Gittell (2003)	A liderança relacional inclui três focos: objetivos compartilhados, conhecimento compartilhado e respeito mútuo.	Nesta organização, compartilhamos uma visão comum. Nesta organização, agimos em direção a objetivos comuns.* Os funcionários desta organização agem sem ter uma direção clara. * Os funcionários desta organização sabem com quais tarefas seus colegas de trabalho lidam. Nesta organização, compartilhamos uns com os outros os assuntos em que trabalhamos. Compartilhar uns com os outros no contexto do trabalho nos permite entender melhor as necessidades uns dos outros. Compartilhar uns com os outros sobre nossos problemas de trabalho nos permite entender melhor como nossas ações impactam outros colegas de trabalho. Há muito respeito entre nós no trabalho. * Quando alguém expressa sua opinião diferente, nós a respeitamos. O respeito mútuo é a base dos nossos relacionamentos nesta organização. *
Estrutural Linkageb	Karahanna e Preston (2013), Smaltz et al. (2006)	A ligação estrutural foi medida como a frequência máxima de interação informal entre os membros da equipe de gestão (TMT). CSO e executivos de negócios.	Eu socializo com os membros do TMT (por exemplo, encontros sociais, golfe, tênis, etc.). Tenho trocas informais com membros do TMT.

Machine Translated by Google

Cognitivo Linkageb	Karahanna e Preston (2013)	A ligação cognitiva mede o grau de que o CSO e os executivos de negócios compartilham linguagem e terminologia comuns em suas comunicação.	Os membros do CSO e do TMT compartilham uma linguagem comum em nossas conversas. uma O CSO usa principalmente terminologia empresarial ao interagir com os membros do TMT. O CSO evita usar jargões de segurança da informação ao interagir com membros do TMT. *
Relacional Linkageb	Karahanna e Preston (2013)	A ligação relacional mede o grau em que o CSO e os executivos de negócios têm desenvolveu uma relação de respeito e confiança.	Os membros do TMT e a CSO agem no melhor interesse da organização. Os membros do TMT e da CSO confiam e respeitam uns aos outros. Os membros do TMT e o CSO são competentes no que fazem.
Integrado Conhecimento	Boynton, Zmud e Jacobs (1994), Karahanna e Preston (2013)	O conhecimento integrado mede o grau em que o CSO e os executivos de negócios têm uma entendimento compartilhado sobre o papel do ISS dentro da organização.	Os membros do CSO e do TMT têm um entendimento compartilhado do papel da segurança da informação em nossa organização. Os membros do CSO e do TMT têm uma visão compartilhada visão do papel da segurança da informação como uma arma competitiva para nossa organização. Os membros do CSO e do TMT têm um entendimento compartilhado de como a segurança da informação pode ser usada para aumentar a produtividade das operações da nossa organização.
—— Eficaz- ss	Hwang e Choi (2017), Kankanhalli e outros (2003), Knapp, Marshall, Rainer e Ford (2007), Straub (1990)	O ISS mede o grau em que a organização estabelece controles que previnem danos de ameaças externas e internas.	Nossa política de segurança da informação descreve os itens básicos em detalhes. * Nossa organização oferece educação e treinamento em segurança da informação para oficiais. Nossa organização estabelece sistemas de resposta eficazes para acidentes de segurança da informação. Os controles de segurança da nossa organização protegem ativos de informação, como hardware e software. Os controles de segurança da nossa organização protegem os dados da organização. Os controles de segurança da nossa organização protegem os serviços de informação da organização.
Organizacional Desempenho- ce	Kim, Shin e Kwon (2012), Powell e Dent-Micallef (1997), Tippins e Sohi (2003)	O desempenho organizacional mede a produtividade financeira da organização e a execução dos processos de negócios dentro da organização.	Nossa organização atingiu uma produtividade maior que a meta nos últimos 3 anos. Nossa organização foi mais lucrativa do que a meta nos últimos 3 anos. Nossa organização alcançou um ROI maior que a meta nos últimos 3 anos. Nossa organização alcançou um desempenho financeiro superior à meta nos últimos 3 anos. Nossa organização é melhor do que outras organizações governamentais na conexão (por exemplo, comunicação e compartilhamento de informações) entre partes. Nossa organização é melhor do que outras organizações governamentais na redução de custos e mão de obra humana. * Nossa organização é melhor do que outras organizações governamentais na aplicação de métodos analíticos complexos às tarefas de processamento. Nossa organização é melhor do que outras organizações governamentais em trazer informações detalhadas para tarefas de processamento. *

Machine Translated by Google

OSCs	Byrd e Turner (2000), Lee, Trauth e Farwell (1995)	O conhecimento técnico mede o conhecimento do CSO em termos de planejamento, organização e liderança de projetos relacionados a TI.	O CSO é muito capaz em termos de planejamento, organização e liderança de projetos. O CSO é muito capaz em termos de planejamento e execução de trabalho em um ambiente coletivo. O CSO é muito capaz em termos de ensinar os outros.
Técnico			
Conhecimento			

* Item descartado.

[um] Os itens foram medidos em uma escala Likert de cinco pontos, onde 1 denotava “discordo totalmente” e 5 denotava “concordo totalmente”.

[b] Os itens que medem as ligações estruturais, relacionais e cognitivas foram medidos em uma escala Likert de cinco pontos, onde 1 denotava “todos os dias” e 5 denotava “nunca”.

Referências

Adler, PS, & Kwon, S.-W. (2002). Capital social: Perspectivas para um novo conceito. Academia de Revista de Administração, 27, 17–40.

BBC (2014). Sistema de identidade sul-coreano será reconstruído do zero. (14 de outubro de 2014) Recuperado de http://www.bbc.com/news/technology-29617196 (Acessado em 01 de junho de 2017).

Bagozzi, RP, & Yi, Y. (1988). Sobre a avaliação de modelos de equações estruturais. Revista de Academia de Ciências de Marketing, 16(1), 74–94.

Baldwin, MW (1997). Esquemas relacionais como fonte de procedimentos de autoinferência se-então . Revista de Psicologia Geral, 1(4), 326–335.

Bergeron, F., Raymond, L., & Rivard, S. (2004). Padrões ideais de alinhamento estratégico e desempenho empresarial. Informação e Gestão, 41(8), 1003–1020.

Boisot, M. (1995). Espaço de informação: uma estrutura para a aprendizagem em organizações e instituições e cultura. Londres: Routledge.

Boynton, AC, Zmud, RW, & Jacobs, JC (1994). A influência das práticas de gestão de TI no uso de TI em grandes organizações. MIS Quarterly, 18(3), 299–318.

Brower, HH, Schoorman, FD, & Tan, HH (2000). Um modelo de liderança relacional: a integração da confiança e da troca líder-membro. The Leadership Quarterly, 11(2), 227–250.

Burt, RS (1997). O valor contingente do capital social. Administrative Science Quarterly, 41(3), 339–365.

Byrd, TA, & Turner, DE (2000). Medindo a flexibilidade da infraestrutura de tecnologia da informação: Análise exploratória de um construto. Journal of Management Information Systems, 17(1), 167–208.

CNN Tech (2017). Pesquisadores descobrem possível ligação da Coreia do Norte com ciberataque em massa. (16 de maio de 2017), recuperado de http://money.cnn.com/2017/05/15/technology/wannacry-hack-responsible-hackers/index.html (Acessado em 02 de julho de 2017).

CSO Online (2009). O que é um diretor de segurança? (19 de abril de 2009) Recuperado em 01/12/2017 de http://www.CSOonline.com/article/221739/What_is_a_Chief_Security_ Officer.

Carmeli, A., & Gittel, JH (2009). Relacionamentos de alta qualidade, segurança psicológica e aprendizado com falhas em organizações de trabalho. Journal of Organizational Behavior, 30(6), 709–729.

Chan, YE, & Reich, BH (2007). Alinhamento de TI: O que aprendemos? Journal of Information Technology, 22(4), 297–315.

Chan, YE, Huff, SL, Barclay, DW, & Copeland, DG (1997). Orientação estratégica de negócios, orientação estratégica de sistemas de informação e alinhamento estratégico. Pesquisa em Sistemas de Informação, 8(2), 125–147.

Chan, YE (2002). Por que não dominamos o alinhamento? A importância da estrutura organizacional informal. MIS Quarterly Executive, 1(2), 97–112.

Chen, R., Sun, C., Helms, MM, & Jih, W. (2008). Alinhando tecnologia da informação e estratégia de negócios com uma perspectiva de capacidades dinâmicas: um estudo longitudinal de uma empresa taiwanesa de semicondutores. International Journal of Information Management, 28(5), 366–378.

Chen, Y., Ramamurthy, K., & Wen, KW (2012). Conformidade com as políticas de segurança da informação das organizações: abordagem de punição ou recompensa? Journal of Management Information Systems, 29(3), 157–188.

Chin, WW, Thatcher, JB, & Wright, RT (2012). Avaliando o viés do método comum: problemas com a técnica ULMC. MIS Quarterly, 36(3), 1003–1019.

Chin, WW (1998). A abordagem dos mínimos quadrados parciais para modelagem de equações estruturais. Em GA Marcoulides (Ed.). Métodos modernos para pesquisa empresarial (pp. 295–336). Mahwah, NJ: Lawrence Erlbaum & Associates.

Choi, M. (2016). Liderança do gestor de segurança da informação sobre a eficácia da segurança dos sistemas de informação para computação segura e sustentável. Sustentabilidade, 8(7), 638.

Chong, AYL, Ooi, KB, Chan, FT, & Darmawan, N. (2011). O alinhamento dos funcionários afeta o alinhamento entre negócios e TI? Uma análise empírica. Journal of Computer Information Systems, 51(3), 10–20.

Clark, KB, & Fujimoto, T. (1991). Desempenho no desenvolvimento de produtos. Boston, MA Harvard: Imprensa da Escola de Negócios.

Cohen, J. (1988). Análise de poder estatístico. Hillsdale, NJ: Erlbaum & Associates.

D'arcy, J., & Herath, T. (2011). Uma revisão e análise da teoria da dissuasão na literatura sobre segurança de SI: Compreendendo as descobertas díspares. Revista Europeia de Sistemas de Informação, 20(6), 643–658.

Drath, W. (2001). O mar azul profundo: Repensando a origem da liderança. São Francisco, CA: Jossey-Bass.

Forbes (2016a). Os custos do crime cibernético devem chegar a US$ 2 trilhões até 2019. (17 de janeiro de 2016) Obtido em https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#535bc38d3a91 (Acessado em 02 de junho de 2017).

Forbes (2016b). Os maiores salários em segurança cibernética nas áreas metropolitanas dos EUA chegam a US$ 380.000. (9 de janeiro de 2016) Obtido em https://www.forbes.com/sites/stevemorgan/2016/01/09/top-cyber- security-salaries-in-us-metros-hit-380000/#59e3f1a47ef8.

Fornell, C., & Larcker, DF (1981). Avaliação de modelos de equações estruturais com un- variáveis observáveis e erro de mensuração. Journal of Marketing Research, 18(1), 39–50.

Gefen, D., & Straub, D. (2005). Um guia prático para validade fatorial usando pls-graph: tutorial e exemplo anotado. Comunicações da Associação para Sistemas de Informação, 16, 91–109.

Gefen, D., Rigdon, EE, & Straub, D. (2011). Comentários do editor: Uma atualização e extensão das diretrizes SEM para pesquisa em ciências administrativas e sociais. MIS Quarterly, 35(2), iii–xiv.

Gibbs, JP (1975). Crime, punição e dissuasão. Southwestern Social Science Quarterly, 48, 515–530.

Gittell, JH, & Douglass, A. (2012). Burocracia relacional: estruturando relacionamentos recíprocos em papéis. Academy of Management Review, 37(4), 709–733.

Gittell, JH (2003). Uma teoria da coordenação relacional. Em K. Cameron, J. Dutton, & R. Quinn (Eds.). Bolsa organizacional positiva: Fundamentos de uma nova disciplina (pp. 279–295). São Francisco, CA: Berrett-Koehler Publishers.

Goles, T., White, GB, & Dietrich, G. (2005). Tela escura: Um exercício em segurança cibernética. MIS Quarterly Executive, 4(2), 303–318.

Goodhue, DL, & Straub, DW (1991). Preocupações de segurança dos usuários do sistema: Um estudo das percepções sobre a adequação da segurança. Informação e Gestão, 20(1), 13–27.

Grant, RM (1996). Prosperando em ambientes dinamicamente competitivos: Capacidade organizacional como integração de conhecimento. Ciência Organizacional, 7(4), 375–387.

Gulati, R., & Puranam, P. (2009). Renovação por meio da reorganização: o valor das inconsistências entre a organização formal e informal. Ciência Organizacional, 20(2), 422–440.

Gupta, M. (2011). Três ensaios sobre gestão da segurança da tecnologia da informação em organizações zações. Universidade Estadual de Nova York em Buffalo.

Hankook Newpaper (17 de setembro de 2015), recuperado de http://www.hankookilbo.com/v_print.aspx?id=c9870a301fa044df9008bdd64f2ff5dd (Acessado em 28 de julho de 2017).

Herath, T., & Rao, HR (2009). Motivação e dissuasão para proteção: Uma estrutura para a conformidade com as políticas de segurança em organizações. European Journal of Information Systems, 18(2), 106–125.

Hiller, NJ, Day, DV, & Vance, RJ (2006). Encenação coletiva de papéis de liderança e eficácia da equipe: um estudo de campo. The Leadership Quarterly, 17(4), 387–397.

Hwang, K., & Choi, M. (2017). Efeitos da cultura de apoio à inovação e do comportamento de cidadania organizacional na segurança de sistemas de informação de governo eletrônico decorrentes do isomorfismo mimético. Government Information Quarterly, 34(2), 183–198. http://dx.doi.org/10.1016/j.giq.2017.02.001 .

ITRC (2015). Relatório de violação de dados. Recuperado de http://www.idtheftcenter.org/images/violação/DataBreachReports_2015.pdf (Acessado em 20 de junho de 2017).

Jones, GR, & George, JM (1998). A experiência e a evolução da confiança: implicações para a cooperação e o trabalho em equipe. Academy of Management Review, 23(3), 531–546.

Kankanhalli, A., Teo, H.-H., Tan, BCY, & Wei, K.-K. (2003). Um estudo integrativo da eficácia da segurança de sistemas de informação. International Journal of Information Management, 23(2), 139–154.

Karahanna, E., & Preston, DS (2013). O efeito do capital social no relacionamento entre o CIO e a alta gerência no desempenho da empresa. Journal of Management Information Systems, 30(1), 15–55.

Katz, D., & Kahn, RL (1978). A psicologia social das organizações. Nova Iorque: Wiley.

Kayworth, T., & Whitten, D. (2010). A segurança da informação eficaz requer um equilíbrio entre fatores sociais e tecnológicos. MIS Quarterly Executive, 9(3), 2012–2052.

Kearns, GS, & Sabherwal, R. (2006). Alinhamento estratégico entre negócios e tecnologia da informação: uma visão baseada em conhecimento de comportamentos, resultados e consequências. Journal of Management Information Systems, 23(3), 129–162 2006-7.

Kim, JY, & Nam, SH (1998). O conceito e a dinâmica da face: implicações para o comportamento organizacional na Ásia. Ciência Organizacional, 9(4), 522–534.

Kim, G., Shin, B., & Kwon, O. (2012). Investigando o valor do sociomaterialismo em conceituando a capacidade de TI de uma empresa. Journal of Management Information Systems, 29(3), 327–362.

Machine Translated by Google

Kim, J. (2012). Agenda e políticas nacionais de segurança da informação. Revista Digital Convergência, 10(1), 105–111.
Knapp, KJ, Marshall, TE, Rainer, RK, Jr., & Morrow, DW (2006). Os principais problemas de segurança da informação enfrentados pelas organizações: o que o governo pode fazer para ajudar. Segurança da Informação e Gestão de Riscos, 15(4), 51–58.
Knapp, KJ, Marshall, TE, Rainer, RK, Jr., & Ford, FN (2007). Eficácia da segurança da informação: Conceitualização e validação de uma teoria. Revista Internacional de Segurança da Informação e Privacidade, 1(2), 37–60.

Kogut, B., & Zander, U. (1996). O que as empresas fazem? Coordenação, identidade e aprendizagem. Ciência Organizacional, 7(5), 502–518.
Kraemer, S., Carayon, P., & Clem, J. (2009). Fatores humanos e organizacionais na segurança da informação e dos computadores: Caminhos para vulnerabilidades. Computador e Segurança, 28(7), 509–520.

Lee, DMS, Trauth, E., & Farwell, D. (1995). Habilidades críticas e requisitos de conhecimento de profissionais de SI: uma investigação conjunta acadêmica e industrial. MIS Quarterly, 19(3), 313–340.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilação de sistemas empresariais: o efeito das pressões institucionais e o papel mediador da alta administração. MIS Quarterly, 31(1), 59–87.

Lind, MR, & Zmud, RW (1991). A influência de uma convergência na compreensão entre provedores e usuários de tecnologia sobre inovação em tecnologia da informação. Ciência da Organização, 2(2), 195–217.
Meyer, JW, & Rowan, B. (1977). Organizações institucionalizadas: estrutura formal como mito e cerimônia. American Journal of Sociology, 83(2), 340–363.
Moffat, PM, & Nzulwa, J. (2016). Efeito das práticas de gestão estratégica de segurança no desempenho da empresa: um caso da autoridade tributária do Quênia. The Strategic Journal of Business & Change Management, 3(4).
Nahapiet, J., & Ghoshal, S. (1998). Capital social, capital intelectual e a vantagem organizacional. Academy of Management Review, 23(2), 242–266.
Nance, WD, & Straub, DW (1988). Uma investigação sobre o uso e a utilidade de software de segurança na detecção de abusos em computadores. Anais da nona conferência internacional sobre sistemas de informação (pp. 283–294).
Oh, H., Labianca, G., & Chung, MH (2006). Um modelo multinível de capital social de grupo. Academia de Revisão de Gestão, 31(3), 569–582.
Okhuysen, GA, & Eisenhardt, KM (2002). Integrando conhecimento em grupos: como intervenções formais simples permitem flexibilidade. Ciência da Organização, 13(4), 370–386.
Park, H., Dai Hwang, S., & Harrison, JK (1996). Fontes e consequências da com- Problemas de comunicação em subsidiárias estrangeiras: o caso das empresas dos Estados Unidos na Coreia do Sul. International Business Review, 5(1), 79–98.
Podsakoff, PM, MacKenzie, SB, Lee, JY, & Podsakoff, NP (2003). Vieses comuns de método em pesquisa comportamental: uma revisão crítica da literatura e soluções recomendadas. Journal of Applied Psychology, 88(5), 879–903.
Powell, TC, & Dent-Micallef, A. (1997). Tecnologia da informação como ad-competitivo Vantagem: O papel dos recursos humanos e tecnológicos nos negócios. Revista de Gestão Estratégica, 18(5), 375–405.
PricewaterhouseCoopers (2015). Pesquisa de violações de segurança da informação de 2015, governo de Sua Majestade. Recuperado de: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf (Acessado em 01 de agosto de 2017).
Reich, BH, & Benbasat, I. (1996). Uma investigação empírica de sistemas estratégicos orientados ao cliente . Pesquisa em Sistemas de Informação, 1(3), 325–347.
Reich, BH, & Benbasat, I. (2000). Fatores que influenciam a dimensão social da alinhamento entre objetivos de negócios e de tecnologia da informação. MIS Quarterly, 24(1), 81–113.

Ringle, CM, Wende, S., & Will, A. (2005). SmartPLS 2.0 (Beta). Hamburgo, Alemanha: Universidade de Hamburgo. http://www.Smartpls.De.
Sabherwal, R., & Chan, YE (2001). Alinhamento entre estratégias de negócios e de SI: uma abordagem configuracional. Pesquisa em Sistemas de Informação, 12(1), 11–33.
Sarkar, KR (2010). Avaliação de ameaças internas à segurança da informação usando medidas técnicas: comportamentais e organizacionais. Relatório Técnico de Segurança da Informação, 15(3), 112–133.

Schermerhorn, JR, Hunt, JG, & Osborn, RN (2003). Comportamento organizacional (8ª ed.). Nova York, NY: Wiley.
Sen, S., & Samanta, S. (2014). Segurança da informação. Revista Internacional de Pesquisa Inovadora em Tecnologia, 1(11), 224–231.
Siponen, M., & Vance, A. (2010). Neutralização: novos insights sobre o problema da em- violações da política de segurança dos sistemas de informação dos funcionários. MIS Quarterly, 34(3), 487–502.
Smaltz, DH, Sambamurthy, V., & Agarwal, R. (2006). Os antecedentes da eficácia do papel do CIO nas organizações: um estudo empírico no setor da saúde. IEEE Transactions on Engineering Management, 53(2), 207–222.
Soda, G., & Zaheer, A. (2012). Uma perspectiva de rede na arquitetura organizacional: efeitos de desempenho da interação entre organizações formais e informais. Strategic Management Journal, 33(6), 751–771.

Filho, JY (2011). Por medo ou desejo? Rumo a uma melhor compreensão da situação dos funcionários. motivação para seguir as políticas de segurança de SI. Informação e Gestão, 48(7), 296–302.
Soomro, ZA, Shah, MH, & Ahmed, J. (2016). A segurança da informação precisa de uma abordagem mais holística: uma revisão da literatura. Revista Internacional de Gestão da Informação, 36(2), 215–225.
Strang, KD (2007). Examinando características e comportamentos eficazes de liderança em projetos de tecnologia viores. Computadores no Comportamento Humano, 23, 424–462.
Straub, DW, & Welke, RJ (1998). Lidando com o risco sistêmico: Modelos de planejamento de segurança para tomada de decisões gerenciais. MIS Quarterly, 22(4), 441–469.
Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Diretrizes de validação para pesquisa positivista em SI. Comunicações da Associação para Sistemas de Informação, 13, 380–427 (Artigo 24).

Straub, DW (1990). Segurança eficaz de SI: um estudo empírico. Sistemas de Informação Pesquisa, 1(3), 255–276.
Thatcher, JB, & Perrewe, PL (2002). Um exame empírico de características individuais como antecedentes da ansiedade e da autoeficácia em relação ao computador. MIS Quarterly, 26(4), 381–396.

Tippins, MJ, & Sohi, RS (2003). Competência em TI e desempenho empresarial: a aprendizagem organizacional é um elo perdido? Strategic Management Journal, 24(8), 745–761.
Tsai, C.-Y., Dionne, SD, Wang, A.-C., & Spain, SM (2017). Efeitos da congruência de esquemas relacionais na troca líder-membro. The Leadership Quarterly, 28(2), 268–284.
Uhl-Bien, M., Graen, G., & Scandura, T. (2000). Implicações da troca líder-membro (LMX) para sistemas estratégicos de gestão de recursos humanos: relacionamentos como capital social para vantagem competitiva. Em GR Ferris (Ed.). Pesquisa em gestão de pessoas e recursos humanos (pp. 103–133). Greenwich, CT: Information Age Publishing.

Uhl-Bien, M. (2006). Teoria da liderança relacional: explorando os processos sociais de liderança e organização. The Leadership Quarterly, 17(6), 654–676.
Vance, A., Lowry, PB, & Eggett, D. (2013). Usando a responsabilização para reduzir violações de políticas de acesso em sistemas de informação. Journal of Management Information Systems, 29(4), 263–290.

Wagner, H.-T., Beimborn, D., & Weitzel, T. (2014). Como o capital social entre unidades de tecnologia da informação e de negócios impulsiona o alinhamento operacional e o valor comercial de TI. Revista de Sistemas de Informação Gerencial, 31(1), 241–271.
Warkentin, M., & Willison, R. (2009). Questões comportamentais e políticas em segurança de sistemas de informação: A ameaça interna. European Journal of Information Systems, 18(2), 101–105.
Whitten, D. (2008). O diretor de segurança da informação: Análise das habilidades necessárias para o sucesso. Journal of Computer Information Systems, 48(3), 15–19.
Jornal Yonhap (16 de setembro de 2015), recuperado de http://www.yonhapnews.co.kr/bulletin/2015/09/16/0200000000AKR20150916221100003.HTML (Acessado em 02 de janeiro de 2017).

Yun Ji Moon é doutora em Sistemas de Informação Gerencial pela Ewha Womans University. Seus interesses de pesquisa incluem adoção de tecnologia da informação, negócios móveis, impacto organizacional da tecnologia da informação, gestão do conhecimento e modelo de qualidade de serviços eletrônicos. Seus artigos foram publicados em Information & Management, Canadian Journal of Administrative Sciences, Journal of Computer Information Systems e International Journal of Hospitality Management. Atualmente, ela trabalha como professora assistente no departamento de Sistemas de Informação Gerencial da Universidade Católica de Pusan, Coreia do Sul. Ela pode ser contatada pelo e-mail yjmoon@cup.ac.kr.

O Dr. Myeonggil Choi obteve seu doutorado no KAIST (Instituto Coreano Avançado de Ciência e Tecnologia) e trabalhou como pesquisador sênior no Instituto de Pesquisa em Eletrônica e Telecomunicações (ETRI) e na Agência de Defesa (ADD). Atualmente, é professor associado no Departamento de Administração de Empresas da Universidade Chung-Ang, em Seul. Ele realizou pesquisas sobre segurança no governo. Seus interesses de pesquisa incluem sistemas de segurança da informação para governo eletrônico, avaliação da segurança da informação e comportamento organizacional em relação à segurança da informação.

Deborah J. Armstrong é professora associada de Sistemas de Informação Gerencial na Faculdade de Administração da Universidade Estadual da Flórida. Os interesses de pesquisa da Dra. Armstrong abrangem uma variedade de questões na interseção entre pessoal de SI e cognição, envolvendo os aspectos humanos da tecnologia, mudança e aprendizagem. Suas pesquisas foram publicadas no Management Information Systems Quarterly, no Journal of Management Information Systems e no European Journal of Information Systems and Communications da ACM, entre outros.