فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال بیستم: شماره ۷۳- بهار ۱٤۰۰
صص: ۳۱ - ۵۵

Amniat Pajouhi: Security Research Quarterly
Vol.20, No.73, Spring 2021
P-P: 31 - 55

تاریخ دریافت: ۱۳۹۹/۹/۲۳ تاریخ پذیرش: ۱۳۹۹/۱۲/۱۰

نقش باورهای انسانی در جذب دانش برای امنیت سایبری

ناصر رحمدل[۱]
مهدی کامکار[۲]

چکیده:

در این پژوهش به بررسی رابطه «باورهای انسانی» با «جذب دانش تخصصی» لازم برای ایجاد امنیت سایبری پرداخته شده است. چارچوب این پژوهش مبتنی بر دیدگاه دانش‌محور بنگاه و هزینه مبادلات دانش بوده و روش پژوهش آن نیز از نوع توصیفی – پیمایشی و ازنظر هدف کاربردی است. برای سنجش فرضیه‌ها از نمونه آماری ۲۶۲ نفری شاغل در مراکز تجزیه‌وتحلیل، تبادل و اشتراک‌گذاری اطلاعات حساس در مورد امنیت سایبری، استفاده شده است. برای گردآوری داده‌ها از پرسشنامه استفاده شده و روایی هر سازه با محاسبه همبستگی «آیتم – آزمون»، «مورد – سایر موارد» و میانگین همبستگی «بین موارد»، مورد آزمایش واقع و اعتبار آن نیز با آلفای کرونباخ تأیید گردیده است. تجزیه‌وتحلیل عاملی مؤلفه اصلی نیز با چرخش مورب (نامتعامد) انجام یافته است. یافته‌های پژوهش نشان می‌دهد که «باور به منبع»، «اعتقاد به سودمندی دانش» و «باور به تبادل متقابل» با جذب دانش رابطه مثبت و معنی‌دار دارند، ولی «اعتقاد به پاداش» رابطه‌ای با «جذب دانش» ندارد. همچنین، در پایان تأثیر یافته‌های پژوهش بر متخصصان این موضوع و تحقیقات آینده مورد بحث قرار گرفته است.

واژگان کلیدی:
امنیت سایبری، تبادل اطلاعات، دیدگاه دانش‌محور، دانش ضمنی، جذب دانش.

۱. استادیار دانشگاه فنی و حرفه‌ای – دانشکده شهید شمسی‌پور (نویسنده مسئول) *naser8700@yahoo.com*
۲. دانشیار دانشگاه عالی دفاع ملی

جستارگشایی

بشر از آغازین روزهای حیاتش در معرض آسیب، تعرض و تهدید قرار داشته و از ابتدا به فکر امنیت، آرامش و آسایش بوده است. امنیت در لغت از ریشه امن به معنای در امان بودن و مصون بودن از هرگونه تهدید و ترس است (جهان بزرگی، ۱۳۸۸:۳۱). کشورها برای مقابله با تهدیدات روزافزون، به‌ویژه در فضای سایبری و همچنین کسب فرصت‌های گسترده و جلوگیری از عقب‌ماندگی سایبری، نیازمند تدوین راهبرد سایبری جامع و کارآمد و مطابق با ماهیت خاص و پویای فضای سایبر هستند (ترابی، ۱۳۹۸: ۱۸۵).

امنیت سایبری مؤثر و کارآمد، در هردوی سازمان‌های دولتی و خصوصی، برای جلوگیری از اختلال در کسب‌وکارها و اطمینان از استمرار فعالیت‌ها، ضرورت داشته (تونسی و رایس[1]، ۲۰۱۸) و ایجاد چنین امنیتی نیازمند دانش است (بن- اشر و گونزالز[2]، ۲۰۱۵). بااینکه اجزای سخت‌افزاری و نرم‌افزاری موردنیاز برای برقراری این امنیت نسبتاً مشابه بوده و به‌راحتی و با هزینه کم یا حتی به‌رایگان در دسترس هستند (هافمن و راماج[3]، ۲۰۱۱)، اما برخورداری از دانشِ کاملاً تخصصی برای ترکیب و به‌کارگیری مؤثر این اجزا برای ایجاد امنیت و دفاع سازمانی (برای مثال، با طراحی معماری سامانه‌های انعطاف‌پذیر و پیاده‌سازی مؤثر آن‌ها) ضروری است (باقری و کائو[4]، ۲۰۱۵)؛ ازاین‌رو باید توجه داشت که امنیت سایبری، توانایی و قابلیت پیچیده‌ای است که به‌راحتی و تنها با خرید اجزای فناورانه ایجاد نمی‌شود؛ بلکه نیازمند مهارت و دانش تخصصی در مورد چگونگی سازماندهی و ایجاد هماهنگی بین این مؤلفه‌ها است. درواقع این دانش تخصصی است که موجب دفاع واقعی می‌شود (سولز و نیکرک[5]، ۲۰۱۳). از مهم‌ترین مسائل در حفظ امنیت سایبری کشور، استقلال و خودکفایی درزمینهٔ تولید محصولات امنیت سایبری است؛ چراکه محصولات وارداتی ازجمله نرم‌افزار، سخت‌افزار و محصولات شبکه، شکاف‌های امنیتی نهفته و آشکاری دارند؛ بنابراین، نقش نهادهای پژوهشی فعال درزمینهٔ امنیت سایبری برای برآورده سازی این نیاز بسیار پراهمیت است (قوچانی خراسانی، ۱۳۹۶).

علاوه بر این، با توجه به پیشرفت سریع فناوری و چرخه عمر کوتاه این اجزا، دانش موردنیاز برای ایجاد امنیت سایبری نیز سریع منسوخ می‌شود (کاساس[6] و همکاران، ۲۰۱۷). ازاین‌رو، سازمان‌ها به‌منظور مقابله با تهدیدات سایبری روزافزون، مجبور به به‌روزرسانی دانش موجود و کسب دانش جدید هستند (کاساس و همکاران، ۲۰۱۷) و هر سازمانی که ساماندهی امنیت سایبری را ضروری می‌داند، مسلماً علاقه‌مند جذب مستمر دانش تخصصی خواهد بود. جذب دانش درواقع به مفهوم توانمندسازی سازمان برای انتقال، ادغام

1. Tounsi & Rais
2. Ben-Asher & Gonzalez
3. Hofmann & Ramaj
4. Bagheri, & Kao
5. Solms & Niekerk
6. Casas

و استفاده از دانش جدید کسب‌شده از منابع خارجی است (پارک[1]، ۲۰۱۱). فضای سایبر به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی گفته می‌شود که بدون در نظر گرفتن جغرافیای فیزیکی شکل می‌گیرد. فضای مجازی به‌عنوان فضای خلق‌شده توسط رایانه‌ها و شبکه‌های الکترونیکی از نمودهای عصر جهانی‌شدن در کنار فضای واقعی به یک واقعیت ملموس تبدیل شده است (افضلی و قالیباف، ۱۳۹۲).

فضای سایبری به‌مانند فضای حقیقی و ژئوپلیتیکی دارای تهدیدها و آسیب‌پذیری‌هایی است که انسان در برخورد با آن شرایطی را برای مصونیت در یک چرخه دائمی شکل می‌دهد. فضای سایبر هم ازآن‌جهت که همه امور آدمی را در برمی‌گیرد و هم ازآن‌جهت که مبانی انسان‌شناختی فضای تولید فنّاوری و محتوی را در برگرفته مخاطراتی را متوجه انسان و جامعه اسلامی می‌نماید (کیان‌خواه، ۱۳۸۹:۳۵). مهم‌ترین عامل امنیت سایبری، دانش سایبری است. به تعبیری دیگر، دانش سایبری عین قدرت است. تحقیقات صورت گرفته حاکی از آن است که اگر سازمان‌ها در جذب دانش موفق باشد، هزینه سرمایه‌گذاری در تمامی سطوح امنیت اطلاعاتی (گال-اور و گوسه[2]، ۲۰۰۵) کاهش یافته و تلاش‌های ناکارآمد نیز کمتر تکرار می‌یابند (فلِدی، فِنز و لچنر[3]، ۲۰۱۳). علاوه بر این، اثربخشی راه‌حل‌های امنیتی نیز بهبود می‌یابد (صفا و وون سولمز[4]، ۲۰۱۶).

ازآنجاکه سازمان‌ها عموماً دانش را با یادگیری توسط اعضای خود یا استخدام اعضای جدید جذب کنند (مارچ[5] ۱۹۹۱؛ سایمون[6]، ۱۹۹۱)، در این مطالعه، جذب دانش در سطح فردی موردتوجه و تجزیه‌وتحلیل قرار گرفته است. گذشته از آن، این انسان‌ها هستند که دانش تخصصی را فراگرفته، توسعه داده و از آن برای هماهنگی اجزای فنی به‌منظور دفاع سایبری مؤثر استفاده می‌کنند؛ بنابراین جای تعجب ندارد که تحقیقات اخیر به این نکته تأکیددارند که بدون بررسی ارتباط اقدامات فردی با نتایج امنیت سایبری، درک ما از امنیت سایبری ناقص و بی‌فایده خواهد بود (لوبه و بومه[7]، ۲۰۱۷). بااین‌حال، تا به امروز مطالعات اندکی در این زمینه صورت گرفته است. بررسی اجمالی ادبیات مرتبط توسط لابه و بومه (۲۰۱۷) نشان می‌دهد که تقریباً کلیه تحقیقات انجام‌شده در مورد تبادل اطلاعات امنیت سایبری و در پی آن جذب دانش موردنیاز، دارای محدودیت‌هایی بوده‌اند: اول، بیشینه آن‌ها به‌جای تجزیه‌وتحلیل افراد به بررسی اطلاعات غیرشخصی مانند فایل‌های سوابق[8] پرداخته‌اند (مایلارت[9] و همکاران، ۲۰۱۷) و بیشتر آن‌ها نیز به تئوری بازی محض یا

1. *Park*
2. *Gal-Or & Ghose*
3. *Feledi, Fenz, & Lechner*
4. *Safa & Von Solms*
5. *March*
6. *Simon*
7. *Laube & Böhme*
8. *log-files*
9. *Maillart*

شبیه‌سازی محدودشده‌اند (فیلدر[1] و همکاران، ۲۰۱۴). دوم، فضای امنیت سایبری غالباً به اطلاعات حساس و طبقه‌بندی‌شده‌ای نیاز دارد که به اشتراک‌گذاری یا انتشار آن از طریق کانال‌های عمومی ممکن نیست (لوبه و بومه، ۲۰۱۷). سوم، دانش موردنیاز برای ایجاد امنیت سایبری، دانش تخصصی است و درواقع بسیار ضمنی است؛ یعنی به تجربه شخصی افراد محدود است؛ بنابراین، نه‌تنها توصیف عینی چنین دانشی (مستندسازی آن به‌صورت راهنما یا کتاب درسی) کار دشواری است، بلکه بدون تعامل اجتماعی قوی بین فرستنده و گیرنده، این دانش به‌راحتی نمی‌تواند منتقل شود (نوناکا و تاکوچی، ۱۹۹۵).

اگرچه برخی تحقیقات انجام‌شده درزمینهٔ امنیت سایبری به بررسی انتقال دانش صریح که امکان مستندسازی آن در قالب انجمن‌ها و بانک‌های اطلاعاتی وجود دارد (به‌عنوان‌مثال، یان[2] و همکاران (۲۰۱۶) و صفا و وون سولمز (۲۰۱۶))، پرداخته‌اند؛ اما هیچ اطلاعی از کار تجربی که به تجزیه‌وتحلیل انتقال و جذب دانش ضمنی درزمینهٔ امنیت سایبری پرداخته باشد، وجود ندارد؛ این امر حاکی از شکاف مهم تحقیقاتی است (ونگ و نو[3]، ۲۰۱۰). چهارم و سرانجام، حتی اگر جذب دانش ضمنی مستلزم تعامل انسانی باشد، فرایند اجتماعی به‌تنهایی بر این دلالت ندارد که دانش درواقع جذب خواهد شد. اگر صاحب هر دانشی نتواند یا مایل به انتقال آن به افراد دیگر نباشد، ممکن است تعامل انسانی بی‌فایده باشد. ادبیات موجود در این زمینه بر نگرش‌ها، انگیزه‌ها و زمینه‌هایی که بر عدم تمایل فرد برای به اشتراک‌گذاری اطلاعات تأثیر می‌گذارند، متمرکز است (زیباک و سیمپسون[4]، ۲۰۱۹) و در مقابل، هیچ اطلاعی از پژوهشی که به بحث مربوط به جذب دانش حاصل از تعامل اجتماعی و تأثیر آن روی امنیت سایبری پرداخته باشد، وجود ندارد.

در بررسی پیشینه داخلی نیز به پژوهشی که بر نقش باورهای انسانی در جذب دانش و امنیت سایبری تمرکز کرده باشد، دست نیافتیم، اما در برخی مقالات به تحقیقاتی اشاره شده است که عمدتاً در خصوص عوامل مؤثر بر اشتراک دانش است که به برخی از آن‌ها اشاره می‌شود. انتظاری و همکاران (۱۳۹۵) در پژوهش «ارائه الگوی رفتار اشتراک دانش متخصصان ایرانی در فضای مجازی» به این نتیجه رسیدند که حضور متخصصان ایرانی در شبکه‌های تخصصی عملاً برای دسترسی هر چه بیشتر به منافع مشترکی است که در کنار دیگر همتایانشان و از طریق ارتباط با آن‌ها حاصل می‌شود. پس انگیزه‌هایی فراتر از منافع شخصی مبنای اشتراک دانش است (انتظاری و همکاران، ۱۳۹۵: ۲۰۵- ۱۶۸). نظافتی و همکاران (۱۳۹٤) در مطالعه‌ای نشان دادند که افزایش سرمایه اجتماعی و بیشتر شدن تعاملات اجتماعی میان افراد، بر افزایش اشتراک‌گذاری دانش در انجمن‌های خبرگی اثر مثبت و معنی‌دار دارد. همچنین عوامل سخت‌افزاری و مادی نسبت به عوامل نرم‌افزاری، تأثیر بیشتری بر اشتراک‌گذاری دانش در انجمن‌های خبرگی دارند

1. *Fielder*
2. *Yan*
3. *Wang & Noe*
4. *Zibak & Simpson*

(نظافتی و همکاران، ۱۳۹۴: ۲۹۵- ۲۷۵). افجه و همکاران (۱۳۹٤) در مطالعه «ارائه الگوی رفتار اشتراک دانش دانشجویان شبکه اجتماعی دانشگاه تهران» دریافتند که به ترتیب عوامل گروهی با شاخص‌های ارتباطات و تعاملات اجتماعی؛ عوامل فردی با شاخص‌های اشتراک دانش آگاهانه، لذت‌بردن از کمک به دیگران و نگرش به‌منظور اشتراک دانش؛ و عوامل محیطی با شاخص‌های فرهنگی (آموزشی) و فنّاورانه بر رفتار اشتراک دانش دانشجویان در شبکه تأثیرگذار است (افجه، انتظاری و مرتجی، ۱۳۹۴: ۱۲۵- ۹۰). این پژوهش با هدف بررسی این محدودیت‌ها به مطالعه میزان دانشی که افراد در محیط محرمانه و مبتنی بر همکاری (که در آن دانش حساس، محرمانه و ضمنیِ موردنیاز برای ایجاد امنیت سایبری از طریق به اشتراک‌گذاری اطلاعات جذب می‌شود)، با موفقیت جذب می‌کنند، متمرکز شده است؛ ازاین‌رو، هم تمرکز و هم واحد تحلیل ما سطح فردی است. تحقیقات اخیر نشان داده است که مطالعه این اشتراک‌گذاری «اطلاعاتی- همکارانه» باید منجر به درک بهتر امنیت سایبری شود (لوبه و بومه، ۲۰۱۷)؛ بنابراین در این پژوهش نه‌تنها به بررسی عناصر مرتبط با این‌گونه اشتراک‌گذاری اطلاعات پرداخته شده، بلکه نتایج آن نیز ازنظر جذب دانش فردی شده است.

در این پژوهش، ابتدا چارچوبی مبتنی بر دیدگاه دانش‌بنیان شرکت‌ها ارائه و استدلال می‌شود که جذب دانش ضمنی با باورهای افراد مرتبط است. سپس با استفاده از رگرسیون پروبیت ترتیبی، این مدل با استفاده از داده‌های روان‌سنجی ۲۶۲ کارمند بخش فناوری اطلاعات و مراکز تجزیه‌وتحلیل و به اشتراک‌گذاری اطلاعات، آزمایش گردید. یافته‌ها نشان می‌دهد که «باور به منابع»، «اعتقاد به سودمندی» و «باور به تبادل متقابل» با جذب دانش رابطه مثبت دارند، درحالی‌که اعتقاد به پاداش‌های مادی این‌گونه نیست.

مبانی نظری

به اشتراک‌گذاری دانش، نوعی توزیع دانش است که از تمامی حالات دیگر متمایز است؛ چراکه اشتراک‌گذاری دانش، به اشتیاق افرادْ برای قرار دادن تجربه و تخصص خود در حوزه مشخص یا مسئله معین در اختیار سایرین بستگی دارد. اشتراک‌گذاری دانش، فرایند قطعی و بدون قید و شرطِ توزیع دانش است که در افزایش سطح دانش گروه یا سازمان بسیار مؤثر است. در سامانه‌های باز، به اشتراک‌گذاری دانش سازوکاری باارزش در افزایش دانش و پویایی سازمان محسوب می‌شود. اهمیت این موضوع در این واقعیت نُهفته است که هدف آن ایجاد پیوند بین سطح فردی (جایی که دانش در آن قرار دارد) و سطح سازمانی (جایی که دانش مورداستفاده واقع و ایجاد ارزش می‌کند) است (سانچز و همکاران[1]، ۲۰۱۳: ۳۹۱). تصمیم یک فرد به اشتراک‌گذاری دانش با فرد دیگر بستگی به اعتماد بین آن‌ها دارد و این اعتماد، بیشتر حالت حسی دارد تا استدلال منطقی؛ بنابراین، بر اساس «میزان تمایل فرد به نسبت دادن نیات خوب به افراد دیگر و اطمینان از حرف‌ها و اقدامات آنان» شکل می‌گیرد (رحمدل، ۱۳۹۸: ۹۲).

1. *Sanchez et al*

دیدگاه دانش‌بنیان شرکت‌ها بر این باور است که دانش منبع باارزش، کمیاب و تقلیدناپذیر بوده و ازاین‌رو منبع و عامل مهم مزیت رقابتی سازمان‌ها محسوب می‌شود (نیکرسون و زنگر[1]، ۲۰۰۴) و دانش تخصصی سهم بسزایی در نوآوری محصول، فرآیند و خدمات دارد (شیلینگ[2]، ۲۰۱۰)؛ بنابراین، سازمان‌ها باید به‌طور مستمر دانش تخصصی جذب کنند تا با نوآوری‌های خود امنیت سایبری را برای اجزای فناوری اطلاعات و معماری سامانه‌ها فراهم کنند. جذب دانش سازمانی نتیجه یادگیری فردی (یعنی انسان) است و سازمان‌ها نیز دانش را فقط با یادگیری اعضای خود یا با استخدام افراد جدید جذب می‌کنند (گرانت[3]، ۱۹۹۶)؛ بنابراین، تمرکز این مقاله به یادگیری اعضای سازمان است. از این منظر دانش سازمانی جدید درنتیجه جذب دانش فردی از سوی این اعضا خلق می‌شود (باک و کیم[4]، ۲۰۰۲).

بااین‌حال، برای همه افراد، جذب دانش از فراسوی مرزهای سازمان کار آسانی نیست؛ به‌طورمعمول، فرد قبل از انجام مبادله، متحمل هزینه‌های زیادی می‌شود. این هزینه‌ها شامل زمان صرف شده، منابع مالی اختصاص‌یافته برای دریافت اطلاعات، تصمیم‌گیری و روند تعامل با دیگران است (ویلیامسون[5]، ۱۹۸۱). در مراکز تجزیه‌وتحلیل و به اشتراک‌گذاری اطلاعات، این هزینه‌ها به‌محض شروع تعامل فرد با دیگران آغاز می‌شود؛ زیرا تعامل اجتماعی تنگاتنگ بین دو فرد برای انتقال موفقیت‌آمیز دانش ضمنی ضروری است (نوناکا و تاکوچی، ۱۹۹۵). همچنین، تحقیقات قبلی حاکی از آن است که اگر اشتراک‌گذاری اطلاعات زمان‌بر، بیش‌ازحد دشوار و یا نیازمند تلاش زیاد باشد، افراد تمایل کمتری به مشارکت در انتقال دانش خواهند داشت و مسلماً میزان دانش منتقل‌شده نیز کاهش خواهد یافت (آژانس امنیت شبکه و اطلاعات اتحادیه اروپا[6]، ۲۰۱۸). علاوه بر این، دانش ممکن است ازنظر فرد مهم یا بی‌ربط باشد؛ بنابراین، بهتر است قبل از انجام هرگونه ارزیابی خاص، افراد بررسی کنند که آیا دانش موجود در مرکز تجزیه‌وتحلیل و اشتراک‌گذاری اطلاعات در کل ارزش هزینه تعامل موردنیاز برای جذب آن را دارد یا نه. تا زمانی که پاسخ این ارزیابی مثبت نباشد، بعید است افراد خود را درگیر هرگونه تعامل عمیق نمایند. هنگامی که افراد چنین ملاحظاتی داشته باشند، معمولاً از سرنخ‌ها و کاوش‌ها برای ساده‌کردن فرایند تصمیم‌گیری استفاده می‌کنند (گابیکس[7] و همکاران، ۲۰۰۶). با استفاده از چنین سرنخ‌هایی، مسلماً در خصوص مفید یا غیرمفید بودن اطلاعات دریافت‌شده، ارزیابی ذهنی و مبتنی بر اعتقاد جایگزین ارزیابی عینی و غیرشخصی می‌شود (بوش، ولبردا و بوئر[8]، ۱۹۹۹)؛ بنابراین هر زمان که چنین اعتقادی ایجاد شود، افراد علاقه‌مند مشارکت در تعامل اجتماعی که مقدم بر جذب دانش است، می‌شوند (لیختنتالر و ارنست[9]،

1. *Nickerson & Zenger*
2. *Schilling*
3. *Grant*
4. *Bock & Kim*
5. *Williamson*
6. *ENISA (European Union Agency for Network Information Security)*
7. *Gabaix*
8. *Bosch, Volberda, & Boer*
9. *Lichtenthaler & Ernst*

۲۰۰۷). ازاین‌رو، جذب دانش می‌تواند با میزان اطمینان فرد به این‌که دانش موجود در سازمان یا مرکز، دارایی یا منبع (بارنی، ۱۹۹۱) باارزش، نادر و غیرقابل تقلید و واجد ارزش جذب (اعتقاد به منبع)، محسوب می‌گردد، ارتباط مثبت داشته باشد؛ بنابراین:

فرضیه اول عبارت است از: «جذب دانش با «اعتقاد به منبع» ارتباط مثبت دارد». فرضیه اول با این اعتقاد فرد که هزینه‌های تبادل دانش بر مزایای حاصل از چنین تعامل اجتماعی (اشتراک‌گذاری دانش) پیشی خواهد گرفت، ارتباط دارد؛ مزایایی که با جذب دانش ناشی از اشتراک‌گذاری تحقق می‌یابند.

فرضیه دوم: باور به مفید بودن دانش. اگرچه اعتقاد به منبع ممکن است فرد را متمایل به تعامل با دیگران کند؛ اما لزوماً به معنای آن نیست که دانش موجود مستقیماً در کارهای خاص شغلی فرد، کاربرد دارد. به‌عنوان‌مثال، کارکنان مراکز تجزیه‌وتحلیل و به اشتراک‌گذاری اطلاعات ممکن است اطلاعاتی را که در کل برای صنعت یا سازمان مفید است را مبادله کنند، اما این اطلاعات ممکن است هیچ کمک خاصی برای انجام وظایف شغلی فرد نکنند. تحقیقات نشان می‌دهد که افراد لزوماً و فقط به نفع سازمان کار نمی‌کنند؛ یعنی صرفاً به نفع سازمان وارد عمل نمی‌شوند (ناگین[1] و همکاران، ۲۰۰۲). البته نظریه همسوسازی اهداف معتقد است که اهداف فردی و سازمانی لزوماً متناقض نیستند (فاس[2]، ۲۰۱۱)، درنتیجه، فرد نه‌تنها مفید بودن کلی دانش موجود برای سایر اعضای مراکز تجزیه‌وتحلیل و به اشتراک‌گذاری اطلاعات را در نظر می‌گیرد – آیا این دانش ارزش هزینه تعامل را دارد؟– بلکه به ارزیابی این مهم که این دانش تا چه اندازه در انجام وظیفه شغلی خاص وی مفید است نیز می‌پردازد.

ازآنجاکه ارزیابی عملکرد شغلی فرد ممکن است به‌عنوان عامل مهمی در امنیت سایبری سازمانی در نظر گرفته شود، بنابراین به‌احتمال‌زیاد افراد انگیزه خاصی برای مطالعه سودمندی اطلاعات خواهند داشت (لوئیف و کلور[3]، ۲۰۱۵). ازاین‌رو، جذب دانش می‌تواند ارتباط مستقیمی با میزان باور افراد به دانش موجود و به‌ویژه نقش آن در انجام وظایف شغلی خود داشته باشند (اعتقاد به سودمندی). پس فرضیه دوم عبارت است از: «جذب دانش با اعتقاد به سودمندی رابطه مثبت دارد».

اگر فرضیه اول مربوط به ارزیابی اساسی فرد و تعیین این‌که آیا مشارکت در به اشتراک‌گذاری دانش ارزش آن را دارد (یعنی هزینه‌های چنین تعامل اجتماعی تحت‌الشعاع مزایای حاصل از جذب دانش حاصل قرار خواهد شد) باشد، آنگاه فرضیه دوم با طرح این بحث که جذب دانش ممکن است برای کارهای شغلی فرد مفید باشد، یک گام جلوتر خواهد بود.

فرضیه سوم: باور به پاداش. بر اساس نظریه همسوسازی هدف افراد ممکن است دانش تخصصی جذب‌شده را در اختیار اعضای دیگر سازمان قرار ندهد. درواقع، افراد معمولاً رفتار خود را با اهداف بازگشتی

1. *Nagin*
2. *Foss*
3. *Luijf & Klaver*

هماهنگ می‌کنند؛ یعنی انتظار دارند هر وقت رفتار موردعلاقه سازمان از آن‌ها سر زند، پاداش به آن‌ها داده شود (ناگین و همکاران، ۲۰۰۲)؛ بنابراین، درصورتی‌که باور نداشته باشند که سازمان چنین پاداش‌هایی را خواهد داد، ممکن است با پرهیز از به اشتراک‌گذاری دانش، جایگاه خود در سازمان را تثبیت نمایند و یا با راه‌اندازی شرکت یا فروش خدمات مشاوره خصوصی به صنعت از عضویت خود در سازمان به نفع خود استفاده کنند. درنتیجه، فرد دانش را نه به خاطر سازمان، بلکه به نفع تجارت خصوصی خود جذب خواهد کرد؛ بنابراین، سازمان‌ها برای حل این مشکل، مجبور به پرداخت پاداش مادی هستند تا دانش جذب و به نفع سازمان به‌اشتراک گذاشته شود. برای مثال، مجموعه آزمایشگاه‌های باکمن هر سال ۱۰۰ کارمند برتر خود درزمینهٔ به اشتراک‌گذاری اطلاعات را در اجلاس سالانه خود شناسایی می‌کند (سینگ[1]، ۲۰۰۵) و لوتوس دولپمنت[2]، بخشی از آی‌بی‌ام، نیز به کارمندان خود در قبال فعالیتشان درزمینهٔ به اشتراک‌گذاری اطلاعات، پاداش می‌دهد (داونپورت و گلیسر[3]، ۲۰۰۲). این پاداش ممکن است شامل ارتقاء شغلی، امنیت بیشتر شغلی، افزایش حقوق یا قدرت و مسئولیت بالاتر در سازمان شود (باک و کیم، ۲۰۰۲). تحقیقات نشان می‌دهد که چنین پاداش‌هایی نقش مثبتی در ساعات کاری، فداکاری و عملکرد افراد دارد (انسینوزا، گاینور و ریتزر[4]، ۲۰۰۷).

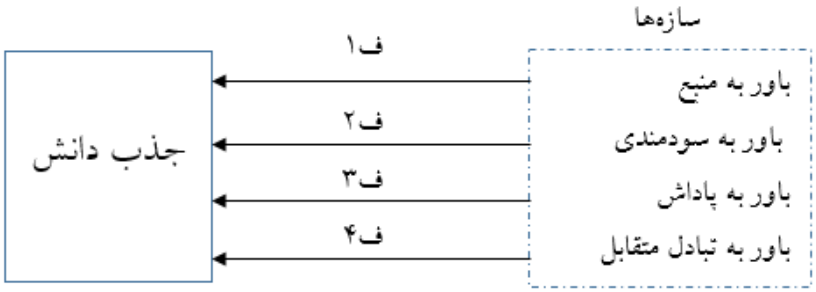
بنابراین، هرچه افراد باور بیشتری به دریافت «پاداش‌های مادی یا سخت» در مقابل جذب موفق دانش داشته باشند (باور به پاداش)، احتمال این‌که بر تحقق چنین جذبی متمرکز شوند، بیشتر است. پس فرضیه سوم عبارت است از: «جذب دانش با باور به پاداش رابطه مثبت دارد».

اگر فرضیه دوم با ارزیابی فرد در این خصوص که آیا مشارکت در اشتراک دانش به انجام موفقیت‌آمیز وظایف شغلی آن‌ها کمک می‌کند (یعنی مزایای ناشی از جذب دانش ازنظر انجام موفق وظایف شغلی بر هزینه‌های چنین تعامل اجتماعی پیشی می‌گیرند.) ارتباط داشته باشد، فرضیه سوم نشان می‌دهد که در صورت جبران چنین جذبی با پاداش‌های ارائه‌شده از سوی سازمان، می‌توان جذب دانش را تقویت کرد.

فرضیه چهارم: باور به تبادل متقابل. با فرض این‌که دانش منبع ارزشمند، کمیاب و غیرقابل تقلید است، ارزش واحد دانش درزمینهٔ امنیت سایبری متناسب با پیشرفت تدریجی امنیت سایبری ناشی از این واحد دانش است (بودین و همکاران، ۲۰۱۸). ازآنجاکه افراد یقین دارند که هر دانشی که به اشتراک می‌گذارند، مزایایی را برای دیگران خواهد داشت، بنابراین، ممکن است در مقابل انتظار داشته باشند که خود نیز دانش مناسب و کافی کسب کنند. به‌طورمعمول، انسان‌ها چنین تبادل عادلانه‌ای را بیش از ترتیبات دیگر ترجیح می‌دهند (کلم و مرسیر- یتر[5]، ۲۰۰۶) و نقض‌کنندگان این اصل عادلانه را مجازات می‌کنند. برخی اوقات

1. Singh
2. Lotus Development
3. Davenport & Glaser
4. Encinosa, Gaynor, & Rebitzer
5. Kolm & Mercier-Ythier

نیز از جبران چیز باارزشی که دیگران ارائه می‌کنند، خودداری می‌نمایند (تریکومی[1] و همکاران، ۲۰۱۰). انصاف متقابل، متغیر مهمی در طراحی الگوریتم‌های انتخاب همتا در شبکه‌های نظیر به نظیر است، طوری‌که اپراتورهای این شبکه‌ها روش‌هایی را برای حذف افراد مزاحم و سربار که بدون ارائه هیچ‌گونه اطلاعاتی خواستار اطلاعات هستند، تدوین کرده‌اند (ونگ[2]، ۲۰۱۱). این‌که یک فرد تا چه اندازه قادر به جذب دانش ضمنی از طریق تبادل اجتماعی است، بستگی به این دارد که این فرد تا چه اندازه مایل است هر زمان که از دیگران اطلاعات دریافت می‌کند، عمل متقابل انجام دهد (یونگ و لئو[3]، ۲۰۰۴)؛ بنابراین، اگر فرد باور داشته باشد که به اشتراک‌گذاری دانش مهم یک‌طرفه خواهد بود، ممکن است به تعامل اجتماعی خاتمه دهد. ازاین‌رو، فرضیه چهارم این پژوهش عبارت است از: «جذب دانش با اعتقاد به تبادل متقابل رابطه متقابل دارد». در شکل زیر سازه‌های مختلف – یعنی مجموعه متغیرهای مستقل و فرضیه مربوط به آن‌ها را نشان داده و بر رابطه بالقوه آن‌ها با متغیر وابسته «جذب دانش» تأکید می‌کند.



شکل ۱: مدل جذب دانش. هر سازه و فرضیه مربوط به آن (ف ۱ تا ف ۴)، **به‌طور بالقوه با متغیر وابسته (جذب دانش) رابطه مثبت دارد.**

روش‌شناسی

در این بخش شیوه نمونه‌گیری، جمعیت آماری، چگونگی اندازه‌گیری متغیر مستقل، سازه‌ها، نحوه توزیع پرسشنامه‌ها (به‌منظور اندازه‌گیری موارد و سازه‌ها) و همچنین چگونگی انجام تحلیل توضیح داده شده است.

جامعه آماری و نمونه‌گیری

ازآنجاکه استدلال نظری این پژوهش بر جذب دانش از طریق تعامل اجتماعی متمرکز است، باید شیوه نمونه‌گیری نیز متناسب با آن باشد؛ بنابراین، با توجه به این‌که مدیران و کارکنان بخش فناوری و امنیت سایبری سازمان‌ها و مراکز، به‌منظور تسهیل تبادل اطلاعات بین فردی، در برخی هم‌اندیشی‌ها حضور یافته

1. *Tricomi*
2. *Wang*
3. *Xiong & Liu*

و سعی در کسب دانش دارند؛ داده‌های پژوهش نیز از گروه‌های کاربری بخش‌های تبادل و تجزیه‌وتحلیل جمع‌آوری شده و نظرسنجی و مجموعه داده‌های مربوط به آن با آنچه مرمود[1] و همکاران (۲۰۱۹) شرح داده‌اند، همخوانی دارد.

جامعه آماری پژوهش، مدیران و متخصصانی بودند که باید امنیت سایبری سازمان‌های مربوطه به خود، چه بخش دولتی و چه بخش خصوصی را فراهم می‌کردند. لازم به ذکر است که این افراد درزمینهٔ کاری خود تقریباً هیچ تعاملی با افراد عادی نداشتند. ازاین‌رو، این شرایط با این استدلال ما که «دانش لازم برای ایجاد امنیت سایبری نه‌تنها دارای طبقه‌بندی بوده و شناسایی آن دشوار است، بلکه ضمنی بوده و در تجربه شخصی افراد نهفته است؛ به‌گونه‌ای که تعامل اجتماعی بین افراد برای انتقال آن ضروری است»، مطابقت دارد.

هر زمان که فرد خاصی اطلاعات مربوط به تهدیدی را به اشتراک بگذارد، سایر افراد از طریق سیستم داخلی با یکدیگر تماس گرفته و با اظهارنظر در مورد اطلاعات به اشتراک گذاشته‌شده، تلاش می‌کنند تا با تداوم این تماس‌ها، تبادل اجتماعی را برقرار کنند. هنگامی که تماس با یک پاسخ کوتاه در مورد اطلاعات مربوط به تهدید برقرار شد، افراد درگیر در مکالمه با ابتکار عمل خود برای به اشتراک‌گذاری اطلاعات دقیق امنیتی، قرار ملاقات می‌گذارند (برای مثال، به‌طور غیررسمی در طول ناهار، جلسات گروهی یا اجلاس‌های مخصوص صنعت). هر فرد خود تصمیم می‌گیرد که با چه کسی و چگونه ملاقات کند. آن‌ها همچنین در مورد میزان اطلاعات به اشتراک گذاشته‌شده نیز تصمیم می‌گیرند.

سنجش و اندازه‌گیری

در این مطالعه افرادی موردتوجه بودند که حاضر به اظهارنظر درباره باورهای خود بودند؛ بنابراین، برای عملیاتی کردن سازه‌های پژوهش از روش روان‌سنجی استفاده گردید (نانلی و برنستین[2]، ۲۰۱۷) و برای کسب اطلاعات از افراد، شاخص ترتیبی جدیدی به‌کاربرده شد. از پاسخ‌دهندگان درخواست گردید تا پاسخ دهند «چه مقدار از اطلاعات انحصاری را از طریق مبادله اطلاعات امنیتی با سایر شرکت‌کنندگان دریافت می‌کنند؟».

برای بررسی باورهای مختلف و مفروض از مقیاس روان‌سنجی موجود استفاده شد. (جدول شماره ۱ جزئیات سازه‌ها، منابع آن‌ها، ترکیب و جمله‌بندی آیتم‌ها، موارد حذف‌شده (در صورت وجود)، بارهای عاملی و آلفای کرونباخ را نشان می‌دهد). پاسخ‌دهندگان ازنظر جنسیت، سن و سطح تحصیلات نیز کنترل شدند. جنسیت به‌صورت (زن، مرد) و سن در قالب چهار گروه سنی (۳۰-۲۱، ۴۰-۳۱، ۵۰-۴۱، ۵۰ سال به بالا) و سطح تحصیلات نیز در شش گروه (دیپلم، لیسانس، کارشناسی ارشد، دکترا، هیچ‌کدام،

1. *Mermoud*
2. *Nunnally & Bernstein*

سایر موارد) دسته‌بندی شد. همچنین موقعیت سلسله مراتبی افراد در سازمان (کارمند، کارمند ارشد، مدیر میانی، مدیر عالی، عضو هیئت‌مدیره و سایر موارد) نیز لحاظ شد. این موقعیت ممکن است به ترتیب بر تمایل افراد برای به اشتراک‌گذاری دانش و شدت آن تأثیر بگذارد (کای[1] و همکاران، ۲۰۱۳). کسانی که دارای دانش باارزش هستند، ممکن است آن را به‌عنوان عامل تضمین‌کنندهٔ امنیت شغلی خود محسوب کنند. البته معقول‌ترین پاسخ به این پرسش، دادن پاداش مادی یا غیرمادی در مقابل ارائه اطلاعات است. راه‌حل ساده، بستن قراردادهای کاری با متخصصان برای ایجاد اعتماد در آنان است (رحمدل، ۱۳۹۶:۱۱۳).

جدول ۱: سازه‌ها

سنجه	نوع	مورد	گزاره	.Fact. l	Cr. α
متغیر وابسته					
جذب دانش	شاخص طبقه‌ای ترتیبی	-	چه مقدار اطلاعات منحصربه‌فرد از طریق تبادل اطلاعات امنیتی دریافت می‌کنید؟	-	-
متغیرهای مستقل			خیلی کم کم متوسط زیاد خیلی زیاد		
باور به منبع	مقیاس لیکرت	RES1	ازنظر من افراد شبکه ما هر جا لازم باشد به دانش یکدیگر ارزش قائل می‌شوند.	حذف	۰,۸۲
		RES2	من معتقدم افراد شبکه من وقتی نیاز دارم پاسخ می‌دهند.	۰,۸۱	
		RES3	من معتقدم افراد شبکه من از دانش یکدیگر به‌طور مناسب استفاده می‌کنند	۰,۸۲	
		RES4	من معتقدم به درخواست‌های من برای دریافت دانش پاسخ داده می‌شود	۰,۸۶	
		RES5	من معتقدم افراد شبکه من بهترین دانش خود را به‌اشتراک می‌گذارند.	حذف	
باور به سودمندی	مقیاس لیکرت	US1	اشتراک‌گذاری اطلاعات زمان لازم برای انجام مسئولیت‌های شغلی من را کاهش می‌دهد.	۰,۸۵	۰,۷۱
		US2	اشتراک‌گذاری اطلاعات اثربخشی انجام کارهای شغلی را افزایش می‌دهد.	۰,۸۶	

1. Cai

سنجه	نوع	مورد	گزاره	.Fact. l	Cr. α
		US3	با در نظر گرفتن تمام جهات اشتراک‌گذاری اطلاعات مفید خواهد بود.	۰٫۶٤	
باور به پاداش	مقیاس لیکرت	HR1	من انتظار دارم در قبال اشتراک‌گذاری دانش با دیگران، با پرداخت حقوق بیشتر از من قدردانی شود.	۰٫۹۱	۰٫۸۱
		HR2	انتظار دارم درازای اشتراک‌گذاری دانش با سایر شرکت‌کنندگان، پاداش‌های پولی (مزایای اضافی) دریافت کنم.	۰٫۹۰	
		HR3	انتظار دارم درازای اشتراک‌گذاری دانش با سایر شرکت‌کنندگان، فرصت‌هایی برای یادگیری از دیگران به دست آورم.	حذف	
		HR4	انتظار دارم درازای به اشتراک‌گذاری دانش با سایر افراد از امنیت شغلی بیشتری برخوردار شوم.	۰٫۷۳	
باور به تبادل متقابل	مقیاس لیکرت	NOR1	من معتقدم کمک به دیگران اقدامی درست و ضروری است، زیرا می‌دانم افراد دیگر روزی به من کمک خواهند کرد.	حذف	۰٫۸
		NOR2	من معتقدم اگر من از طریق شبکه سازمان اطلاعات خود را با دیگران به اشتراک بگذارم، دیگران نیز در صورت نیاز به من کمک می‌کنند.	۰٫۸۲	
		NOR3	من معتقدم اگر دانش خود را از طریق شبکه با دیگران به اشتراک بگذارم، سایرین به درخواست من در مورد اطلاعات و دانش پاسخ خواهند داد.	۰٫۸۷	
		NOR4	من فکر می‌کنم افراد، باور تبادل متقابل خود را بر اساس بده و بستان، نیت و رفتار دیگران توسعه می‌دهند.	۰٫۷۹	

همچنین تعداد سال‌هایی که فرد درزمینهٔ اشتراک‌گذاری اطلاعات تجربه داشته است به‌صورت (تجربه به اشتراک‌گذاری اطلاعات در گذشته: خیر، کمتر از ۱، ۱ تا ۳، ۳ تا ۶، بیش از ۶)، کنترل گردید. چنین تجربه‌ای در حد زیادی با قصد به اشتراک‌گذاری اطلاعات (لی و ما[1]، ۲۰۱۲) مرتبط است؛ علاوه بر این، توان فرد در جذب دانش را نیز می‌توان با مدت‌زمان عضویت وی در سازمان ارزیابی کرد؛ زیرا افراد با گذشت زمان بینش بیشتری پیداکرده و روابط بین‌فردی را توسعه می‌دهند؛ ازاین‌رو، مدت همکاری افراد با سازمان نیز در نظر گرفته شد.

1. *Lee & Ma*

سرانجام، با بررسی وابستگی سازمانی هر فرد، ناهمگونی صنعت (آموزش، بانکداری و مالی، انرژی، بهداشت و سایر صنایع) کنترل شد. از این اطلاعات برای ساخت شاخص‌های دوگانه (متغیرهای مجازی) استفاده و پاسخ‌دهندگان به پنج گروه آموزش، بانکداری و مالی، انرژی، بهداشت و سایر صنایع گروه‌بندی شدند. اگر فردی وابسته به صنعت خاص بود برای هر متغیر مجازی مقدار ۱ و در غیر این صورت مقدار ۰ لحاظ می‌شد. ابزار گردآوری داده‌ها نیز پرسشنامه بود و تمام مراحل و توصیه‌های دیلمن، اسمیت و کریستین (۲۰۱۴) در طراحی پرسشنامه، پیش‌آزمون و اجرای پرسشنامه رعایت گردید. مقیاس لیکرت به‌صورت کاملاً مخالف (۱)، کاملاً موافق (۵) و نظری ندارم (۳)، رتبه‌بندی شد. پرسشنامه ابتدا در اختیار هفت گروه تمرکز در دانشگاه و بخش امنیت سایبری قرار داده شد و از بازخورد به‌دست‌آمده برای بهبود پرسشنامه و افزودن توضیحات اضافی استفاده گردید. پرسشنامه‌ها به‌صورت حضوری در جلسات و یا از طریق ایمیل در اختیار پاسخ‌دهندگان قرار گرفت و مرتب طی چهار ماه حضوری و یا از طریق تماس تلفنی و شبکه‌های اجتماعی پیگیری شد تا درنهایت داده‌های موردنیاز جمع‌آوری گردید.

تجزیه و تحلیل داده‌ها

پس از اتمام نظرسنجی، داده‌ها کنترل و به‌منظور تجزیه‌وتحلیل آماری فایل *STATA* تهیه گردید. آزمون‌های تعاملی هیچ تأثیر معنی‌داری در خصوص زمان پاسخ هر سنجه نشان نداد. روایی هر سازه با محاسبه همبستگی مورد – آزمون[۱]، همبستگی مورد سایر موارد[۲] و میانگین همبستگی بین موارد[۳] مورد آزمایش قرار گرفت (هایر[۴]، ۲۰۰۶). اعتبار آن نیز توسط آلفای کرونباخ تائید گردید. تجزیه‌وتحلیل عاملی مؤلفه اصلی تکراری با چرخش مورب (نامتعامد) انجام یافت تا واریانس کل استخراج‌شده یا تشریح شده به حداکثر برسد و هر مورد به‌وضوح روی یک عامل قرار گیرد. طی این فرایند، چهار مورد به دلیل عدم تطابق با این معیارها کنار گذاشته شدند. جدول شماره ۲ نتایج این روش و جدول ۱ موارد حذف‌شده را نشان می‌دهد. بارهای عاملی مستقیم و بارهای عاملی متقاطع از چهار عامل نهایی، درجه بالایی از روایی همگرا را نشان می‌دهد (هایر، ۲۰۰۶). همه این‌ها از ارزشی بالاتر از واحد برخوردار بودند. عامل اول ۱۹/۱ درصد از واریانس کل را تشریح و عدم وجود واریانس روش مشترک در نمونه را نشان داد (پادساکوف و ارگان[۵]، ۱۹۸۶). برای ساخت مقادیر مقیاس، نمرات آیتم‌های فردی اضافه شد و این مقدار به تعداد اقلام موجود در مقیاس تقسیم گردید (رینهولت، پدرسن و فاس[۶]، ۲۰۱۱). سازه وابسته در این پژوهش، ترتیبی و طبقه‌ای است؛ بنابراین مدل پروبیت ترتیبی مورد سنجش قرار گرفت. ضمن مقایسه با تخمین منطقی ترتیبی جایگزین، برآورد اصلی

---

۱. همبستگی آیتم–آزمون (*item–test*) میزان ارتباط هر یک از آیتم‌ها با مقیاس کلی را نشان می‌دهد.
۲. همبستگی آیتم– بقیه موارد (*item–rest correlation*) به عنوان همبستگی بین نمره مورد و نمره بقیه موارد تعریف و مشخص می‌شود. در ساخت آزمون از همبستگی آیتم–بقیه موارد برای تعریف ارتباط آیتم با کل امتیاز موارد دیگر استفاده می‌شود.
۳. میانگین همبستگی (*Average inter–item correlation*) روشی برای تحلیل پایایی داخلی است.
4. *Hair*
5. *Podsakoff & Organ*
6. *Reinholt, Pedersen, & foss*

تأیید و مشخص شد که مدل پروبیت ترتیبی تناسب بهتری با داده‌ها دارد. مدل با خطاهای استاندارد قوی برای خنثی کردن هرگونه ناهمگن بودن واریانس (انحراف) یا ناهم‌واریانسی، ارزیابی شد. برای کنترل سن، صنعت و تحصیلات، «گروه معیار» به‌طور خودکار در طول برآورد انتخاب شد. با توجه به توصیه کوهن و همکاران (۲۰۰۲)، همه مدل‌ها به‌تدریج و با واردکردن کنترل‌ها در مدل پایه، شکل گرفتند و سپس جلوه‌های اصلی اضافه گردید. در هر دو تخمین، قبل از واردکردن سنجه‌ها به تجزیه‌وتحلیل، متوسط فاصله مرکزی همه آن‌ها تعیین گردید. تناسب مدل نیز با مقایسه مکرر معیارهای اطلاعاتی آکائیکه[1] و بیزی[2] بین مشخصات مختلف مورد بررسی قرار گرفت.

جدول ۲: بارهای عاملی پس از چرخش مورب

مورد	بارگذاری روی عامل چرخش مورب				
	عامل ۱	عامل ۲	عامل ۳	عامل ٤	منحصر بودن
HR1	۰.۹۱				۰.۱٤
HR2	۰.۹۰				۰.۱۸
HR4	۰.۷۳				۰.٤٤
US1				۰.۸۵	۰.۲۶
US2				۰.۸۶	۰.۲۲
US3				۰.۶٤	۰.۳۹
NOR2			۰.۸۲		۰.۲۶
NOR3			۰.۸۷		۰.۲۱
NOR4			۰.۷۹		۰.۳۶
RES2		۰.۸۱			۰.۲۸
RES3		۰.۸۲			۰.۲۸
RES4		۰.۸۶			۰.۲٤
مقدار خاص	۲.۲۹	۲.۲۹	۲.۲۲	۱.۹٤	
نسبت واریانس	%۱۹.۱۰	%۱۹.۰۵	%۱۸.٤۸	%۱۶.۲۰	
واریانس تجمعی	%۱۹.۱۰	%۳۸.۱۶	%۵۶.۶٤	%۷۲.۸٤	

1. *Akaike*
2. *Bayesian*

یافته‌ها

آمار توصیفی پژوهش به‌طور خلاصه در جدول شماره ۳ ارائه شده است. همچنان که ملاحظه می‌شود، ۹۵ درصد پاسخ‌دهندگان مرد و ۳۲ درصد زیر ۴۰ سال و ۶۸ بالای ۴۰ سال هستند. درحالی که ۶۸ درصد گواهی دوره‌های مرتبط یا مدرک لیسانس دارند، کارورزان بدون مدرک رسمی ۲۰ درصد نمونه را تشکیل می‌دهند و فقط ۴/۶ درصد افراد دارای مدرک کارشناسی ارشد یا دکترا هستند. اکثر افراد نمونه در دو گروه کارمندان یا سرپرستان (۴۲ درصد پاسخ‌دهندگان) و مدیران میانی یا صف (۵۱ درصد) قرار می‌گیرند. تنها ۲/۷ درصد آنان مدیران عالی یا اعضای هیئت‌مدیره هستند. ۴۳ درصد پاسخ‌دهندگان حداکثر تا سه سال و ۴۸ درصد نیز بیش از سه سال تجربه اشتراک‌گذاری اطلاعات را دارند و ۵۲ درصد نیز در یکی از جلسات یا رویدادهای قبلی شرکت کرده‌اند.

جدول ۳: آمار توصیفی

متغیرها	Obs	Mean	.Std. Dev	Min	Max
جذب دانش	۲۶۰	۳.۱۳	۰.۸۶	۱	۵
باور به منبع دانش	۱۹۰	۳.۸۲	۰.۵۲	۱.۶۷	۵
باور به مفید بودن دانش	۲۰۸	۳.۷۸	۰.۶۲	۱.۶۷	۵
باور به پاداش	۱۹۵	۲.۱۶	۰.۷۵	۱	٤
باور به تبادل متقابل	۱۹۵	۳.۸۹	۰.۶۱	۱.۶۷	۵
اندازه سازمان	۲۶۰	٤.۵۷	۰.۹۰	۱	۵
کیفیت روابط با همکاران	۲۶۰	۳.۹۳	۰.۷۰	۳	۵
مشارکت بالقوه فردی	۲٤۳	۳.۰۷	۰.۹۱	۱	۵
مدت عضویت	۲۶۰	۶.۰۵	۵.۳۵	۰	۱۷

ازآنجاکه متغیر وابسته در این پژوهش از نوع ترتیبی است، باید تحلیل همبستگی یکنواخت انجام می‌شد. گذشته از آن، داده‌های این نوع متغیرها نیازی به توزیع نرمال ندارند؛ بنابراین در جدول شماره ۴ به‌جای همبستگی پیرسون، همبستگی اسپیرمن ارائه شده و به‌منظور پرهیز از طولانی شدن مطالب، همبستگی‌های مربوط به کنترل‌ها حذف گردیده است. جدول شماره ۵ مدل مناسب و نهایی را به همراه اقدامات تشخیصی آن ارائه می‌دهد.

جدول ۴: تجزیه‌وتحلیل همبستگی

	جذب دانش	باور به منبع دانش	باور به مفید بودن دانش	باور به پاداش	باور به تبادل متقابل
جذب دانش	۱				
باور به منبع دانش	۰.۲۸۶۰***	۱			
باور به مفید بودن دانش	۰.۲۷۷۹***	۰.۲۰۴۲**	۱		
باور به پاداش	۰.۰۲۵۸	−۰.۱۵۶۸	−۰.۰۶۰۲	۱	
باور به تبادل متقابل	۰.۳۵۴۳***	۰.۳۵۰۰***	۰.۲۴۸۹***	−۰.۰۰۰۱	۱
aρ: *p < ۰.۰۵; **p < ۰.۰۱; ***p < ۰.۰۰۱.					

یافته‌ها حاکی از تائید فرضیه اول است. «باور به منبع» با سطح معنی‌داری ($p<0.05$) با جذب دانش رابطه مثبت دارد؛ بنابراین، هرگاه شخصی به کسب دانش ارزشمند باور داشته باشد، تمایل بیشتری برای سرمایه‌گذاری روی تعامل و جذب دانش ضمنی خواهد داشت و در حد زیاد نیز قادر به جذب چنین دانشی خواهد بود. فرضیه دوم نیز تائید گردید؛ اعتقاد به سودمندی نیز با سطح معنی‌داری ($p<0.01$) با جذب دانش رابطه مثبت دارد. این یافته مطابق با این انتظار است که افراد به دنبال جذب دانش هستند، اما نه به خاطر خودشان بلکه برای تقویت کارایی و اثربخشی در ایجاد امنیت سایبری خود. فرضیه سوم مورد تائید قرار نگرفت؛ باور به پاداش، ارتباط معنی‌داری با جذب دانش ندارد. برخلاف یافته‌های مربوط به فرضیه اول و دوم، این یافته نشان می‌دهد که تصمیم فرد برای شرکت در فرایند انتقال دانش، در درجه اول ناشی از انگیزه ذاتی وی است. شاید این یافته ناشی از این واقعیت باشد که ونگ و هو[1] (۲۰۱۵) معیار باور به پاداش را درزمینهٔ به اشتراک‌گذاری و جذب اطلاعات عادی و غیرمحرمانه مطرح کرده‌اند و این بدان معنی است که در وضعیت و شرایط محرمانه برای جذب دانش، ممکن است انگیزه‌های ذاتی یا درونی بر انگیزه‌های بیرونی پیشی بگیرند. فرضیه چهارم هم تائید شد. اعتقاد به تبادل متقابل به میزان زیاد با جذب دانش رابطه مثبت دارد ($p<0.01$) . این یافته مطابق با انتظارات نظری این پژوهش است که معتقد است «جذب دانش درنهایت نتیجه تعامل متقابل انسانی است». اگرچه کلیه متغیرهای کنترل و متغیرهای مجازی یا ساختگی دارای واریانس هستند، اما سطح معنی‌داری یکی از آن‌ها ($p<0.05$) است. یافته‌های پژوهش نشان می‌دهد که جذب دانش با موقعیت شغلی فرد، تجربه به اشتراک‌گذاری قبلی اطلاعات، اندازه سازمان، کیفیت روابط همسالان، مشارکت بالقوه فردی، جنسیت فرد، سن، سطح

1. *Wang and Hou*

تحصیلات، وابستگی به صنعت و مدت فعالیت در سازمان، رابطه معنی‌دار ندارد. البته نبود این رابطه نه‌تنها نگرانی در مورد ناهمگونی بررسی‌نشده در بین پاسخ‌دهندگان را کاهش می‌دهد، بلکه از طرف دیگر، بی‌اهمیت بودن متغیر مجازی صنعت نیز نگرانی در مورد نمایندگی بیش‌ازحد یک صنعت خاص یا شرکت را در میان پاسخ‌ها کاهش می‌دهد. یکی از موارد مهم دیگر در یافته‌های این پژوهش، مشارکت در رویدادهای قبلی (مانند جلسات گروهی، اجلاس‌ها و مذاکرات خاص صنعت) است که با جذب دانش رابطه معنی‌دار دارد. این یافته نشان می‌دهد که جذب دانش با گذشت زمان روند تکاملی پیدا می‌کند؛ چراکه افراد در چنین وقایعی روابط اجتماعی برقرار می‌کنند.

جدول ۵: نتایج تخمین مدل (رگرسیون پروبیت ترتیبی)

جذب دانش		
سازه‌ها	ضریب	خطای استاندارد قوی
باور به منبع دانش	۰.٤۲۵۶*	۰.۱۶۹۵
باور به مفید بودن دانش	۰.٤۱۶۷**	۰.۱۶۰۱
باور به پاداش	۰.۰۹۷۳	۰.۱۲۰۳
باور به تبادل متقابل متغیرهای کنترل	۰.٤۰۱۲**	۰.۱۵۲۵
موقعیت در سازمان	−۰.۰۷۶۹	۰.۰۵۶۷
تجارب قبلی در مورد اشتراک‌گذاری	−۰.۱۲۸۵	۰.۰۹۳٤
اندازه سازمان	۰.۰٤۱۲	۰.۰۹۱۶
مشارکت در رویدادهای قبلی	۰.٤۲۶۷*	۰.۲۰۰۰
کیفیت روابط با همکاران	۰.۳۰۶۶	۰.۱۷۰۶
مشارکت فردی بالقوه	−۰.۰۳۷۷	۰.۱۰۰۹
جنسیت	۰.٤۹۵۵	۰.۳۳۸۸
سن (۳۰-۲۱)	۰.۰۱۱۶	۰.٤۲۳۰
سن (۴۰-۳۱)	−۰.۳۳۹۲	۰.۲۳۸۶
سن (۵۰-۴۱)	−۰.۳۵۹۵	۰.۲۰۶۰
تحصیلات (هیچ‌کدام)	−۰.۲٤۱۶	۰.٤۳۵٤
تحصیلات (فوق‌لیسانس)	−۰.۰۱۵۳	۰.٤۲۰۷
تحصیلات (لیسانس)	−۰.۱۳۵۰	۰.٤۰۰۳
تحصیلات (دکترا)	−۰.٤۳۳۹	۰.٤۷۰۰

جذب دانش		
سازه‌ها	ضریب	خطای استاندارد قوی
مدت عضویت	−۰.۰۱۳۰	۰.۰۱۹۶
آموزش	۰.۵۸۶۲	۰.۳۶۹۳
بانکداری و مالی	۰.۵٤۷٤	۰.۳٤۸۶
سایر	۰.۵۱۶۰	۰.۳۶۳۶
انرژی	۰.۵۷۱۷	۰.۳۹۰۰
بهداشت	۰.٤۹۸۱	۰.٤۳۶۲
Log pseudolikelihood	−۲۰٤.۲۳	
Pseudo R^2	۰.۱۳۸۵	
Wald χ^2 (24 *d.f.*)	۸۳.۹۵	
$p>\chi^2$	۰.۰۰۰***	
$*p < ۰.۰۵; **p < ۰.۰۱; ***p < ۰.۰۰۱.$		

نتیجه‌گیری

ایجاد امنیت سایبری در سازمان با میزان توانمندی اعضای آن، یعنی انسان‌ها، در جذب دانش ضمنی موردنیاز برای ایجاد امنیت سایبری ارتباط دارد. با طرح این استدلال در چارچوب دیدگاه دانش‌بنیان شرکت و هزینه تعامل، نشان داده شد که باور انسانی با میزان جذب دانش در ارتباط است. قبل از این پژوهش، برخی محققین تعامل انسان در بستر امنیت سایبری را تقریباً و منحصراً در محیط‌های عمومی و عادی بررسی کرده بودند؛ اما در این مطالعه، ادبیات تجربی با تمرکز بر انتقال دانش ضمنی در محیط طبقه‌بندی‌شده، توسعه یافت و ثابت شد که این موضوع با هر دو نوعِ دانش موردنیاز برای ایجاد امنیت سایبری و کانال‌های انتقال که به‌وسیله آن‌ها این دانش حساس و طبقه‌بندی‌شده به‌اشتراک گذاشته می‌شود، مطابقت نزدیک دارد.

این تحقیق با اثبات این‌که امنیت سایبری فقط یک مسئله فنی نیست، سعی در کمک به گسترش ادبیات درزمینهٔ اقتصاد امنیت اطلاعات دارد. با این‌که راه‌حل‌های فناورانه زیادی در مورد امنیت سایبری ارائه شده‌اند، اما تعداد کمی از آن‌ها به موفقیت رسیده و یا می‌رسند؛ مگر این‌که چشم‌انداز اقتصادی مناسبی اتخاذ کنند (اندرسون و مور[1]، ۲۰۰۶). این مطالعه، این گزاره را که «آن دسته از رویکردهای بین‌رشته‌ای که هنگام بررسی امنیت سایبری سعی در ادغام تفکر اقتصادی و روانشناسی دارند، مفیدند» را تقویت می‌کند (اندرسون و مور، ۲۰۰۶؛ فرنل و کلارک[2]، ۲۰۱۲). به همین دلیل، ازنظر ما درک صحیح باورها و

1. *Anderson & Moore*
2. *Furnell & Clarke*

رفتارهای ذهنی انسان‌ها می‌تواند تجزیه‌وتحلیل داده‌های عینی مانند فایل‌های سوابق را تکمیل کند. استدلال ما این است که انسان‌ها قبل از انجام هرگونه فعالیتی، هزینه‌های مبادله را در جذب دانش در نظر می‌گیرند؛ بنابراین، این تصور که انسان‌ها «ابزارهای خنثی» هستند که فقط برای تولید کالای عمومی یا رفاه اجتماعی کار می‌کنند غیرمنطقی است (گوردون[1] و همکاران، ۲۰۱۵). ازاین‌رو، این مطالعه به رفع این پارادوکس که انسان‌ها علی‌رغم اینکه می‌دانند جذب دانشِ مربوط به امنیت سایبری توسط دیگران منجر به ایجاد امنیت سایبری فردی و جمعی می‌شود، غالباً مایل به ارائه این دانش نیستند، کمک می‌کند (آژانس امنیت شبکه و اطلاعات اتحادیه اروپا، ۲۰۱۸).

پیشنهاد ما این است که در تحقیقات آتی میزان جذب دانش مؤثر درنتیجه فرایند تصمیم‌گیری چندمرحله‌ای تفسیر شود. یافته‌های ما نشان می‌دهد که افراد ابتدا هزینه تبادل اجتماعی را که مقدم بر جذب دانش (باور به منابع) است، برآورد می‌نمایند؛ اگر این برآورد مثبت باشد، تعامل اجتماعی را آغاز و برخی عناصر اولیه دانش را جذب و میزان تأثیر آن‌ها بر وظایف شغلی خود (باور مفید بودن) را ارزیابی می‌کنند؛ هنگامی که باور پیدا کردند، احتمالاً به‌منظور تسهیل در جذب بیشتر دانش، رفتارها اجتماعی خود را تطبیق می‌دهند؛ یعنی برای حفظ روند تبادل (باور به تبادل متقابل) دست به اقدام متقابل می‌زنند. درنتیجه، همکاری و اشتراک‌گذاری دانش پایدار می‌شود.

توصیه دیگر به پژوهشگران این است که این مطالعه را در سطح سازمانی انجام داده و به مطالعه و تجزیه‌وتحلیل این‌که چگونه و چرا دانش ضمنی جذب‌شده به‌صورت فردی، به ایجاد امنیت سایبری در سطح سازمانی کمک کند، بپردازند. امروزه، ریزسازه‌های فرایندهای سازمانی که به‌وسیله آن‌ها دانش ضمنی (به‌صورت فردی) موردنیاز امنیت سایبری به‌دست‌آمده و با سایر دارایی‌های دانشی و منابع مادی مؤثر در امنیت سایبری واقعی ترکیب می‌شوند تا حد زیادی ناشناخته‌اند. تحقیقات آینده ممکن است سامان‌دهی منابع و روند ترکیب این دارایی‌ها را موردمطالعه قرار دهند تا شکاف پژوهشی بین جذب دانش فردی و امنیت سایبری در سطح سازمانی را پر نمایند.

اگرچه بسیاری از سازمان‌ها برای تشویق کارمندان خود برای به اشتراک‌گذاری اطلاعات با دیگران، سامانه پاداش ایجاد کرده‌اند (بارتول و سیرواستاوا[2]، ۲۰۰۲)، اما این فرضیه که جذب دانش با «باور به پاداش» ارتباط دارد، تأیید نشد؛ بنابراین، همسویی بین اهداف (منافع) فردی و سازمانی با وعده پاداش‌های پولی و شغلی، حاصل نمی‌شود. ازاین‌رو، مدیران باید از طریق تسهیل تبادل اجتماعی، کمک به برقراری روابط طولانی‌مدت انسانی و تأکید بر سودمندی جذب دانش در موفقیت شغلی فرد، تمهیداتی را برای کاهش هزینه‌های تعامل فراهم کنند.

1. *Gordon*
2. *Bartol & Srivastava*

منابع

- افجه، سید علی‌اکبر؛ انتظاری، اردشیر؛ مرتجی، نجمه سادات، ۱۳۹۴، **الگوی رفتار اشتراک دانش در شبکه اجتماعی**، فصلنامه علوم اجتماعی، دوره ۲۵، شماره ۷۱.
- افضلی، رسول و قالیباف، محمدباقر، **۱۳۹۲ تبیین تحولات مفهوم مرز در فضای سیاسی مجازی**، پژوهش‌های جغرافیای انسانی، دوره ۴۵، شماره ۱، بهار، صص ۲۳۸-۲۱۷.
- انتظاری، اردشیر؛ امیری، مقصود؛ مرتجی، نجمه سادات، ۱۳۹۵، **ارائه الگوی رفتار اشتراک دانش متخصصان ایرانی در فضای مجازی**، فصلنامه مطالعات رسانه‌های نوین، سال دوم، شماره ۵.
- ترابی، قاسم، ۱۳۹۸، **ضرورت‌ها و الزامات تدوین راهبرد سایبری کارآمد**، فصلنامه مطالعات راهبردی، سال بیست و دوم، شماره سوم پاییز، شماره مسلسل ۱.
- جهان بزرگی، احمد، ۱۳۸۸، **امنیت در نظام سیاسی اسلام**، انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.
- رحمدل، ناصر، ۱۳۹۶، **دانش باارزش (حفظ دانش و تجربه کارکنان سازمان)**، انتشارات موسسه آموزشی و تحقیقاتی دفاعی.
- رحمدل، ناصر، ۱۳۹۸، **مدیریت دانش (پیشینه، فرایندها، مدل‌ها و استراتژی‌ها)**، انتشارات نوشناخت.
- قوچانی خراسانی، محمدمهدی، حسین‌پور، داود،۱۳۹۶، «**حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری**». مجله علمی پژوهشی فرایند مدیریت و توسعه: دوره ۳۰، بهار ۹۶، شماره ۱، پیاپی ۹۹.
- کیان خواه احسان، ۱۳۸۹، **مدیریت امنیت اطلاعات**، انتشارات ناقوس.
- نظافتی نوید؛ عظیمی، غلامرضا؛ توکلی، نرجس، ۱۳۹۴، **تبیین و ارزیابی الگوی ارتقاء اشتراک دانش در انجمن‌های خبرگی**، فصلنامه علمی پژوهشی مطالعات مدیریت راهبردی.

- *ENISA* (2018). ***INformation Sharing and Analysis Centres (ISACs): Cooperative models***.*Attiki, Greece: European Union Agency for Network Information Security.*
- *Xiong, Li, & Liu, Liang* (2004). ***Peertrust: Supporting reputation-based trust for peer-topeer electronic communities***. *IEEE Transactions on Knowledge and Data Engineering,16(7), 843–857*
- *Tounsi, Wiem, & Rais, Helmi* (2018). ***A survey on technical threat intelligence in the age of sophisticated cyber attacks***. *Computers & Security, 72.*
- *Bock, Geea W., & Kim, Young-Gul* (2002). ***Breaking the myths of rewards: An exploratory study of attitudes about knowledge sharing***. *Information Resources Management Journal (IRMJ), 15(2), 14–21.*
- *Nickerson, Jack A., & Zenger, Todda R.* (2004). ***A knowledge-based theory of the***

firm - the problem-solving perspective. *Organization Science*, 15(6), 617–632.

- *Nonaka, Ikujiro., & Takeuchi, Hirotaka (1995).* ***The knowledge-creating company: How Japanese companies create the dynamics of innovation (first ed.)***. *New York, USA: Oxford University Press, ISBN: 978-0-19-509269-1.*
- *Grant, R. M. (1996a).* ***Prospering in dynamically-competitive environments: Organizational capability as knowledge integration.*** *Organization Science, 7(4), 359–467*
- *Schilling, Melissa A. (2010).* ***Strategic management of technological innovation (third ed.)***. *New York, USA: McGraw-Hill Education, ISBN: 978-0-07-128957-3.*
- *Williamson, Olivera E. (1981).* ***The economics of organization: The transaction cost approach.*** *American Journal of Sociology, 87(3), 548–577.*
- *Wang, Sheng, & Noe, Raymond A. (2010).* ***Knowledge sharing: a review and directions for future research.*** *Human Resource Management Review, 20(2), 115–131.*
- *Zibak, Adam, & Simpson, Andrew (2019).* ***Cyber threat information sharing: Perceived benefits and barriers.*** *In Proceedings of the 14th international conference on availability, reliability and security (p. 85). ACM.*
- *Yan, Zhijun, et al. (2016).* ***Knowledge sharing in online health communities: a social exchange theory perspective.*** *Information & Management, 53(5), 643–653.*
- *Fielder, Andrew, et al. (2014).* ***Game theory meets information security management.*** *In Nora Cuppens-Boulahia, et al. (Eds.), ICT systems security and privacy protection, IFIP international information security conference, Vol. 428 (pp. 15–29). Berlin, Heidelberg, Germany: Springer.*
- *Maillart, Thomas, et al. (2017).* ***Given enough eyeballs, all bugs are shallow? Revisiting eric raymond with bug bounty programs.*** *Journal of Cybersecurity, 3(2), 81–90*
- *March, James G. (1991).* ***Exploration and exploitation in organizational learning***. *Organization Science, 2(1), 71–87.*
- *Laube, Stefan, & Böhme, Rainer (2017).* ***Strategic aspects of cyber risk information***

sharing. *ACM Computing Surveys* (CSUR), 50(5), 77

- *Feledi, Daniel, Fenz, Stefan, & Lechner, Lukas* (2013). ***Toward web-based information security knowledge sharing.*** *Information Security Technical Report, [ISSN: 1363-4127] 17*(4), 199–209
- *Gal-Or, Esther, & Ghose, Anindya* (2005). ***The economic incentives for sharing security information.*** *Information Systems Research*, 16.
- *Park, Byunga Il* (2011). ***Knowledge transfer capacity of multinational enterprises and technology acquisition in international joint ventures.*** *International Business Review*, 20(1), 75–87.
- *Safa, Nadera Sohrabi, & Von Solms, Rossouw* (2016). ***An information security knowledge-sharing model in organizations.*** *Computers in Human Behavior*, 57, 442–451
- *Simon, Herbert A.* (1991). ***Bounded rationality and organizational learning.*** *Organization Science*, 2(1), 125–134.
- *Solms, Rossouw von, & Niekerk, Johan van* (2013). ***From information security to cyber security.*** *Computers & Security*, 38, 97–102.
- *Casas, Pedro, et al.* (2017). ***Network security and anomaly detection with big-dama, a big data analytics framework.*** *In IEEE 6th international conference on cloud networking (pp. 1–7). IEEE*
- *Lee, Jay., Bagheri, B., & Kao, Hung-An* (2015). ***A cyber-physical systems architecture for industry 4.0-based manufacturing systems.*** *Manufacturing Letters*, 3(5), 18–23.
- *Hofmann, Annette, & Ramaj, Hidajet* (2011). ***Interdependent risk networks: the threat of cyber attack.*** *International Journal of Management and Decision Making, 11*(5), 312–323
- *Ben-Asher, Noam, & Gonzalez, Cleotilde* (2015). ***Effects of cyber security knowledge on attack detection.*** *Computers in Human Behavior*, 48.
- *Singh, Kavita* (2005). ***Organisation change and development.*** *New Delhi, India: Excel Books*, ISBN: 978-81-7446-442-2.

- ENISA (2018). **INformation Sharing and Analysis Centres (ISACs): Cooperative models.** Attiki, Greece: European Union Agency for Network Information Security.
- Encinosa, William E., Gaynor, Martin, & Rebitzer, James B. (2007). **The sociology of groups and the economics of incentives: Theory and evidence on compensation systems.** Journal of Economic Behaviour and Organization, 62(2), 187–214.
- Davenport, Thomas H., & Glaser, John (2002). **Just-in-time delivery comes to knowledge management.** Harvard Business Review, 80(.
- Nagin, Daniel S., et al. (2002). **Monitoring, motivation, and management: The determinants of opportunistic behavior in a field experiment.** American Economic Review, 92(4), 850–873.
- Lichtenthaler, Ulrich, & Ernst, Holger (2007). **Developing reputation to overcome the imperfections in the markets for knowledge.** Research Policy, 36(1), 37–55.
- Foss, N. J. (1996). **More critical comments on knowledge-based theories of the firm.** Organization Science, 7(5), 519–523.
- Luiijf, Eric, & Klaver, Marieke (2015). **On the sharing of cyber security information.** In Critical infrastructure protection IX: 466, International conference on critical infrastructure protection, Vol. 466 (pp. 29–46).
- Gabaix, Xavier, et al. (2006). **Costly information acquisition: Experimental analysis of a boundedly rational model.** American Economic Review, 96(4), 1043–1068.
- Bosch, Frans A. J. van den, Volberda, Henk W, & Boer, Michiel de (1999). **Coevolution of firm absorptive capacity and knowledge environment: Organizational forms and combinative capabilities.** Organization Science, 10(5), 551–568.
- Cai, Shun, et al. (2013). **Knowledge sharing in collaborative supply chains: Twin effects of trust and power.** International Journal of Productions Research, 51(7), 2060–2076 Nunnally, Jum C., & Bernstein, Ira H. (2017). McGraw-hill series in psychology, Psychometric theory (third ed.). New York, USA: McGraw-Hill, ISBN: 978-0-07-047849-7
- Mermoud, Alain, et al. (2019). **To share or not to share: A behavioral perspective**

on human participation in security information sharing. *Journal of Cybersecurity*, 5(1).

- *Kolm, Serge-Christophe, & Mercier-Ythier, Jean (Eds.), (2006).* ***Handbook of the economics of giving,*** *altruism and reciprocity, Vol. 1.*
- *Tricomi, Elisabeth, et al. (2010).* ***Neural evidence for inequality-averse social preferences.*** *Nature, 463(7284), 1089–1091.*
- *Xiong, Li, & Liu, Liang (2004).* ***Peertrust: Supporting reputation-based trust for peer-topeer electronic communities.*** *IEEE Transactions on Knowledge and Data Engineering, 16(7), 843–857.*
- *Bartol, Kathryn M., & Srivastava, Abhishek (2002).* ***Encouraging knowledge sharing: The role of organizational reward systems.*** *Journal of Leadership & Organizational Studies, 9(1), 64–76.*
- *Anderson, Ross, & Fuloria, Shailendra (2010).* ***Security economics and critical national infrastructure.*** *In Tyle Moore, David Pym, & Christos Ioannidis (Eds.), Economics of information security and privacy (pp. 55–66). Springer, ISBN: 978-1-4419-6967-5.*
- *Furnell, Steven, & Clarke, Nathan (2012).* ***Power to the people? The evolving recognition of human aspects of security.*** *Computers & Security, 31(8), 983–988.*
- *Gordon, Lawrence A., Loeb, Martin P., Lucyshyn, William, & Zhou, Lei (2015).* ***Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model.*** *Journal of Information Security, 6(1), 24–30.*
- *Wang, Wei-Tsong, & Hou, Ya-Pei (2015).* ***Motivations of employees' knowledge sharing behaviors: A self-determination perspective****. Information and Organization, 25(1), 1–26.*
- *Reinholt, Mia, Pedersen, Torben, & Foss, Nicolai J. (2011).* ***Why a central network position isn't enough: The role of motivation and ability for knowledge sharing in employee networks.*** *Academy of Management Journal, 54(6), 1277–1297*
- *Podsakoff, Philip M., & Organ, Dennis W. (1986).* ***Self-reports in organizational***

research: Problems and prospects. *Journal of Management*, 12.

- *Hair, J. F. (2006).* ***Multivariate data analysis****, Vol. 1 (fifth ed.). Taramani, India: Pearson Education India.*
- *Lee, Cheia Sian, & Ma, Long (2012).* ***News sharing in social media: The effect of gratifications and prior experience.*** *Computers in Human Behavior, 28(2), 331–339.*