بررسی عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان

فصلنامه علمی- پژوهشی

مدیریت اطلاعات

دوره ۲، شماره ۵

زمستان ۹۵

سیدمحمدباقر جعفری*[1]

استادیار دانشگاه تهران

علی حمیدی‌زاده

استادیار دانشگاه تهران

راضیه منتظری‌نجف‌آبادی

کارشناس ارشدسیستم‌ها دانشگاه تهران

چکیده: با توجه به گسترش روزافزون به‌کارگیری سیستم‌های اطلاعاتی در سازمان‌ها و الکترونیکی شدن قسمت اعظم اطلاعات سازمان‌ها، خطرات مربوط به امنیت اطلاعات چالش بزرگی برای بسیاری از سازمان‌ها است. این خطرات ممکن است عواقب وخیمی ازجمله، از دست دادن اعتبار سازمان و آسیب‌های مالی سنگین در پی داشته باشد. آمارها نشان می‌دهند آسیب‌های امنیتی سیستم‌های اطلاعاتی در حال افزایش است. بسیاری از سازمان‌ها کارکنان خود را ضعیف‌ترین حلقه در امنیت اطلاعات در نظر می‌گیرند، اما همین کارکنان می‌توانند سرمایه‌های بزرگی در تلاش برای کاهش خطر امنیت سیستم‌های اطلاعاتی باشند. بررسی پژوهش‌های پیشین نشان از عدم توجه کافی به موضوع امنیت سیستم‌های اطلاعاتی از جنبه انسانی آن در ایران دارد. ازاین‌رو هدف از پژوهش حاضر بررسی عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان است. به‌منظور شناسایی این عوامل مدل پژوهش بر پایه مدل بالگارکیو که بر مبنای نظریه رفتار برنامه‌ریزی‌شده در زمینه امنیت سیستم‌های اطلاعاتی است، توسعه‌یافته و مورد آزمون قرار گرفت. بدین منظور ۲۲۱ نفر (شامل کارکنان ۵ سازمان مختلف) به روش نسبتی انتخاب و مورد پرسش واقع شدند. پس از جمع‌آوری داده‌ها، فرضیه‌ها از طریق مدل یابی معادلات ساختاری مورد تجزیه‌وتحلیل قرار گرفتند. نتایج نشان داد خودکارآمدی برای پیروی و نگرش نسبت به پیروی بر تمایل به پیروی از سیاست‌های امنیت اطلاعات تأثیر دارد که نگرش نسبت به پیروی دراین‌بین بیشترین تأثیر را دارد.

کلیدواژه‌ها: *آگاهی از امنیت اطلاعات، امنیت اطلاعات، سیستم‌های اطلاعاتی، سیاست امنیت اطلاعات، پیروی.*

[1] sm.jafari@ut.ac.ir(نویسنده مسئول)

مقدمه

امنیت اطلاعات مسئله‌ای حیاتی برای سازمان‌ها در سراسر جهان در عصر حاضر است. امنیت سیستم‌های اطلاعاتی شامل دو بعد فناوری و افراد (عوامل انسانی) می‌شود. بررسی‌ها نشان می‌دهد در بیشتر پژوهش‌هایی که در زمینه امنیت سیستم‌های اطلاعاتی صورت گرفته؛ یک نوع دید و رویکرد فنی وجود داشته است (الهی و همکاران، ۱۳۸۸: ۱). امروزه سازمان‌ها توافق دارند که یکی از اولویت‌های مدیران عالی، افزایش امنیت منابع فناوری و اطلاعات است (رانزباسم و میترا[1]، ۲۰۰۹). ازآنجاکه راه‌حل‌های مبتنی بر فناوری نشان داده‌اند که می‌توانند به بهبود امنیت اطلاعات کمک کنند، بنابراین معمولاً سازمان‌ها برای مقابله با چالش امنیت سیستم‌های اطلاعاتی کار را با راه‌حل‌های فنی آغاز می‌کنند. علی‌رغم این واقعیت که سازمان‌ها به‌طور فزاینده‌ای در حال سرمایه‌گذاری در راه‌حل‌های مبتنی بر فناوری هستند، اما شواهد نشان می‌دهد که حوادث مربوط به امنیت اطلاعات هنوز در حال افزایش است؛ بنابراین رشد حوادث امنیتی حاکی است که افزایش امنیت اطلاعات صرفاً با سرمایه‌گذاری در منابع سازمانی و فردی و منابع فناوری به دست نخواهد آمد (بالگارکیو و همکاران[2]، ۲۰۱۰b: ۱).

با توجه به جدید بودن حوزه امنیت اطلاعات، به نظر می‌رسد بحث امنیت سیستم‌های اطلاعاتی در ایران چندان موردتوجه قرار نگرفته و در عمل سازمان‌های محدودی هستند که زیرساخت‌های لازم را برای تأمین امنیت سیستم‌های اطلاعاتی در سازمان خود فراهم آورده‌اند؛ بنابراین، حفاظت از منابع اطلاعاتی سازمان هم در زمینه سیستم‌های اطلاعاتی وهم در مورد اعضای سازمان امری بسیار حیاتی و ضروری است. امنیت سیستم‌های اطلاعاتی هم فناوری و هم عوامل انسانی را شامل می‌شود (الهی و همکاران، ۱۳۸۸: ۲).

بسیاری از نقض امنیت اطلاعات در محل کار، ناشی از عدم پیروی کارکنان از سیاست‌های امنیت اطلاعات در سازمان است. بررسی‌های اخیر نشان می‌دهند که ۷۸ درصد از حملات کامپیوتری به شکل ویروس‌های جاسازی‌شده در پیوست ایمیل‌ها ظاهر می‌شوند (چان و همکاران[3]، ۲۰۰۵: ۳). بر اساس پژوهش‌های مؤسسه استراتژی و پژوهش جاولین[4] در سال ۲۰۰۵، ۹ میلیون آمریکایی قربانی سرقت هویت شده‌اند و درمجموع ۵۵۶ میلیارد دلار زیان‌دیده‌اند. همچنین آمار نشان می‌دهد که تعداد قربانیان سرقت هویت در ایالات‌متحده ۱۲ درصد در سال ۲۰۰۹ افزایش‌یافته است (بانگ و همکاران[5]، ۲۰۱۲). سازمان ملل متحد (2005, p. xxiii) گزارش داده است که «ده‌ها، نه صدها میلیارد دلار» از آسیب‌های سالانه اقتصادی در سراسر جهان ناشی از به خطر انداخته شدن امنیت اطلاعات است (دارسی و همکاران[6]، ۲۰۰۹: ۱). در ایران آمار دقیقی از خسارت‌های وارده به سیستم‌های اطلاعاتی سازمان‌ها و درصد

---

[1] Ransbotham & Mitra
[2] Bulgurcu et al
[3] Chan et al
[4] Javelin Strategy & Research
[5] Bang et al
[6] D'Arcy et al

آلودگی این سیستم‌ها در دسترس نیست؛ اما برای نمونه بر اساس اطلاعاتی که شرکت «سایمنتک» منتشر کرده است در حدود ۶۰ درصد از سیستم‌های رایانه‌ای که به ویروس خطرناک استاکس نت (Stuxnet) آلوده‌شده‌اند در ایران قرار دارند. این وضعیت نشان می‌دهد سازمان‌های ایرانی شدیداً نیازمند تأمین امنیت سیستم‌های اطلاعاتی خود هستند (جهان نیوز، ۱۳۹۳). به همین دلیل سازمان‌ها اسناد سیاست‌های امنیت اطلاعات را برای ارائه دستورالعمل‌هایی به کارکنان مبنی بر این‌که آن‌ها باید برای دست‌یابی به امنیت اطلاعات چه‌کارهایی را انجام دهند و چه مسئولیت‌هایی در این راستا دارند را ایجاد کرده‌اند؛ بنابراین درک رفتار پیروی کارکنان برای سازمان‌ها بسیار حیاتی است (بالگارکیو و همکاران،b۲۰۱۰).

درنتیجه مسئله پژوهش حاضر شناسایی و بررسی عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان است. بدین منظور مدل پژوهش با نظرخواهی از خبرگان و پس از ترکیب و تعدیل مدل بالگارکیو و همکاران (a۲۰۱۰) و (b۲۰۱۰) و مدل بالگارکیو و همکاران (۲۰۰۹) ارائه‌شده است.

چارچوب نظری پژوهش

مروری بر نظریه‌های بررسی‌کننده عوامل تأثیرگذار بر رفتار انسان‌ها

نظریه عمل منطقی

نظریه عمل منطقی[1] تمایل فرد برای انجام رفتار را پیش‌بینی می‌کند. نظریه عمل منطقی بر این پندار است که رفتار فرد با تمایل رفتاری او تعیین می‌شود و به‌عبارت‌دیگر تمایل رفتاری، رفتار را پیش‌بینی می‌کند. تمایل رفتاری نیز تابع دو عامل است؛ نگرش نسبت به رفتار و هنجارهای ذهنی (مادن و همکاران،[2] ۱۹۹۲). تمایل رفتاری برای انجام یک رفتار (در اینجا پیروی از سیاست‌های امنیت سیستم-های اطلاعاتی)، به‌صورت مشترک به‌وسیله نگرش شخص نسبت به پیروی و هنجارهای ذهنی در مورد رفتار تعیین می‌شود.

نظریه رفتار برنامه‌ریزی‌شده

نظریه رفتار برنامه‌ریزی‌شده[3] وقوع یک رفتار ویژه را پیش‌بینی می‌کند؛ مشروط بر این‌که فرد تمایل انجام آن را داشته باشد. طبق این مدل، تمایل انجام یک رفتار توسط سه عامل نگرش نسبت به رفتار، هنجارهای ذهنی و کنترل رفتاری درک شده، پیش‌بینی می‌شود.

---

[1] Theory of Reasoned Action (TRA)

[2] Madden et al

[3] Theory of Planned Behavior (TPB)

نگرش نسبت به رفتار[1]ارزشیابی مثبت یا منفی در مورد انجام یک رفتار است که از دو زیر سازه باورهای رفتاری و ارزیابی نتایج رفتار که باعث حصول نگرش نسبت به رفتار می‌شود، تشکیل‌شده است (شارما،[2] ۲۰۱۰).

هنجارهای ذهنی[3]به فشار اجتماعی درک شده توسط افراد برای انجام یا عدم انجام رفتار اشاره دارد. افراد غالباً بر مبنای ادراکشان از تصور دیگران، عمل می‌کنند و تمایل آن‌ها برای پذیرش رفتار، متأثر از افرادی است که ارتباطات نزدیکی با آن‌ها دارند. در این نظریه هنجار ذهنی فرد، حاصل‌ضرب باورهای هنجاری در انگیزه پیروی برای انجام رفتار باوجوداین انتظارات است (براتی و همکاران، ۱۳۹۰).

کنترل رفتاری درک شده[4]عبارت است از مقداری از احساس فرد در مورد این‌که عدم انجام یا انجام یک رفتار تا چه حد تحت کنترل ارادی وی است. عوامل کنترل شامل عوامل داخلی و خارجی است. عوامل داخلی مربوط به شخص فرد بوده و شامل مهارت‌ها، توانایی‌ها، اطلاعات و احساسات است و در بررسی عوامل خارجی به عواملی همچون عوامل محیطی یا شغلی اشاره‌شده است (طاووسی و همکاران، ۱۳۸۸).

نظریه انتخاب عقلایی

نظریه انتخاب عقلایی[5] استدلال می‌کند که شخص چگونه با ایجاد تعادل بین هزینه‌ها و مزایای انتخاب‌هایش تصمیم می‌گیرد (مک کارتی،[6] ۲۰۰۲). در تصمیم‌گیری عقلایی، یک فرد ابتدا جایگزین‌های کار را مشخص می‌کند و سپس محتمل‌ترین نتایج هر مرحله از کار را در نظر می‌گیرد (پاترنوستر و پوگارسکی،[7] ۲۰۰۹). ازآنجاکه افراد به نتایج اولویت می‌دهند، هر نتیجه می‌تواند با هزینه یا سود بسته به این‌که چقدر رضایت برای فرد ایجاد می‌کند درک شود (مک کارتی، ۲۰۰۲). طبق نظریه انتخاب عقلایی، زمانی که افراد برای تصمیم‌گیری راه‌های متنوعی دارند که هرکدام از آن‌ها نتایجی را در پی دارد، فرد راهی را انتخاب خواهد کرد که بهترین پیامد را برایش داشته باشد (الفرز و همکاران،[8] ۲۰۰۳).

نظریه مبادله اجتماعی

در نظریه مبادله اجتماعی[9]آمده است روابط کارکنان با رهبرانشان در سازمان‌ها همچون یک دادوستد غیررسمی بر طبق یک قرارداد روانی است. زمانی که سازمان توقعات و انتظارات کارکنان را برآورده سازد،

---

[1] Attitude
[2] Sharma
[3] Subjective Norms
[4] Perceived Behavioral Control (PBC)
[5] Rational Choice Theory (RCT)
[6] McCarthy
[7] Paternoster & Pogarsky
[8] Elffers et al
[9] Social Exchange Theory (SET)

کارکنان نیز انتظارات و توقعات سازمان را برآورده خواهند کرد. اُستراف و باون[1](۲۰۰۰) با تکیه‌بر نظریه مبادله اجتماعی، فرضیه‌هایی در مورد ارتباطات میان رویه‌های مدیریت منابع انسانی، نگرش‌ها و عملکرد ارائه دادند. آن‌ها مطرح کردند که اقدامات منابع انسانی توسط نگرش نیروی کار و آنچه بر انتظارات آن‌ها تأثیر می‌گذارد، شکل می‌گیرد. نگرش‌ها و رفتار کارکنان ادراک و انتظارات کارکنان را منعکس می‌کند.

پیشینه تجربی پژوهش

حسن‌زاده و همکاران (۱۳۹۱) در پژوهشی تحت عنوان «ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران» به ارزیابی آگاهی از امنیت اطلاعات کاربران پرداختند. هدف این پژوهش، ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران است. در این پژوهش همچنین میزان سطح آگاهی از امنیت اطلاعات در سه سطح دانش، نگرش و رفتار مورد ارزیابی قرار گرفت. این پژوهش به لحاظ گردآوری اطلاعات به روش پیمایشی انجام‌گرفته است.

الهی و همکاران (۱۳۸۸) در پژوهشی تحت عنوان «ارائه چارچوبی برای عوامل انسانی مرتبط در امنیت سیستم‌های اطلاعاتی» با در نظر گرفتن اهمیت امنیت، برای سازمان‌های امروزی، یک مدل مدیریتی برای بررسی نقش عوامل انسانی در امنیت سیستم‌های اطلاعاتی ارائه کردند. هدف این پژوهش، به‌طور خاص شناسایی و مدل‌سازی سازه‌های[2] مدیریتی حیاتی و اساسی مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی است.

کیم و همکاران[3](۲۰۱۴) در پژوهشی تحت عنوان «یک مدل یکپارچه رفتاری برای پیروی از سیاست‌های امنیت اطلاعات» عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت اطلاعات را موردبررسی قراردادند. در این پژوهش تأثیر عواملی مانند نگرش، خودکارآمدی، باورهای اصولی و باورها در مورد هزینه‌های پیروی بر تمایل به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی موردبررسی قرار گرفت.

سیپونن و همکاران[4](۲۰۱۴) در پژوهشی تحت عنوان «تبعیت کارکنان از سیاست‌های امنیت اطلاعات: یک مطالعه اکتشافی» عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت اطلاعات را موردبررسی قراردادند. آن‌ها یک نظریه جدید ارائه دادند که تبعیت کارکنان از سیاست‌های امنیت اطلاعات را توضیح می‌دهد. در توسعه این مدل از نظریه‌هایی چون نظریه حمایت انگیزش، نظریه عمل منطقی و نظریه ارزیابی شناختی استفاده‌شده است. در این پژوهش هفت عامل که بر تمایل به پیروی از سیاست‌های امنیت اطلاعات تأثیرگذار هستند موردبررسی قرارگرفته است.

---

[1] Ostroff & Bowen
[2] Constructs
[3] Kim & et al
[4] Siponen & et al

کاجتازی و بالگارکیو[1](۲۰۱۳) در مقاله‌ای تحت عنوان «پیروی از سیاست‌های امنیت اطلاعات: یک مطالعه تجربی برافزایش تعهد» به بررسی عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت اطلاعات در سازمان پرداختند. هدف این پژوهش تسهیل فهم نگرش کارکنان نسبت به پیروی از سیاست‌های امنیت اطلاعات از طریق افزایش تعهد آن‌ها است. در این پژوهش سه عامل موانع کاری، عدم تقارن اطلاعات و ایمنی منابع نقش میانجی را در توضیح نگرش نسبت به پیروی دارند. در این پژوهش آگاهی از امنیت اطلاعات به‌عنوان یک متغیر مستقل از طریق متغیرهای میانجی تأثیر غیرمستقیم بر نگرش دارد.

در پژوهشی دیگر از ونس و همکاران[2](۲۰۱۲) تحت عنوان «ترغیب به پیروی از امنیت سیستم‌های اطلاعاتی: بینشی از عادت و نظریه انگیزه حمایت» عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان موردبررسی قرار گرفت. در این پژوهش با استفاده از نظریه انگیزه حمایت تأثیر متغیرهای مختلف ازجمله خودکارآمدی بر تمایل به پیروی از سیاست‌های امنیت اطلاعات موردبررسی قرار گرفت.

بالگارکیو و همکاران (۲۰۱۰a) در پژوهشی تحت عنوان «پیروی از سیاست‌های امنیت اطلاعات: یک مطالعه موردی از باورهای مبتنی بر عقلانیت و آگاهی از امنیت اطلاعات» به ارائه مدلی برای پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان پرداختند. هدف از این پژوهش گسترش دانش در مورد پیروی کارکنان از سیاست‌های امنیت اطلاعات به‌وسیله شناسایی عوامل مبتنی بر عقلانیت برگرفته از نظریه انتخاب عقلایی است. در این پژوهش همچنین با استفاده از نظریه رفتار برنامه‌ریزی‌شده مدل پژوهش ارائه‌شده است.

بالگارکیو و همکاران (۲۰۱۰b) در پژوهشی دیگر با عنوان «کیفیت و عدالت سیاست‌های امنیت اطلاعات به‌عنوان نیازی از امنیت کارکنان در محل کار: یک پژوهش تجربی» تأثیر ویژگی‌های سیاست-های امنیت اطلاعات بر پیروی کارکنان از امنیت در محیط کار را بررسی کردند. در این پژوهش دو عامل که برای پیروی از امنیت توسط کارکنان موردنیاز است، پیشنهاد شد. این دو عامل عدالت و کیفیت سیاست‌های امنیت اطلاعات را شامل می‌شود.

هراث و رائو[3](۲۰۰۹) در پژوهشی با عنوان «رفتارهای مشوق امنیت اطلاعات در سازمان: نقش جریمه‌ها، فشارها و اثربخشی درک شده» مدلی نظری مبتنی بر اثرات جریمه‌ها، فشارها و اثربخشی درک شده از رفتار کارکنان را توسعه داده و آزمایش کردند که باعث افزایش پیروی کارکنان از سیاست‌های امنیت اطلاعات می‌گردد.

بالگارکیو و همکاران (۲۰۰۹) در پژوهشی تحت عنوان «نقش آگاهی از امنیت اطلاعات و عدالت درک شده بر پیروی از سیاست‌های امنیت اطلاعات» با استفاده از دو عامل اساسی آگاهی از امنیت اطلاعات و

[1] Kajtazi & Bulgurcu
[2] Vance & et al
[3] Herath & Rao

عدالت به ارائه مدلی برای پیروی کارکنان از سیاست‌های امنیت اطلاعات پرداختند. چارچوب این پژوهش بر اساس نظریه رفتار برنامه‌ریزی‌شده است.

پاهنیلا و همکاران[1](۲۰۰۷) در پژوهشی تحت عنوان «رفتار کارکنان نسبت به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی» با ارائه مدلی شامل عواملی که پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی توسط کارکنان را توضیح می‌دهد، به بررسی این موضوع پرداختند. هدف از این پژوهش پیشنهاد مدلی برای نشان دادن این است که چرا کارکنان در سازمان‌ها از سیاست‌های امنیت سیستم‌های اطلاعاتی پیروی نمی‌کنند و چه عواملی بر پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی مؤثر است.

در این پژوهش دودسته از متغیرها شامل انگیزش‌های خارجی و داخلی بر تمایل به پیروی از سیاست‌های امنیت اطلاعات اثرگذار است. انگیزش‌های خارجی خود به دودسته جریمه‌ها (شامل: شدت جریمه و قطعیت بازرسی) و فشارهای اجتماعی (شامل: باورهای اصولی و رفتار همکاران) تقسیم می‌شود. انگیزه‌های داخلی شامل اثربخشی درک شده می‌باشند.

در پژوهشی چان و همکاران (۲۰۰۵) با عنوان «ادراکات از امنیت اطلاعات در محل کار: ارتباط شرایط امنیت اطلاعات با رفتار پیروی» عوامل اجتماعی مؤثر بر پیروی کارکنان از سیاست‌های امنیت اطلاعات را بررسی کردند. این پژوهش اثر خودکارآمدی بر پیروی از سیاست‌های امنیت اطلاعات را موردبررسی قرار داده است. مدل این پژوهش بر اساس مفاهیم منطبق با ادبیات امنیت توسعه‌یافته است که برای شرح رفتار سالم کارکنان در سازمان استفاده‌شده است. در این پژوهش هم عوامل سازمانی و هم عوامل فردی مؤثر بر پیروی موردبررسی قرارگرفته است. عامل فردی در نظر گرفته‌شده در این پژوهش به نام خودکارآمدی مطابق با پژوهش حاضر است.

توسعه مدل پژوهش

با توجه به‌مرور ادبیات صورت گرفته در زمینه تمایل به پیروی از سیاست‌های امنیت اطلاعات، در این بخش با توجه به مدل بالگارکیو و همکاران (۲۰۱۰a) و (۲۰۱۰b) و با توجه به سایر روابط منطقی استخراج‌شده از پژوهش‌های مشابه در این زمینه به توسعه مدل پژوهش پرداخته می‌شود.

تمایل به پیروی از سیاست‌های امنیت اطلاعات

بالگارکیو و همکاران (۲۰۱۰) ذکر می‌کنند که خط اصلی از پژوهش‌های عوامل انسانی در رابطه با امنیت اطلاعات، پیدا کردن عواملی است که مرتبط با رفتار کارکنان و پیروی آن‌ها از سیاست‌های امنیت اطلاعات در سازمان است. اشتباه‌ها، خطاها، عادات نامناسب و جهل افراد می‌تواند موجب به خطر افتادن

[1] Pahnila & et al

امنیت اطلاعات در سازمان گردد؛ بنابراین باید به این نکته توجه کرد که پیروی کارکنان مهم‌ترین عامل در امنیت سیستم‌های اطلاعاتی در سازمان است.

منظور از تمایل به پیروی از سیاست‌های امنیت اطلاعات، قصد کارکنان برای حفاظت از منابع فناوری و اطلاعات سازمان خویش در برابر نقض بالقوه امنیت است (آجزن،[1] ۱۹۹۱؛ بالگارکیو و همکاران، ۲۰۱۰a؛ فیش‌بن و آجزن،[2] ۱۹۷۵؛ پاهنیلا و همکاران، ۲۰۰۷). طبق نظریه رفتار برنامه‌ریزی‌شده، تمایل به پیروی، باورهایی هستند که با توجه به احتمالات ذهنی فرد نتیجه تأثیر نگرش افراد نسبت به رفتار را نشان می‌دهد.

باورهای اصولی

باورهای اصولی فشار اجتماعی درک شده کارکنان در مورد پیروی از الزامات سیاست‌های امنیت اطلاعات است که ناشی از انتظارات رفتاری است (آجزن، ۱۹۹۱؛ فیش‌بن و آجزن، ۱۹۷۵). باورهای اصولی همان بایدها و نبایدهایی است که رفتار افراد را تحت تأثیر قرار می‌دهد و فرد تصمیم می‌گیرد که رفتاری را انجام دهد یا ندهد (فیش‌بن و وایزر،[3] ۲۰۰۳:۱۶۶). زمانی که فرد قصد انجام کاری را دارد به رفتار دیگران رجوع می‌کند. فرد رفتاری را انجام می‌دهد که اکثر افراد آن را بپذیرند (گلانز و همکاران،[4] ۲۰۰۸).

بنابراین عضویت در یک محیط اجتماعی یا تأثیر افراد مهم ممکن است تأثیر مهمی بر انجام یا عدم انجام رفتار خاصی داشته باشد. با توجه به سیاست‌های امنیت سیستم‌های اطلاعاتی نگرش مثبت مدیران و کارکنان نسبت به پیروی از سیاست‌های امنیتی، ممکن است نگرش افراد را به سمت رفتار مثبت هدایت کند (پاهنیلا و همکاران، ۲۰۰۷).

مطابق با نظریه مبادله اجتماعی فشارهای اجتماعی تأثیر مهمی بر رفتار فرد دارند. به‌عنوان مثال کرپس[5](۱۹۹۷) بیان می‌کند، زمانی که افراد از اخراج یا سرزنش شدن توسط همکاران به دلیل عدم پیروی از سیاست‌های امنیتی بترسند، به سمت پیروی از سیاست‌های امنیتی تحریک می‌شوند. افراد توسط انتظاراتی که از رفتار دیگر افراد مشاهده می‌کنند تحت تأثیر قرار می‌گیرند. اگر کارکنان باور داشته باشند که مدیران، کارکنان و همکاران از فرد انتظار دارند که از سیاست‌های امنیت اطلاعات در سازمان پیروی کند، احتمال بیشتری وجود خواهد داشت که فرد از سیاست‌ها پیروی کند (هراث و رائو، ۲۰۰۹).

تأثیر باورهای اصولی بر تمایل به پیروی

بالگارکیو و همکاران (۲۰۱۰a)، هراث و رائو (۲۰۰۹)، کیم و همکاران (۲۰۱۴)، سیپونن و همکاران (۲۰۱۰) و (۲۰۱۴)، پاهنیلا و همکاران (۲۰۰۷) بر اساس نظریه رفتار برنامه‌ریزی‌شده عنوان کردند که

[1] Ajzen
[2] Fishbein & Ajzen
[3] Fishbein & Yzer
[4] Glanz et al
[5] Kreps

باورهای اصولی بر تمایل به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی تأثیر مثبتی دارد؛ بنابراین فرضیه زیر ارائه‌شده است:

H_1: باورهای اصولی کارکنان تأثیر مثبت و معناداری بر تمایل به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی دارد.

نگرش نسبت به پیروی

نگرش به احساسات مثبت یا منفی فرد نسبت به برخی انگیزه‌های رفتاری اشاره دارد (آجزن، ۱۹۹۱). مطابق با نظر آجزن، نگرش جزئی از عوامل انگیزشی است که بر رفتار تأثیر می‌گذارد و نشان می‌دهد که چگونه مردم برای انجام کارها مشتاق هستند و تلاش می‌کنند (پاهنیلا و همکاران، ۲۰۰۷).

تأثیر نگرش نسبت به پیروی بر تمایل به پیروی

بالگارکیو و همکاران (۲۰۱۰a) و (۲۰۰۹)، فیش‌بن و وایزر (۲۰۰۳)، ایفندو[1](۲۰۱۲) و (۲۰۱۴)، سیپونن و همکاران (۲۰۱۴)، کیم و همکاران (۲۰۱۴)، پاهنیلا و همکاران (۲۰۰۷) و هراث و رائو (۲۰۰۹) بر اساس نظریه رفتار برنامه‌ریزی‌شده بیان کرده‌اند که نگرش نسبت به پیروی بر تمایل به پیروی تأثیر دارد؛ بنابراین فرضیه زیر ارائه‌شده است:

H_2: نگرش نسبت به پیروی تأثیر مثبت و معناداری بر تمایل به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی دارد.

باورها در مورد پیامدهای پیروی

باورها در مورد پیامدهای پیروی از سیاست‌های امنیت اطلاعات به درک منافع پیروی از سیاست‌های امنیت اطلاعات منجر می‌گردد. باورها در مورد پیامدهای پیروی می‌تواند پاداش‌ها (ملموس یا ناملموس) را شامل شود به این صورت که سازمان در ازای پیروی کارکنان از سیاست‌های امنیت اطلاعات، پاداش-هایی را برای کارکنان در نظر می‌گیرد. این پاداش‌ها ممکن است شامل افزایش حقوق، پاداش‌های مالی یا غیرمالی، تقدیر از کارکنان به‌صورت اهدای جوایز و یا ذکر در گزارش‌های ارزیابی به‌صورت شفاهی یا کتبی و همچنین ترفیع درجه شود. پاداش‌ها به‌عنوان سازوکاری مشخص برای تغییر رفتارها در زمینه‌های مختلف ازجمله، آموزش، رفتار سازمانی و روانشناسی موردتوجه قرارگرفته است (بالگارکیو و همکاران، ۲۰۱۰a). در نظر گرفتن پاداش برای کارکنان می‌تواند باعث تقویت رفتار پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان شود؛ بنابراین باورهای رفتاری می‌تواند به ارزیابی احتمال بروز نتایج دلخواه از رفتار منجر شود (آجزن، ۱۹۹۱).

باورها در مورد ارزیابی کلی عواقب عدم پیروی

[1] Ifinedo

طبق ادبیات موجود نگرش کارکنان نسبت به انجام یک رفتار به باورهایش در مورد عواقب مربوط به رفتار مرتبط است (آجزن، ۱۹۹۱؛ فیش‌بن و آجزن، ۱۹۷۵؛ فیش‌بن، ۲۰۰۷). مطابق نظریه تصمیم‌گیری عقلایی، می‌توان فرض کرد که ارزیابی کلی عواقب که منتج به پیروی (عدم پیروی) از سیاست‌ها می‌شود، به‌وسیله ادراک افراد از نتایج بالقوه مرتبط با پیروی و عدم پیروی تحت تأثیر قرار می‌گیرد. نتایج را می‌توان رویدادهایی تعریف کرد که به‌احتمال‌زیاد بعد از انجام (عدم انجام) رفتار پیروی اتفاق خواهد افتاد. ازنظر تولمن[1](۱۹۳۲) افراد انتظاراتی را که نتیجه باورهای مرتبط با بعضی رویدادها است یاد می‌گیرند. باورها در مورد ارزیابی کلی عواقب عدم پیروی مربوط به ارزیابی افراد از مجموع رویدادهای آینده است.

باورها در مورد هزینه‌های پیروی

باورها در مورد هزینه‌های پیروی به‌عنوان ادراک کارکنان از پیروی از سیاست‌های امنیت اطلاعات تعریف‌شده است که منظور از هزینه‌های پیروی اقداماتی وقت‌گیر هستند که مانع پیشرفت کار یا بهره‌وری شخصی فرد می‌شود. ازآنجاکه رفتارهای امنیتی که از کارمندان انتظار می‌رود به زمان و تلاش نیاز دارد، اغلب کارکنان پیروی از سیاست‌های امنیت اطلاعات را مانع پیشرفت کار و بهره‌وری خود می‌دانند (بالگارکیو، ۲۰۰۸). در برخی موارد، ممکن است پیروی از الزامات امنیتی در تضاد با وظایف اولیه کارکنان باشد و درنتیجه امنیت اطلاعات در ازای انجام وظایف اصلی به خطر بیافتد (پاهنیلا و همکاران، ۲۰۰۷). علاوه بر این، هزینه‌های پیروی برخلاف بازده مثبت پیروی، مانند ایمنی و پاداش، که مبهم است معمولاً واقعی و فوری است (کیرسچ و باوس[2] ۲۰۰۷). از آنجاکه امنیت نیازمند وظایف پیچیده‌ای است بنابراین ممکن است که کارمندان الزامات امنیتی را در انجام وظایفشان در نظر نگیرند. ازاین‌رو کارکنان آنچه که باعث سرعت در انجام وظایفشان شود را به آنچه که باید انجام دهند ترجیح می‌دهند (پاهنیلا و همکاران، ۲۰۰۷).

طبق نظریه انتظار – ارزش، انتظار فرد از یادگیری کسب منفعت و نتایج مطلوب است نه نتایج نامطلوب؛ بنابراین اگر کارکنان منافع و یا مضرات حاصل از پیروی را درک کنند، یا نگرش مطلوب نسبت به پیروی شکل خواهد گرفت یا تلاش کمتری برای پیروی صرف می‌کنند (بالگارکیو و همکاران، ۲۰۱۰a). پست و کاگان[3](۲۰۰۷) دریافتند که کاربران اقدامات امنیتی را به‌عنوان مانعی برای روال عادی فعالیت‌های خود می‌دانند.

تأثیر باورها در مورد پیامدهای پیروی بر نگرش نسبت به پیروی

[1] Tolman
[2] Kirsch & Boss
[3] Post and Kagan’s

طبق بررسی انجام‌شده توسط بالگارکیو و همکاران (۲۰۱۰a)، کیم و همکاران (۲۰۱۴) باورها در مورد پیامدهای پیروی تأثیر مثبتی بر نگرش دارد؛ بنابراین فرضیه زیر ارائه‌شده است:

H_3: باورها در مورد پیامدهای پیروی تأثیر مثبت و معناداری بر نگرش کارکنان نسبت به پیروی از سیاست‌های امنیت اطلاعات در سازمان دارد.

تأثیر باورها در مورد ارزیابی کلی عواقب عدم پیروی بر نگرش نسبت به پیروی

طبق بررسی انجام‌شده توسط بالگارکیو و همکاران (۲۰۱۰a)، کیم و همکاران (۲۰۱۴) باورها در مورد ارزیابی کلی عواقب عدم پیروی تأثیر مثبتی بر نگرش دارد؛ بنابراین فرضیه زیر ارائه‌شده است:

H_4: باورها در مورد ارزیابی کلی عواقب عدم پیروی تأثیر مثبت و معناداری بر نگرش نسبت به پیروی از سیاست‌های امنیت اطلاعات در سازمان دارد.

تأثیر باورها در مورد هزینه‌های پیروی بر نگرش نسبت به پیروی

بالگارکیو و همکاران (۲۰۱۰a)، کیم و همکاران (۲۰۱۴) در پژوهشی با استفاده از نظریه انتظار- ارزش فیش‌بن و آجزن (۱۹۷۵) بیان کردند که باورها در مورد هزینه‌های پیروی تأثیر منفی بر نگرش دارد؛ بنابراین فرضیه زیر ارائه‌شده است:

H_5: باورها در مورد هزینه‌های پیروی تأثیر منفی بر نگرش کارکنان نسبت به پیروی از سیاست‌های امنیت اطلاعات در سازمان دارد.

خودکارآمدی برای پیروی

خودکارآمدی به‌عنوان درک افراد از توانایی‌های خود برای انجام اقدامات ضروری برای رسیدن به اهداف تعیین‌شده تعریف‌شده است. خودکارآمدی به احساس عزت‌نفس، ارزش خود، احساس کفایت و کارایی در برخورد با زندگی اطلاق می‌شود (باندورا و همکاران[1] ۱۹۷۷). پورافکاری (۱۳۸۵) باورهای شخص در مورد توانایی برای کنار آمدن با موقعیت‌های متفاوت را خودکارآمدی می‌داند. آلبرت باندورا[2] (۱۹۸۶) خودکارآمدی را به‌عنوان قضاوت مردم از توانایی‌های خویش برای سازمان‌دهی و اجرای رفتارهای موردنیاز برای رسیدن به اهداف از پیش تعیین‌شده تعریف کرده است. به‌طور خاص، خودکارآمدی به‌عنوان یک تأثیر مشخصی بر توانایی افراد برای انجام وظایفشان مانند استفاده از سیستم‌های اطلاعاتی نشان داده‌شده است (کامپو و هیگینز،[3] ۱۹۹۵).

[1] Bandura et al
[2] Albert Bandura
[3] Compeau & Higgins

تأثیر خودکارآمدی برای پیروی بر تمایل به پیروی

مطالعات قبلی نشان می‌دهند که در افراد با خودکارآمدی بالا به‌عنوان‌مثال، کسانی که بر این باور هستند که توانایی انجام کاری را دارند، انگیزه نسبت به رفتار افزایش می‌یابد (برانچو و همکاران[1] ۱۹۹۶؛ چامبلیز و موری[2] ۱۹۷۹).

کامپو و هیگینز (۱۹۹۵)، چان و همکاران (۲۰۰۵)، بالگارکیو و همکاران (۲۰۱۰a)، هراث و رائو (۲۰۰۹)، کیم و همکاران (۲۰۱۴) و ونس و همکاران (۲۰۱۲)، سیپونن و همکاران (۲۰۱۴) و (۲۰۱۰)، ایفندو و همکاران (۲۰۱۴) و (۲۰۱۲) نشان دادند که افراد با خودکارآمدی بالاتر استفاده بیشتری از سیستم‌های اطلاعاتی نسبت به افراد با خودکارآمدی پایین‌تر دارند و خودکارآمدی تأثیر مثبتی بر تمایل به پیروی از سیاست‌های امنیت اطلاعات دارد؛ بنابراین فرضیه زیر ارائه‌شده است:

H_6: خودکارآمدی برای پیروی تأثیر مثبت و معناداری بر تمایل به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان دارد.

عدالت سازمانی

عدالت سازمانی به ادراک کارکنان از انصاف و رفتارهای عادلانه شغلی اشاره می‌کند (جکس و بی‌یر[3] ۱۹۹۱) که شامل ابعاد عدالت توزیعی، عدالت رویه‌ای و عدالت مراوده‌ای است.

عدالت توزیعی[4] به قضاوت در مورد برابری در توزیع نتایج مثل سطح پرداخت و فرصت‌های ارتقاء در ساختار سازمانی اشاره دارد (حقیقی و همکاران، ۱۳۸۸). عدالت رویه‌ای[5] انصاف درک شده از رویه‌های مورداستفاده برای تصمیم‌گیری از سوی کارکنان است. به‌عبارت‌دیگر هنگام قضاوت در مورد میزان رعایت عدالت رویه‌ای در سازمان، کیفیت رفتار بین تصمیم‌گیرندگان با کارکنان سازمان به‌عنوان یک عامل کلیدی در نظر گرفته می‌شود (دهقان و همکاران، ۱۳۹۱). عدالت مراوده‌ای[6] برمبنای انصاف ادراک‌شده از ارتباطات بین شخصی مرتبط با رویه‌های سازمانی و کیفیت ارتباطات بین شخصی تعریف‌شده است (بیز و مواگ[7] ۱۹۸۶).

بر اساس نظریه مبادله اجتماعی زمانی که سازمان توقعات و انتظارات کارکنان را برآورده سازد، کارکنان نیز انتظارات و توقعات سازمان را برآورده خواهند کرد. ازجمله انتظارات مهمی که کارکنان از رهبران سازمان خوددارند، رفتار عادلانه و همراه باانصاف با آن‌ها است. کارکنان انتظار دارند که رفتار رهبرانشان توأم باانصاف و بی‌طرفی باشد، در این صورت است که آنان نیز سعی خواهند نمود در آورده-

---

[1] Brancheau et al
[2] Chambliss & Murray
[3] Jex & Beehr
[4] Distributive Justice
[5] Procedural Justice
[6] Interactional Justice
[7] Bies & Moag

هایشان به سازمان انصاف را رعایت کرده، بیشتر خود را در کار درگیر کرده و عملکرد بالاتری از خود نشان دهند (خنیفر و همکاران، ۱۳۸۹).

تأثیر عدالت سازمانی بر نگرش و تمایل به پیروی

مطالعات مختلف در مورد عدالت بر این نکته تأکید می‌کنند که اگر سازمانی در مقرر ساختن رویه‌های عادلانه شکست خورد، رفتارهای مخرب افزایش می‌یابد. بالگارکیو و همکاران (۲۰۰۹) نشان دادند که عدالت بر نگرش و تمایل به پیروی کارکنان تأثیر مثبت دارد؛ بنابراین فرضیه‌های زیر ارائه‌شده است:

H_7: عدالت سازمانی تأثیر مثبت و معناداری بر نگرش نسبت به پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان دارد.

H_8: عدالت سازمانی تأثیر مثبت و معناداری بر تمایل به پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان دارد.

آگاهی از امنیت اطلاعات

انجمن امنیت اطلاعات(۲۰۰۳) آگاهی از امنیت اطلاعات را به‌عنوان درجه یا میزانی که هر عضو از کارکنان اهمیت امنیت اطلاعات را درک می‌کنند، تعریف کرده است. ابعاد کلیدی آگاهی از امینت اطلاعات، آگاهی عمومی و آگاهی از سیاست امنیت اطلاعات است. آگاهی عمومی از امینت اطلاعات به‌عنوان دانش کلی کارکنان و درک آن‌ها از مسائل مربوط به امنیت اطلاعات و پیامدهای آن است. فراتر از آگاهی عمومی از امنیت اطلاعات، سازمان‌ها از کارکنانشان انتظارات خاصی دارند که در سیاست‌های امنیت اطلاعات سازمان منعکس‌شده است. آگاهی از سیاست امنیت اطلاعات به‌عنوان دانش و درک کارکنان از الزامات مقرر در سیاست‌های امنیت اطلاعات و اهداف این الزامات تعریف‌شده است (بالگارکیو و همکاران، ۲۰۱۰a).

آگاهی از سیاست‌های امنیت اطلاعات با آگاهی عمومی از امنیت اطلاعات متفاوت است. برای مثال، ممکن است یک کارمند به‌طورکلی آگاهی داشته باشد که استفاده از رمز عبور بنا بر احتیاط ضروری است اما ممکن است از اینکه رمز عبور باید به‌صورت دوره‌ای تغییر کند یا رمز عبور باید شامل ترکیب خاصی از حروف و اعداد با تعداد مشخصی کاراکتر باشد، آگاه نباشد. به همین دلیل می‌توان آگاهی از امنیت اطلاعات را شامل آگاهی عمومی و آگاهی از سیاست‌های امنیت اطلاعات در نظر گرفت (بالگارکیو و همکاران، ۲۰۱۰a).

تأثیر آگاهی از امنیت اطلاعات بر باورها

[1] Information security forum (ISF)

بر اساس نقش عوامل پس‌زمینه در نظریه رفتار برنامه‌ریزی‌شده که توسط آجزن و آلباراسین (۲۰۰۷) شرح داده‌شده، اثبات‌شده است که آگاهی از امنیت اطلاعات بر باورهای کارکنان تأثیر می‌گذارد؛ که در پژوهش حاضر سه دسته باور در مورد، هزینه‌های پیروی، ارزیابی کلی عواقب عدم پیروی و پیامدهای پیروی ارائه‌شده است. همچنین طبق بررسی انجام‌شده توسط بالگارکیو و همکاران (۲۰۱۰a) آگاهی از امنیت اطلاعات اثر مثبتی بر باورها در مورد هزینه‌های پیروی، باورها در مورد ارزیابی کلی عواقب عدم پیروی و باورها در مورد پیامدهای پیروی دارد و این تأثیر مورد تائید قرارگرفته است؛ بنابراین فرضیه‌های زیر پیشنهادشده است:

H_9: آگاهی از امنیت اطلاعات تأثیر مثبت و معناداری بر باورها در مورد پیامدهای پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی دارد.

H_{10}: آگاهی از امنیت اطلاعات تأثیر مثبت و معناداری بر باورها در مورد ارزیابی کلی عواقب عدم پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی دارد.

H_{11}: آگاهی از امنیت اطلاعات تأثیر مثبت و معناداری بر باورها در مورد هزینه‌های پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی دارد.

تأثیر آگاهی از امنیت اطلاعات بر نگرش نسبت به پیروی

بالگارکیو (۲۰۰۹) در پژوهشی بر اساس مدل پنج مرحله‌ای در فرآیند تصمیم‌گیری نوآورانه راجرز[1] (۲۰۰۳) بیان کرده است که آگاهی از امنیت اطلاعات به‌طور مستقیم بر شکل‌گیری نگرش نسبت به امنیت اطلاعات اثرگذار است. ازنظر راجرز (۲۰۰۳) آگاهی بر ترغیب و تشویق مؤثر است، پس می‌توان نتیجه گرفت که آگاهی از امنیت اطلاعات بر نگرش کارکنان نسبت به پیروی تأثیرگذار است. این رویکرد با نظر سیپونن (۲۰۰۰) که آگاهی از امنیت اطلاعات، عامل بسیار مهمی در ترغیب کارکنان به تغییر رویکرد پیروی از سیاست‌های امنیت اطلاعات است، سازگار است (بالگارکیو و همکاران، ۲۰۰۹).

آلبرستسن[2] (۲۰۰۷)، بالگارکیو و همکاران (۲۰۱۰a)، کاجتازی[3] و همکاران (۲۰۱۳) با استفاده از نظریه رفتار برنامه‌ریزی‌شده آجزن (۱۹۹۱) و مدل تصمیم‌گیری راجرز (۲۰۰۳) بیان کردند که آگاهی از امنیت اطلاعات تأثیر مستقیمی بر نگرش کارکنان نسبت به پیروی از سیاست‌های امنیت اطلاعات دارد؛ بنابراین فرضیه زیر ارائه‌شده است:

H_{12}: آگاهی از امنیت اطلاعات بر نگرش کارکنان نسبت به پیروی از سیاست‌های امنیت اطلاعات در سازمان تأثیر مثبت و معناداری دارد.

تأثیر آگاهی از امنیت اطلاعات بر عدالت سازمانی

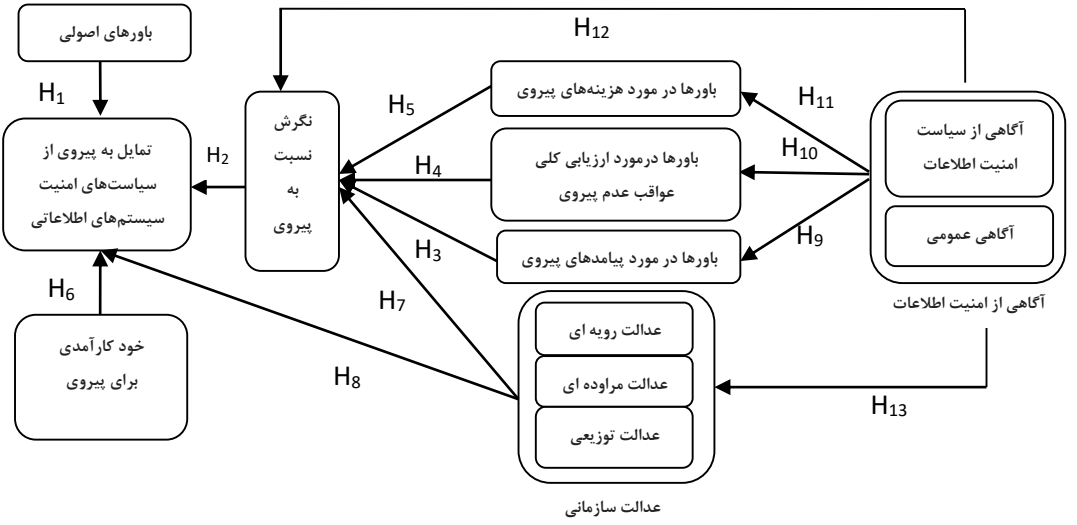
[1] Rogers
[2] Albrechtsen
[3] Kajtazi

آگاهی از امنیت اطلاعات کارکنان بر ادراک آن‌ها نسبت به عادلانه بودن قوانین و مقررات امنیت اطلاعات در سازمان تأثیرگذار است. دانش کارکنان از قوانین و مقررات امنیتی و همچنین درک اهداف و مقاصد اصلی این مقررات، عدالت رعایت شده در قوانین و مقررات را افزایش می‌دهد (بالگارکیو و همکاران، ۲۰۰۹). طبق بررسی انجام‌شده توسط بالگارکیو و همکاران (۲۰۰۹) آگاهی از امنیت اطلاعات اثر مثبتی بر عدالت سازمانی دارد؛ بنابراین فرضیه زیر پیشنهادشده است:

H_{13}: آگاهی از امنیت اطلاعات تأثیر مثبت و معناداری بر عدالت سازمانی دارد.

مدل مفهومی پژوهش

بر اساس مطالب بالا و فرضیه‌های ارائه‌شده مدل مفهومی پژوهش (شکل ۱) در پی آن است تا عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان را موردبررسی قرار دهد. این مدل با نظرخواهی از خبرگان و پس از ترکیب و تعدیل مدل بالگارکیو و همکاران (۲۰۱۰a) و (۲۰۱۰b) و مدل بالگارکیو و همکاران (۲۰۰۹) ارائه‌شده است.



شکل ۱. مدل مفهومی پژوهش

روش‌شناسی پژوهش

این پژوهش با توجه به هدف، از نوع کاربردی و روش اجرای آن توصیفی – پیمایشی از نوع همبستگی است. جامعه آماری این پژوهش شامل کارکنان پنج اداره دولتی شهرستان نجف‌آباد در مقطع زمانی سال ۱۳۹۴ است و حجم نمونه ۲۱۷ نفر بر اساس جدول کرجسی و مورگان (۱۹۷۰) انتخاب‌شده که تعداد پرسشنامه‌های جمع‌آوری‌شده ۲۲۱ عدد است. به‌منظور ایجاد تناسب بین جمعیت هر اداره و تعداد نمونه

موردنیاز از روش نسبتی استفاده‌شده است. برای گردآوری داده‌ها از پرسشنامه استفاده‌شده است. روایی پرسشنامه توسط اساتید خبره در حوزه سیستم‌های اطلاعاتی و فناوری اطلاعات سنجیده شده است و پایایی پرسشنامه نیز از طریق ضریب آلفای کرونباخ اندازه‌گیری شده که مقدار آن طبق جدول ۱ برای همه متغیرها بالاتر از ۰/۷ است که نشان‌دهنده پایایی بالای متغیرها است.

جدول ۱. آلفای کرونباخ و پایایی پرسشنامه

متغیر	آلفا
عدالت مراوده‌ای	۰/۸۵۰
عدالت رویه‌ای	۰/۸۸۶
عدالت توزیعی	۰/۸۷۸
باورها در مورد هزینه‌های پیروی	۰/۷۴۹
باورها در مورد پیامدهای پیروی	۰/۷۴۰
باورها در مورد ارزیابی کلی عواقب عدم پیروی	۰/۷۸۲
نگرش نسبت به پیروی	۰/۹۴۰
خودکارآمدی برای پیروی	۰/۷۵۶
باورهای اصولی	۰/۷۷۲
آگاهی از سیاست‌های امنیت اطلاعات	۰/۸۲۸
آگاهی عمومی از امنیت اطلاعات	۰/۷۶۳
تمایل به پیروی	۰/۸۸۹

پرسشنامه این پژوهش شامل ۴۸ گویه بوده که در آن از پاسخ‌دهنده خواسته‌شده است، نظر خود را در خصوص شناسایی عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت اطلاعات با استفاده از طیف لیکرت بیان نماید. منابع نشانگرهای اندازه‌گیری سازه‌ها در جدول ۲ آمده است. در ضمن همه مراحل پردازش داده‌ها با استفاده از نرم‌افزارهای SPSS، Word، Excel و Amos صورت گرفته است.

جدول ۲. تعداد سازه‌ها و منابع نشانگرهای سازه‌ها

سازه‌ها	تعداد گویه‌ها	منابع
تمایل به پیروی	۳	بالگارکیو و همکاران (۲۰۱۰a)
آگاهی عمومی از امنیت اطلاعات	۳	بالگارکیو و همکاران (۲۰۱۰a)
آگاهی از سیاست‌های امنیت اطلاعات	۳	بالگارکیو و همکاران (۲۰۱۰a)
باورهای اصولی	۳	بالگارکیو و همکاران (۲۰۱۰a)
خودکارآمدی برای پیروی	۳	بالگارکیو و همکاران (۲۰۱۰a)
نگرش نسبت به پیروی	۴	بالگارکیو و همکاران (۲۰۱۰a)
باورها در مورد ارزیابی کلی عواقب عدم پیروی	۶	بالگارکیو و همکاران (۲۰۱۰a)
باورها در مورد هزینه‌های پیروی	۴	بالگارکیو و همکاران (۲۰۱۰a)
باورها در مورد پیامدهای پیروی	۷	بالگارکیو و همکاران (۲۰۱۰a)

سازه‌ها	تعداد گویه‌ها	منابع
عدالت توزیعی	۴	فیوچس[1](۲۰۱۰)
عدالت رویه‌ای	۴	فیوچس (۲۰۱۰)
عدالت مراوده‌ای	۴	فیوچس (۲۰۱۰)

یافته‌های پژوهش

الف) یافته‌های توصیفی جمعیت شناختی

- توزیع فراوانی نمونه برحسب جنسیت نشان می‌دهد، حدود ۶۸ درصد پاسخگویان مرد و ۳۲ درصد از آن‌ها زن هستند.
- توزیع فراوانی نمونه برحسب سطح تحصیلات نشان می‌دهد، تعداد افراد با سطح تحصیلات لیسانس ۱۲۶ نفر (۵۷ درصد کل) بیشترین حجم نمونه را تشکیل می‌دهند. سایر تحصیلات کمترین حجم نمونه را به خود اختصاص داده‌اند و تعداد افرادی که دیپلم، فوق‌لیسانس و فوق‌دیپلم به ترتیب، بعد از لیسانس بیشترین حجم نمونه را دارند.
- توزیع فراوانی نمونه برحسب سن نشان می‌دهد، بیشترین حجم نمونه (معادل ۳۰/۸ درصد)، بالاتر از چهل سال سن دارند، افراد ۲۱ تا ۲۵ سال با ۳/۶ درصد کمترین حجم نمونه را تشکیل می‌دهند. در نمونه موردبررسی هیچ فردی ۲۰ سال و کمتر نبود.
- توزیع فراوانی نمونه برحسب سابقه کار نشان می‌دهد، بیشترین حجم نمونه (معادل ۴۲/۵ درصد)، بیش از ۱۵ سال سابقه کار دارند. درصد کسانی که ۱ تا ۵ سال سابقه کار دارند، با ۹/۴ درصد کل نمونه، کمترین میزان را دارا است.
- توزیع فراوانی نمونه برحسب پست سازمانی نشان می‌دهد، کمترین حجم نمونه یعنی ۹ نفر مدیر هستند و ۱۴ درصد نمونه کارشناس ارشد هستند.

ب) یافته‌های تحلیلی

به‌منظور ارزیابی مدل اندازه‌گیری مراحل زیر طی شد:

ارزیابی نرمال بودن داده‌ها: ارزیابی نرمال بودن داده‌ها از طریق چولگی و کشیدگی صورت گرفت که نشان داده شد داده‌ها دارای توزیع نرمال هستند.

بررسی پایایی و روایی مدل اندازه‌گیری: در این پژوهش پایایی و روایی اجزای مدل اندازه‌گیری (مقیاس اندازه‌گیری) به روش‌های زیر بررسی شد:

الف) روایی همگرا:[2] که به‌صورت زیر بررسی شد:

[1] Fuchs

[2] Convergent Validity

بار عاملی: طبق گفته فورنل و لارکر[۱](۱۹۸۱) و هیر[۲]و همکاران (۲۰۰۶) بارهای عاملی که حداقل برابر با ۰/۵ باشند، اعتبار را نشان می‌دهند. همان‌طور که در جدول ۳ مشاهده می‌شود، بارهای عاملی در این مدل بین ۰/۵۱۸ برای گویه ۳-خودکارآمدی در پیروی از سیاست‌های امنیت اطلاعات تا ۰/۹۱۲ برای گویه ۳- باورها در مورد هزینه‌های پیروی از سیاست‌های امنیت اطلاعات دامنه دارد که همگی در محدوده قابل‌قبول قرار دارند. همچنین، از آنجاکه در سطح اطمینان ۹۹ درصد آماره تی برای همه گویه‌ها بیش از ۱/۹۶ است، درنتیجه، بارهای عاملی معنادار است.

شاخصAVE[۳]: طبق عقیده هیر و همکاران (۲۰۰۶) درصورتی‌که این شاخص بالاتر از ۰/۵ باشد، اعتبار سازه قابل‌قبول است. طبق جدول ۳ شاخص AVE برای متغیرهای مدل بین ۰/۷۱۱ تا ۰/۸۰۹ به دست آمد که نشان‌دهنده اعتبار قابل‌قبول و خوب است.

ب) پایایی مرکب (شاخصCR[۴]**)**: طبق نظر هیر و همکاران (۲۰۰۶) درصورتی‌که این شاخص بالاتر از ۰/۷ باشد، اعتبار سازه خوب است و بین ۰/۶ تا ۰/۷ قابل‌قبول است.

طبق جدول ۳ شاخص CR برای متغیرهای مدل بین ۰/۶۳۲ تا ۰/۸۱۱ به دست آمد که نشان‌دهنده پایایی قابل‌قبول و خوب است.

جدول۳. بررسی پایایی و روایی مدل اندازه‌گیری

متغیر	شاخص	بارعاملی	آماره تی	AVE	CR	VIF	TOL
عدالت سازمانی				۰/۷۴۹	۰/۸۰۱	۲/۳۸۰	۰/۴۲۰
	عدالت توزیعی	۰/۷۸۹	۸/۵۲۱				
	عدالت رویه ای	۰/۹۰۸	۱۲/۲۲۲				
	عدالت مراوده ای	۰/۶۹۹	۹/۴۵۱				
آگاهی از امنیت اطلاعات				۰/۷۴۴	۰/۶۹۵	۲/۵۰۶	۰/۳۹۹
	آگاهی عمومی	۰/۷۰۱	۱۰/۳۱۸				
	آگاهی از سیاست‌های امنیت اطلاعات	۰/۸۱۵	۱۱/۲۱۱				
باورها در مورد ارزیابی عواقب عدم پیروی				۰/۸۰۱	۰/۷۵۱	۲/۴۸۷	۰/۴۰۲
	گویه ۱	۰/۵۵۰	۸/۲۰۱				

[۱] Fornell & Larcker

[۲] Hair

[۳] Average Variance Extracted

[۴] Composite Reliability

متغیر	شاخص	بارعاملی	آماره تی	AVE	CR	VIF	TOL
	گویه ۲	۰/۶۲۳	۹/۲۱۴				
	گویه ۳	۰/۷۶۴	۹/۶۵۹				
	گویه ۶	۰/۵۴۱	۶/۲۱۵				
باورهـا در مـورد پیامـدهای پیروی				۰/۷۱۱	۰/۶۸۱	۲/۳۵۲	۰/۴۲۵
	گویه ۱	۰/۵۴۹	۶/۵۴۱				
	گویه ۳	۰/۶۵۳	۸/۸۵۲				
	گویه ۴	۰/۶۰۵	۸/۶۵۴				
	گویه ۷	۰/۵۷۸	۷/۵۴۵				
تمایل به پیروی				۰/۸۱۱	۰/۸۰۹		
	گویه ۱	۰/۸۰۸	۱۰/۶۵۴				
	گویه ۲	۰/۹۰۶	۱۲/۱۲۶				
	گویه ۳	۰/۵۸۱	۷/۳۱۶				
باورهای اصولی				۰/۸۰۰	۰/۷۱۵	۳/۴۹۳	۰/۴۰۱
	گویه ۱	۰/۶۲۸	۸/۶۹۰				
	گویه ۲	۰/۸۳۸	۱۰/۳۵۲				
	گویه ۳	۰/۸۱۹	۱۰/۹۶۵				
نگرش نسبت به پیروی				۰/۷۶۳	۰/۶۳۲	۱/۹۸۴	۰/۵۰۴
	گویه ۱	۰/۶۹۸	۸/۳۲۵				
	گویه ۲	۰/۸۲۳	۱۰/۲۵۴				
	گویه ۳	۰/۷۸۲	۷/۳۵۹				
خودکارآمدی برای پیروی				۰/۷۵۹	۰/۷۲۱	۲/۰۰۴	۰/۴۹۹
	گویه ۱	۰/۷۵۴	۹/۲۱۲				
	گویه ۲	۰/۹۰۶	۱۰/۵۲۱				
	گویه ۳	۰/۵۱۸	۸/۲۱۵				
باورها در مورد هزینه های پیروی				۰/۷۸۴	۰/۷۵۴	۲/۶۳۸	۰/۳۷۹
	گویه ۱	۰/۵۱۹	۶/۶۴۷				
	گویه ۳	۰/۹۱۲	۱۲/۲۵۴				
	گویه ۴	۰/۶۷۴	۸/۹۵				

ب) اعتبارتشخیصی[1] به دلیل این‌که در این مدل بیش از یک متغیر پنهان وجود دارد، اعتبار تشخیصی نیز بررسی شد. چنانچه ریشه دوم شاخص AVE برای هر متغیر از همبستگی بین متغیر مذکور با سایر متغیرهای مدل بیشتر باشد، سازه‌ها دارای اعتبار تشخیصی هستند. بر اساس جدول ۴، ریشه دوم AVE

[1] Discriminant validity

برای هر متغیر بیشتر از همبستگی آن متغیر با سایر متغیرهاست؛ بنابراین، اعتبار تشخیصی سازه‌ها تأیید شد.

جدول ۴. بررسی اعتبار تشخیصی داده‌ها

سازه	عدالت سازمانی	آگاهی از امنیت اطلاعات	ارزیابی کلی عواقب عدم پیروی	باور در پیامدهای پیروی	تمایل به پیروی امنیت اطلاعات	باورهای اصولی	نگرش به پیروی	خودکارآمدی در پیروی	باور در مورد هزینه پیروی
۱	۰/۸۹۱**								
۲	۰/۳۲۵	۰/۸۶۵**							
۳	۰/۱۲۲	۰/۳۹۱	۰/۸۹۴**						
۴	۰/۵۰۶	۰/۴۴۹	۰/۵۴۶	۰/۷۴۳**					
۵	۰/۰۶۲	۰/۲۷۵	۰/۱۷۱	۰/۳۳۹	۰/۸۹۹**				
۶	۰/۰۴۲	۰/۴۱۷	۰/۴۰۷	۰/۳۹۵	۰/۳۸۷	۰/۸۹۴**			
۷	۰/۰۵۱	۰/۴۴۸	۰/۳۹۴	۰/۲۸۹	۰/۵۰۵	۰/۴۹۰	۰/۸۷۳**		
۸	۰/۱۳۲	۰/۷۳۰	۰/۱۶۳	۰/۳۱۴	۰/۱۰۹	۰/۲۵۶	۰/۱۴۰	۰/۸۶۷**	
۹	۰/۰۳۸	-۰/۰۶۰	-۰/۱۱۳	۰/۰۰۸	۰/۰۰۶	-۰/۱۲۶	-۰/۰۰۵	-۰/۰۴۰	۰/۸۸۵**

** ریشه دوم AVE

بررسی هم خطی چندگانه[1]

به‌منظور بررسی عدم وجود همبستگی بالا بین متغیرهای مستقل که در صورت وجود باعث ایجاد اشکال در آزمون مدل پژوهش می‌شود هم خطی چندگانه بررسی شد. به دلیل اینکه همبستگی بین سازه‌ها (جدول ۴) پایین‌تر از ۰/۹ است و هیچ پیام خطایی مبنی بر همبستگی خطی سازه‌ها از طریق خروجی نرم‌افزار AMOS دریافت نشد؛ درنتیجه، همبستگی خطی وجود ندارد. برای اطمینان از این ادعا، دو شاخص VIF و TOL در مورد تک‌تک متغیرها بررسی شد، نتایج در جدول ۳ درج‌شده است.

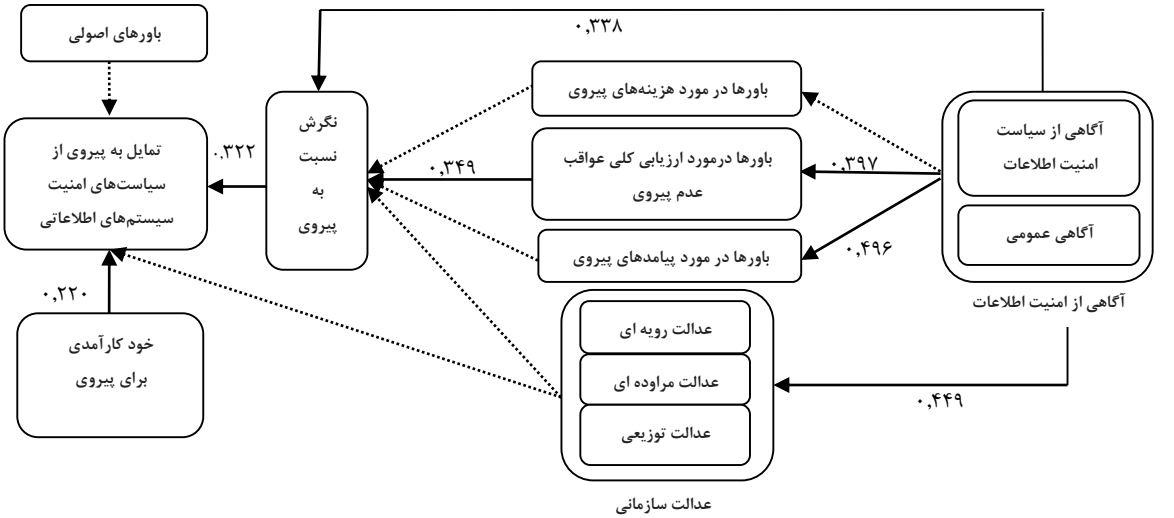
طبق نظر هیر و همکاران (۲۰۰۶) چنانچه VIF≥ ۴ و یا TOL<۰/۳، نشان از وجود هم خطی چندگانه است. با توجه به جدول ۳، داده‌ها در تمامی متغیرها در محدوده قابل‌قبول قرار دارند و هم خطی در هیچ‌یک مشاهده نشد.

تحلیل مسیر و آزمون فرضیه‌های پژوهش

[1] Multicollinearity

نتایج مدل‌سازی معادلات ساختاری و تحلیل مسیر در شکل ۲ نشان داده‌شده است.

همان‌طور که در شکل ۲ مشاهده می‌شود، شاخص‌های CFI، IFI، GFI و RMSEA، به ترتیب، برابر با ۰/۹۰۷، ۰/۹۱۱، ۰/۹۰۱ و ۰/۰۶۳هستند که همگی قابل‌قبول‌اند.



شکل ۲. مدل ساختاری پژوهش

نتایج تجزیه‌وتحلیل مسیر نشان داد باورهای اصولی با β= ۰/۱۵۱ و p>۰/۰۵ بر تمایل به پیروی تأثیر معنادار ندارد، بنابراین در سطح اطمینان ۹۵٪ فرضیه اول رد می‌شود؛ اما نگرش نسبت به پیروی با β= ۰/۳۲۲ و p<۰/۰۱ بر تمایل به پیروی تأثیر معنادار دارد، بنابراین در سطح اطمینان ۹۹٪ فرضیه دوم تأیید می‌شود. تأثیر باورها در مورد پیامدهای پیروی بر نگرش نسبت به پیروی معنادار نیست. درنتیجه، فرضیه سوم پژوهش رد می‌شود. همچنین، باورها در مورد ارزیابی کلی عواقب عدم پیروی با β= ۰/۳۴۹ و p<۰/۰۱ بر نگرش نسبت به پیروی تأثیر دارد، بنابراین در سطح اطمینان ۹۹٪ فرضیه چهارم پژوهش تأیید می‌شود. تأثیر باورها در مورد هزینه‌های پیروی بر نگرش نسبت به پیروی معنادار نیست. درنتیجه، فرضیه پنجم پژوهش رد می‌شود. خودکارآمدی برای پیروی با β= ۰/۲۲۰ و p<۰/۰۵ بر نگرش نسبت به پیروی تأثیر دارد، بنابراین در سطح اطمینان ۹۵٪ فرضیه ششم تأیید می‌شود. عدالت سازمانی با β= ۰/۱۱۶ و β= ۰/۰۰۷، به ترتیب در سطح اطمینان ۹۵٪ بر نگرش نسبت به پیروی و تمایل به پیروی تأثیر ندارد، بنابراین فرضیه‌های هفتم و هشتم رد می‌شوند. آگاهی از امنیت اطلاعات با β= ۰/۴۹۶ و β=۰/۳۹۷، به ترتیب در سطح اطمینان ۹۹٪ بر باورها در مورد پیامدهای پیروی و باورها در مورد ارزیابی کلی عواقب عدم پیروی تأثیر دارد، بنابراین فرضیه‌های نهم و دهم تأیید می‌شوند. تأثیر آگاهی از امنیت اطلاعات بر باورها در مورد هزینه‌های پیروی معنادار نیست. درنتیجه، فرضیه یازدهم پژوهش رد می‌شود. همچنین، آگاهی از امنیت اطلاعات با β= ۰/۳۳۸ و β=۰/۴۴۹، به ترتیب در سطح اطمینان ۹۹٪ بر

نگرش نسبت به پیروی و عدالت سازمانی تأثیر دارد، بنابراین فرضیه‌های دوازدهم و سیزدهم تأیید می‌شوند.

جدول ۵. ضرایب تعیین متغیرهای مدل

متغیر	باورها در مورد ارزیابی کلی عواقب عدم پیروی	باورها در مورد پیامدهای پیروی	عدالت سازمانی	نگرش نسبت به پیروی	تمایل به پیروی
ضریب تعیین	۰/۱۵۸	۰/۲۴۷	۰/۲۰۲	۰/۲۸۲	۰/۱۸۰

از طرفی با توجه به جدول ۵ ضریب تعیین باورها در مورد ارزیابی کلی عواقب عدم پیروی برابر با ۰/۱۵۸ به دست آمد یعنی حدود ۱۶ درصد تغییرات این متغیر توسط متغیر آگاهی از امنیت اطلاعات تعیین می‌شود و بقیه تغییرات این متغیر توسط متغیرهای دیگری که در این پژوهش مدنظر قرار نگرفته است، تعیین می‌شود. متغیرهای باورها در مورد ارزیابی کلی عواقب عدم پیروی و آگاهی از امنیت اطلاعات درمجموع، ۲۸ درصد تغییرات نگرش به پیروی را تبیین می‌کنند. همچنین، حدود ۲۵ درصد تغییرات متغیر باور به نتایج پیروی و ۲۰ درصد تغییرات متغیر عدالت سازمانی توسط متغیر آگاهی از امنیت اطلاعات تبیین می‌شود. ضریب تعیین تمایل به پیروی از سیاست‌های امنیت اطلاعات ۰/۱۸ به دست آمد این به این معناست که فقط ۱۸ درصد تغییرات متغیر از سیاست‌های امنیت اطلاعات به پیروی توسط نگرش به پیروی و خودکارآمدی در پیروی تبیین می‌شود و ۸۲ درصد تغییرات آن توسط متغیرهایی که در این پژوهش مدنظر قرار نگرفته است، تبیین می‌شود. همچنین در جدول۶ اثرات مستقیم، غیرمستقیم، اثرات کل و نتیجه آزمون فرضیه‌ها آمده است.

جدول ۶. اثرات مستقیم، غیرمستقیم و اثرات کل و آزمون فرضیه‌ها

فرضیه	متغیر مستقل	متغیر وابسته	اثر مستقیم	اثر غیرمستقیم	اثر کل	نتیجه
اول	باورهای اصولی	تمایل به پیروی	۰/۱۵۱		۰/۱۵۱	رد
دوم	نگرش به پیروی	تمایل به پیروی	۰/۳۳۲**		۰/۳۳۲**	تأیید
سوم	باورها در مورد پیامدهای پیروی	نگرش به پیروی	-۰/۰۸۹		-۰/۰۸۹	رد
چهارم	باورها در مورد عواقب عدم پیروی	نگرش به پیروی	۰/۲۶۹**	۰/۰۸۹*	۰/۳۵۸**	تأیید
پنجم	باورها در مورد هزینه‌های پیروی	نگرش به پیروی	۰/۰۱۷		۰/۰۱۷	رد
ششم	خودکارآمدی برای پیروی	تمایل به پیروی	۰/۲۲۰*		۰/۲۲۰*	تأیید
هفتم	عدالت سازمانی	نگرش به پیروی	۰/۱۱۶		۰/۱۱۶	رد
هشتم	عدالت سازمانی	تمایل به پیروی	۰/۰۰۷	۰/۰۳۹	۰/۰۴۶	رد
نهم	آگاهی از امنیت اطلاعات	باورها در مورد پیامدهای پیروی	۰/۴۹۶**		۰/۴۹۶**	تأیید

فرضیه	متغیر مستقل	متغیر وابسته	اثر مستقیم	اثر غیرمستقیم	اثر کل	نتیجه
دهم	آگاهی از امنیت اطلاعات	باورها در مورد عواقب عدم پیروی	۰/۳۹۷**		۰/۳۹۷**	تأیید
یازدهم	آگاهی از امنیت اطلاعات	باورها در مورد هزینه‌های پیروی	-۰/۰۶۷		-۰/۰۶۷	رد
دوازدهم	آگاهی از امنیت اطلاعات	نگرش به پیروی	۰/۳۳۸**	۰/۱۱۴**	۰/۴۵۲**	تأیید
سیزدهم	آگاهی از امنیت اطلاعات	عدالت سازمانی	۰/۴۴۹**		۰/۴۴۹**	تأیید

*معنی‌داری در سطح p<۰/۰۵ ** معنی‌داری در سطح p <۰/۰۱

نتیجه‌گیری، محدودیت‌ها و پیشنهادها

از بین متغیرهای مدل مفهومی پژوهش، نتایج نشان داده است که بر مبنای تحلیل مسیر، دو متغیر نگرش نسبت به پیروی از سیاست‌های امنیت اطلاعات و خودکارآمدی برای پیروی از سیاست‌های امنیت اطلاعات به‌طور مستقیم بر تمایل به پیروی از سیاست‌های امنیت اطلاعات تأثیر دارد که دراین‌بین تأثیر متغیر نگرش نسبت به پیروی از سیاست‌های امنیت اطلاعات قوی‌تر است. همچنین، آگاهی از سیاست‌های امنیت اطلاعات بر تمایل به پیروی از سیاست‌های امنیت اطلاعات به‌طور غیرمستقیم تأثیر بسزایی داشته است.

از طرفی، با توجه به ضریب تعیین ۰/۲۸۲ که شدت تأثیر نگرش نسبت به پیروی تأثیر را بر روی تمایل به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی نشان می‌دهد، می‌توان اذعان داشت که مسئولان و مدیران سیستم‌های اطلاعاتی و سازمان‌ها باید به دنبال راهی باشند که نگرش کارکنان نسبت به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی را بهبود دهند و درنتیجه تمایل آن‌ها به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی افزایش خواهد یافت.

ازجمله محدودیت‌های این پژوهش می‌توان به محافظه‌کاری کارمندان در پاسخ به سؤالات مربوط به عدالت، میزان وفاداری و صداقت پاسخ‌دهندگان در پاسخگویی به سؤالات ناشی از نگرانی پاسخ‌دهندگان در مشخص شدن اظهارنظر آن‌ها و یا رفتار را نام برد.

در پژوهش حاضر آنچه نتیجه‌گیری شد نشان‌دهنده این موضوع بود که نگرش کارکنان نسبت به پیروی از سیاست‌های امنیت سیستم‌های اطلاعاتی بیشترین تأثیر را بر پیروی دارد. توجه به این نکته لازم است که نگرش‌ها قابل‌تغییر هستند و این امر می‌تواند به نفع سازمان باشد. ازآنجاکه هر سازمان و هر مدیری می‌کوشد نگرش‌های کارکنان را تغییر دهند راه‌هایی برای تغییر نگرش ارائه می‌شود. ازجمله این راه‌ها:

الف) روش‌شناختی؛ ارائه اطلاعات جدید: در این روش مدیران می‌توانند با قرار دادن اطلاعاتی در مورد انواع تهدیدات امنیتی و راه‌های مقابله با آن کارکنان را با این تهدیدات آشنا کرده و زمینه‌های تغییر نگرش کارکنان به‌سوی مثبت بودن پیروی از سیاست‌های امنیتی را فراهم کنند.

ب) روش عاطفی؛ نفوذ همکاران: مدیران می‌توانند از نفوذ کارکنانی که خود از سیاست‌های امنیتی پیروی می‌کنند و همچنین در نزد کارکنان محبوب هستند استفاده کنند. گاهی اوقات کارکنان با توجه به رفتار سایر همکاران رفتار می‌کنند حتی اگر برخلاف نگرش آن‌ها باشد.

ج) روش اجباری؛ به‌کارگیری زور: در این روش رفتارهای مطلوب اعلام و فرد مجبور می‌شود خود را با آن‌ها وفق دهد. از طرفی نیز می‌توان رفتارهای نامطلوب را مشخص کرده و عواقب آن را برای کارکنان بیان کرد (پایگاه جامع دانش مدیریت، ۱۳۸۹).

با توجه به نتایج پژوهش آگاهی از امنیت اطلاعات بر نگرش نسبت به پیروی و درنتیجه بر تمایل به پیروی تأثیرگذار است. قطعاً یکی از راه‌های مهم برای حفاظت و مدیریت امنیت سیستم‌های اطلاعاتی، ارتقای آگاهی کاربران از امنیت اطلاعات است. در این صورت، افراد آگاهی‌های لازم در مورد مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می‌کنند؛ بنابراین پیشنهاد می‌شود علاوه بر سرمایه‌گذاری بر عوامل فنی امنیت، بر عواملی چون ارتقای سطح آگاهی کارکنان در مورد امنیت سیستم‌های اطلاعاتی نیز در سازمان سرمایه‌گذاری صورت پذیرد. بدین منظور می‌توان این مراحل را طی کرد:

۱) شناسایی نقش‌های سازمانی نیازمند آموزش امنیت،
۲) نیازسنجی و تعیین سطح آموزش برای نقش‌ها،
۳) برنامه‌ریزی و طراحی طرح آموزش امنیت،
۴) طراحی دوره‌های بومی امنیت سازمان برای نقش‌ها با توجه به فرهنگ‌سازمانی،
۵) اجرا و برگزاری دوره‌های آموزشی و
۶) ارزیابی کارایی دوره‌های آموزش به‌منظور بهبود و تقویت آن‌ها و سنجش سطح بلوغ امنیت.

با توجه به این‌که سیاست‌های امنیت سیستم‌های اطلاعاتی جزئی ضروری برای حفظ امنیت اطلاعات در سازمان است، لذا به نظر می‌رسد مدیران سطوح عالی برای برقراری امنیت سیستم‌های اطلاعاتی در سازمان می‌توانند با تدوین سیاست‌های امنیت اطلاعات و شفاف‌سازی مسئولیت‌ها، مشخص نمودن سرمایه‌هایی که باید امن شوند، تعیین سطح دسترسی افراد و تعیین محدودیت‌ها به این هدف دست یابند.

بر اساس نتایج پژوهش مدیران می‌توانند با افزایش خودکارآمدی کارکنان از طریق روش‌های مختلف ازجمله برگزاری دوره‌های آموزشی، تلاش برای افزایش اعتمادبه‌نفس، مهارت و تجربیات کارکنان، ایجاد فرهنگ امنیتی، واگذاری وظایف دشوار به کارکنان، دادن اختیار کافی برای انجام کارها بدون نظارت دقیق، قرار دادن زمانی برای جویا شدن در مورد نظرات افراد و گوش سپردن دقیق به آن‌ها، انتقال حس اعتقاد به شایستگی به کارکنان و حمایت مدیران عالی؛ تمایل به پیروی از سیاست‌های امنیت سیستم-های اطلاعاتی در سازمان را افزایش دهند.

ازجمله پیشنهادها برای پژوهش‌های آینده می‌توان به مواردی از این قبیل اشاره نموده: موضوع این پژوهش با رویکرد کیفی و یا ترکیبی موردبررسی قرار گیرد. همچنین تأثیر عدالت سازمانی بر نگرش و تمایل به پیروی به‌صورت دقیق‌تری موردپژوهش قرار گیرد.

فهرست منابع

الهی، شعبان، مهدی طاهری و علیرضا حسن‌زاده. ۱۳۸۸. ارائه چارچوبی برای عوامل انسانی مرتبط در امنیت سیستم‌های اطلاعاتی. *مدرس علوم انسانی*، (۶۱)، ۲۲-۱.

براتی، مجید، حمید الهودی‌پور، بابک معینی، عبدالله فرهادی‌نسب، حسین محجوب و فرزاد جلیلیان. ۱۳۹۰. اثربخشی آموزش مهارت جراتمندی در کاهش هنجارهای انتزاعی ترغیب‌کننده مصرف مواد مخدر در بین دانشجویان. *دانشگاه علوم پزشکی و خدمات بهداشتی درمانی همدان*، ۱۸ (۳)، ۴۰-۴۹.

پایگاه جامع دانش مدیریت ۱۳۸۹. ایجاد و تغییر نگرش. بازیابی شده در تاریخ (۹۴/۶/۲۶) از آدرس اینترنتی http://tasmim.blogfa.com/post-82.aspx.

جهان نیوز ۱۳۹۳. اقدامات ایران برای مقابله با تروریسم سایبری. بازیابی شده در تاریخ (۹۳/۹/۳) از آدرس اینترنتی http://jahannews.com/vdcaemn6e49nea1.k5k4.html.

حقیقی، محمدعلی، ایمان احمدی و حمید رامین‌مهر. ۱۳۸۸. بررسی تأثیر عدالت سازمانی بر عملکرد کارکنان. مدیریت فرهنگ سازمانی، ۷ (۲۰)، ۱۰۱-۷۹.

حسن‌زاده، محمد، داوود کریم‌زادگان‌مقدم و نرگس جهانگیری. ۱۳۹۱. ارائه یک چارچوب مفهومی برای ارزیابی پرمایگی و آموزش آگاهی از امنیت اطلاعات کاربران. *نظام‌ها و خدمات اطلاعاتی*، ۱ (۲)،-۱ ۱۶.

خنیفر، حسین، علی‌نقی امیری، غلامرضا جندقی، هادی احمدی‌آزرم و مجتبی حسینی‌فرد. ۱۳۸۹. درگیر شدن در کار و رابطه آن با عدالت سازمانی در چهارچوب نظریه مبادله اجتماعی و فرهنگی. *مدیریت فرهنگ سازمانی*، ۸ (۲۱)، ۲۰۰-۱۷۷.

دهقان، نبی اله، عباس عمرانی‌فر، محمدرضا حسینی و صمد فتحی. ۱۳۹۱. بررسی رابطه بین رعایت عدالت سازمانی و رضایت شغلی کارکنان (مورد مطالعه یک سازمان نظامی). *مدیریت نظامی*، ۴۶ (۱۲)، ۶۵-۱۰۲.

طاووسی، محمود، علیرضا حیدرنیا، علی منتظری، فرهاد طارمیان، حسین اکبری و علی‌اصغر حائری. ۱۳۸۸. تمایز بین دو سازه کنترلی: کاربردی از نظریه رفتار برنامه‌ریزی‌شده برای پرهیز از سوء مصرف مواد مخدر در نوجوانان. *افق دانش*، ۱۵ (۳)، ۴۵-۳۶.

Ajzen, Icek. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, (2): 179-211.

Ajzen, Icek., and Dolores Albarracin. 2007. *Chapter 1. Predicting and Changing Behavior: A Reasoned Action Approach*. Prediction and Change of Health Behaviour, Applying the Reasoned Action Approach. New Jersey: Lawrence Erlbaum

Albrechtsen, Eirik. 2007. A qualitative study of users' view on information security. *Computers & security* 26,. (4): 276-289.

Bandura, Albert., Nancy E. Adams, and Janice Beyer.1977.*Cognitive processes mediating behavioral change. Journal of personality and social psychology*35,. (3) : 125.

Bandura, Albert. 1986. Social foundations of thought and action: A social cognitive theory. *Englewood Cliffs, NJ, US: Prentice-Hall, Inc*.

Bang, Youngsok, Dong-Joo Lee, Yoon-Soo Bae, and Jae-Hyeon Ahn. 2012. *Improving information security management: An analysis of ID–password usage and a new login vulnerability measure.* international journal of information management 32,.(5) : 409-418.

Bies, R.., and R. Moag. 1986. *Interactional justice: Communication criteria of fairness in*: RJ Lewicki, BH Sheppard, MH Bazerman (eds.) Research on negotiations in organizations (pp. 43-55).

Brancheau, James C., Brian D. Janz, and James C. Wetherbe.1996. *Key issues in information systems management: 1994-95 SIM Delphi results.* MIS quarterly : 225-242.

Bulgurcu, Burcu. 2008. The antecedents of information security policy compliance. (MSc thesis). *Canada: The University of British Columbia*.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2009. *Roles of information security awareness and perceived fairness in information security policy compliance.* AMCIS 2009 Proceedings : 419.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010a. *Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness.* MIS quarterly 34,. (3) : 523-548.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat.2010b. *Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: an empirical investigation*. In System Sciences (HICSS), 2010 43rd Hawaii International Conference on, pp. 1-7. IEEE,.

Chambliss, Catherine, and Edward J. Murray. 1979. *Cognitive procedures for smoking reduction: Symptom attribution versus efficacy attribution*. Cognitive Therapy and Research 3,. (1): 91-95.

Chan, Mark, Irene Woon, and Atreyi Kankanhalli.2005. *Perceptions of information security in the workplace: linking information security climate to compliant behavior.* Journal of information privacy and security 1,. (3) : 18-41.

Compeau, Deborah R., and Christopher A. Higgins.1995. *Computer self-efficacy: Development of a measure and initial test.* MIS quarterly : 189-211.

D'Arcy, John, Anat Hovav, and Dennis Galletta. 2009. *User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach*. Information Systems Research 20,. (1) : 79-98.

Elffers, Henk, Peter Van Der Heijden, and Merlijn Hezemans. 2003. *Explaining regulatory non-compliance: A survey study of rule transgression for two Dutch instrumental laws, applying the randomized response method*. Journal of Quantitative Criminology 19,. (4) : 409-439.

Fishbein Martin and Ajzen, Icek,.1975. *Belief, attitude, intention and behavior: An introduction to theory and research*.

Fishbein, Martin.2007. A reasoned action approach: Some issues, questions, and clarifications. *Prediction and change of health behavior: Applying the reasoned action approach* : 281-295.

Fishbein, Martin, and Marco C. Yzer.2003. *Using theory to design effective health behavior interventions.* Communication theory 13,. (2) : 164-183.

Fornell, Claes., and Larcker, David F. 1981. *Evaluating Structural Equation Models with Unobservable Variables and Measurement Erro*., Journal of Marketing Research (18:1), pp. 39-50.

Glanz, Karen, Barbara K. Rimer, and Kasisomayajula Viswanath, eds.2008. *Health behavior and health education: theory, research, and practice*. John Wiley & Sons,.

Hair Joseph .F., Black, Bill ., Babin, Barry .J., Anderson Rolph,. E., & Tatham, Ronald,. L. 2006. *Multivariate Data Analysis* (6th ed.). New Jersey: Pearson

prentice Hall.Herath, Tejaswini, and H. Raghav Rao.2009. *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.* Decision Support Systems 47,. (2) : 154-165.

Ifinedo, Princely. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31,(1) : 83-95.

Ifinedo, Princely. 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management* 51.(1) : 69-79.

Isf, I. S. F. 2003. The Standard of Good Practices for Information Security. *In USA: Information Security Forum ISF*.

Jex, Steve M., and Terry A. Beehr. 1991. *Emerging theoretical and methodological issues in the study of work-related stress.* Research in personnel and human resources management 9,. (31) : l-365.

Kajtazi, Miranda, and Burcu Bulgurcu. 2013.*Information security policy compliance: An empirical study on escalation of commitment*.

Krejcie, Robert V., and Daryle W. Morgan. 1970. *Determining sample size for research activities*. Educational and psychological measurement 30. (3) : 607-610.

Kreps, David M. 1997. The interaction between norms and economic incentives. In AEA Papers and Proceedings, pp. 359-364..

Kim, Sang Hoon, Kyung Hoon Yang, and Sunyoung Park.2014. *An integrative behavioral model of information security policy compliance*. The Scientific World Journal 2014 .

Kirsch, Laurie, and Scott Boss. 2007. *The last line of defense: motivating employees to follow corporate security guidelines*. ICIS 2007 Proceedings: 103.

Madden, Thomas J., Pamela Scholder Ellen, and Icek Ajzen.1992. *A comparison of the theory of planned behavior and the theory of reasoned action*. Personality and social psychology Bulletin 18,. (1) : 3-9.

McCarthy, Bill. 2002. New economics of sociological criminology. *Annual Review of Sociology* 28,. (1) : 417-442.

Ostroff, Cheri, and David E. Bowen.2002. *Moving HR to a higher level: HR practices and organizational effectiveness*.

Pahnila, Seppo, Mikko Siponen, and Adam Mahmood.2007. *Employees' behavior towards IS security policy compliance.* In System sciences, 2007. HICSS

2007. 40Th annual hawaii international conference on, pp. 156b-156b. IEEE, .

Paternoster, Ray, and Greg Pogarsky.2009. *Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices.* Journal of Quantitative Criminology25,. (2) : 103-127.

Post, Gerald V., and Albert Kagan. 2007. *Evaluating information security tradeoffs: Restricting access can interfere with user tasks*. Computers & Security 26,. (3) : 229-237.

Ransbotham, Sam, and Sabyasachi Mitra. 2009. *Choice and chance: A conceptual model of paths to information security compromise*. Information Systems Research 20,. (1) : 121-139.

Rogers, Everett M. 2003. Diffusion of Innovations (5th ed.), New York: Free Press.

Sharma, Manoj. 2010. *Theoretical foundations of health education and health promotion.*

Siponen, Mikko T. 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security* 8,. (1) : 31-41.

Siponen, Mikko, M. Adam Mahmood, and Seppo Pahnila. 2014. *Employees' adherence to information security policies: An exploratory field study*. Information & management 51,.(2) : 217-224.

Siponen, Mikko, Seppo Pahnila, and M. Adam Mahmood. 2010. *Compliance with information security policies: An empirical investigation*. Computer 43,.(2) .

Tolman, Edward C. 1932. Purposive behavior in man and animals. *New York: Appleton-Century-Crofts* .

Vance, Anthony, Mikko Siponen, and Seppo Pahnila. 2012.*Motivating IS security compliance: insights from habit and protection motivation theory*. Information & Management 49,.(3-4) : 190-198.

Factors Influencing Employees' Compliance with Information Security Policy in Organization

Abstract

Today, risks related to information security are a major challenge for many organizations, since these risks may have direct consequences, including loss of credibility and monetary damage. Statistics suggest that damages the information systems security is increasing. Many organizations recognize that their employees, who are often considered the weakest link in information security, can also be great assets in the effort to reduce risk related to information security. There is not significant research on the human aspect of information systems security and practice. Hence the purpose of this study was to examine factors influencing the employee compliance with information systems security policy in organization. To this end, 221 persons (including staff of 5 different organizations) were selected with the proportional method. After collecting the data, hypotheses were analyzed through confirmatory factor analysis and structural equation modeling using AMOS software. The results showed that self-efficacy and attitude about the compliance have the most effects on the intention to comply with information security policy in organization.

Keywords: Information security awareness, Information security, Information systems, Information security policy, Compliance.