فصلنامه علمی پژوهشی
دانش حسابداری و حسابرسی مدیریت
دوره ۱۵/ شماره ۲ (پیاپی ۵۸)/ تابستان ۱۴۰۵
صفحه ۵۳۷ تا ۵۴۷

تبیین ارتباط میان ارزیابی تهدید امنیت ، ترس و انگیزه حفاظت از سیستم های اطلاعاتی حسابداری : آزمون نظریه روانشناسی مثبت گرا

علی ترچانی نارنج بن
دانشجوی دکتری حسابداری ، گروه حسابداری، واحد قزوین ، دانشگاه آزاد اسلامی ، قزوین ، ایران

فرزین رضایی
دانشیار گروه حسابداری، واحد قزوین ، دانشگاه آزاد اسلامی ، قزوین ، ایران
(نویسنده مسئول)
Farzin.rezaei@iau.ac.ir

مهدی بشکوه
استادیار گروه حسابداری، واحد قزوین ، دانشگاه آزاد اسلامی ، قزوین ، ایران

تاریخ دریافت: ۱۴۰۳/۰۹/۱۱ تاریخ پذیرش: ۱۴۰۳/۱۱/۱۶

چکیده

هدف اصلی این تحقیق آن است تا روابط میان ارزیابی تهدید امنیت ، ترس و انگیزه حفاظت از سیستم های اطلاعاتی درمیان حسابداران و مدیران مالی را مورد مطالعه قرار دهد. جامعه آماری تحقیق شامل حسابداران و مدیران مالی شاغل شرکت های پذیرفته شده در بورس اوراق بهادار تهران است. از این جامعه ، نمونه ای بالغ بر ۴۰۷ نفر به صورت تصادفی انتخاب شده است. روش تحقیق برای جمع آوری مبانی نظری تحقیق ، روش کتابخانه ای و برای جمع آوری داده های تحقیق پیمایشی و پرسش نامه ای می باشد. یافته های این تحقیق نشان می دهد با افزایش درک افراد از تهدید علیه سیستم های اطلاعاتی حسابداری، انگیزه آن ها برای حفاظت از سیستم اطلاعاتی به طور معنی داری افزایش می یابد. هم چنین یافته های تحقیق تایید می نمایند که با افزایش درک افراد از ارزیابی تهدید علیه سیستم های اطلاعاتی حسابداری ، ترس آن ها کاهش و در نهایت با افزایش ترس افراد ، انگیزه آن ها برای حفاظت از سیستم اطلاعاتی نیز به طور معنی داری کاهش می یابد.

واژه‌های کلیدی: سیستم های اطلاعاتی ، تهدید امنیت و ترس.

۱- مقدمه

در دهه های اخیر سرقت اطلاعات و سوء استفاده از داده ها یکی از نگرانی های صاحبان صنایع و بنگاه های مالی و اقتصادی است. از این رو، امنیت اطلاعات سیستم های کامپیوتری موضوع و چالش با اهمیتی است که سازمان ها با آن روبرو هستند. هر چند در سال های اخیر پیشرفت های چشمگیری در حفاظت از اطلاعات و امنیت داده ها در سیستم های اطلاعاتی حسابداری رخ داده است. اما علی رغم این پشرفت ها ، به دلیل رشد فن آوری اطلاعات و پیچیدگی سیستم های نرم افزاری ، امنیت سیستم های اطلاعاتی هم چنان در حال تهدید است(موسوی و لگزیان، ۱۳۹۷). مدیران و حسابداران، اطلاعات حسابداری حاصل از سیستم های اطلاعاتی را بسیار ارزشمند و سودمند می دانند و برای حفظ و نگهداری سیستم های اطلاعاتی ، و خطراتی که این سیستم ها را تهدید می کنند باید آگاهی کافی داشته باشند. از سوی دیگر ، با توجه به افزایش روزافزون تقلب هاو جرایم رایانه ای ، ضروری است حسابداران ومدیران که نقش کلیدی در طراحی سیستم های اطلاعاتی دارند با ماهیت تقلب و فرایندی که افراد برای انجام تقلب و مخفی سازی آن انجام می دهندآگاه باشند. مطالعات قبلی نشان داده‌اند عواملی چون تجربه کاربر، آموزش کاربر، حمایت مدیریت از جمله عوامل انسانی اثرگذار بر امنیت اطلاعات می‌باشند (باغانی و همکاران، ۱۴۰۳). در مطالعه ای دیگر نشان داده شد آگاهی مدیران، حسابداران و حسابرسان از عوامل تهدیدکننده سیستم‌های اطلاعاتی حسابداری نقش با اهمیتی در پیشگیری از تهدیدهای امنیتی دارد(واعظ و احمدی؛ ۱۳۹۲). در مطالعه ای دیگر تجویدی و احمدی (۱۳۹۹) نیز دریافتند توانایی های شرکت در مدیریت فناوری اطلاعات، موجب بهبود عملکرد سیستم اطلاعاتی حسابداری می شود. نوآوری پژوهش حاضر در مقایسه با پژوهش های قبلی آن است که بر اساس نظریه روانشناسی مثبت گرا، انگیزه حفاظت از سیستم های اطلاعاتی حسابداری مورد مطالعه و بررسی قرار می دهد. از این رو، هدف اصلی این مقاله آن است تا روابط میان ارزیابی تهدید امنیت ، ترس و انگیزه حفاظت از سیستم های اطلاعاتی درمیان حسابداران و مدیران مالی مورد بررسی قرار دهد. هم چنین ارزش افزوده علمی مقاله حاضر این است که به عنوان یک مطالعه میان رشته ای می تواند خلاء های پژوهش های رفتاری در سیستم های اطلاعاتی حسابداری را تا حدودی برطرف و موجب بسط مبانی نظری مطالعات رفتاری در سیستم اطلاعاتی حسابداری شود. ادامه مقاله به مبانی نظری، روش شناسی ، یافته ها و نتیجه گیری اختصاص دارد.

۲- مبانی نظری و پیشینه تحقیق

۲-۱- روانشناسی مثبت گرا

این شاخه از روانشناسی بر توانمندی ها ، قابلیت ها و فضایل افراد در بهبود عملکرد تاکید دارد و به بررسی ویژگی ها و هیجانات مثبت و ویژگی های مثبت شخصیتی مانند هوش هیجانی ، خودکارآمدی ، اعتماد و....بر ارتقای عملکرد فردی و سازمانی می پردازد. به عنوان نمونه کارکنانی که از خودکارآمدی بالایی برخوردار هستند، معمولاً در مقابل تغییرات در فن آوری اطلاعات ، از توانایی بالایی در پذیرش آن تغییرات برخوردار هستند.بنابراین، روانشناسی مثبت گرا می تواند از طریق برنامه های توسعه منابع انسانی این قابلیت را در کارکنان شکوفا نماید(رفاهی بخش و همکاران، ۱۳۹۸). پژوهش در زمینه امنیت اطلاعات نیز تایید می نماید خودکارآمدی، نگرش، باورها و عادات هنجاری تأثیر مثبت و معنی داری با رفتارهای حفاظت از اطلاعات دارد(شارما[1] و همکاران، ۲۰۲۱).

۲-۲- ارزیابی از تهدید و حفاظت از امنیت سیستم‌های اطلاعاتی

مطالعات نشان می دهد هرگاه کارکنان به این نتیجه برسند که سیستم های اطلاعاتی شرکت با تهدید امنیتی روبرو است، تلاش می کنند تا آن تهدیدات را کاهش و با آن مقابله می نمایند. شواهد نشان می دهد هر چه شدت تهدیدات بالقوه امنیت اطلاعات بیشتر باشد، آن گاه نگرش کارکنان نسبت به پیروی از سیاست‌های امنیت اطلاعات نیز افزایش می یابد(سی پونن[2] و همکاران ، ۲۰۱۴). در پژوهشی دیگر نتایج نشان داد کمتر از واقع جلوه دادن تهدید امنیت سیستم های اطلاعاتی می تواند انگیزه کارکنان را از حفاظت از آن سیستم ها را کاهش دهد. اما اگر وقتی کاربران بر این باور باشند که کنترل یک تهدید امنیتی را در کنترل خود دارند، کمتر احتمال دارد که با این موضوع بر اساس هیجانات و احساسات خود مقابله کنند(تامپسن[3] و همکاران، ۲۰۲۴). شواهد مطالعه لی[4] و همکاران (۲۰۲۳) در بررسی تهدیدات امنیتی سیستم بلاک چین بیانگر آن است که شاخص‌های ارزیابی امنیت بلاک چین و روش‌های ارزیابی آن می‌تواند به ارزیابی امنیت و اعتبار سیستم‌های بلاک چین و تعیین اقدامات امنیتی مربوطه کمک کنند.

[1] Sharma
[2] Siponen
[3] Thompson
[4] Li

بر اساس آن چه که درباره ارتباط میان ارزیابی تهدید و انگیزه حفاظت از امنیت سیستم‌های اطلاعاتی حسابداری عنوان شد ، فرضیه اول به صورت زیر نوشته می شود:

فرضیه اول: ارزیابی کارکنان از تهدید امنیت سیستم‌های اطلاعاتی بر انگیزه حفاظت از امنیت سیستم‌های اطلاعاتی حسابداری تاثیر معنی داری دارد.

۳-۲- ارزیابی تهدید از امنیت سیستم‌های اطلاعاتی و ترس کارکنان

شی[1] و همکاران (۲۰۲۴) طی پژوهشی دریافتند با افزایش درک از تهدیدات هوش مصنوعی در صنعت پزشکی اعتماد بیماران از خدمات پزشکی کاهش و ترس آن ها از پیامدهای نامطلوب هوش مصنوعی افزایش می یابد. لزتاری[2] و همکاران (۲۰۲۴) نیز نشان دادند هرگاه مشتریان بانک به این نتیجه برسند که احتمال تهدیدهای امنیتی از جمله تجربه کلاهبرداری در سیستم های آنلاین بانک ها وجود دارد ، در آن صورت ترس آن ها از جرایم سایبری و بی اعتمادی به خدمات بانکداری آنلاین به طور فزاینده ای افزایش می یابد. نتایج پژوهش ون زونن[3] و همکاران (۲۰۲۲) نشان می‌دهد هرگاه کارکنان احساس نمایند که استفاده از فن آوری های اطلاعاتی نظیر شبکه های اجتماعی تهدیدی برای از دست دادن شغل آن ها باشد ، در آن صورت ترس از پاسخ گویی در آن ها ایجاد می شود و استفاده از رسانه‌های اجتماعی سازمانی را محدود می نمایند. یافته های شارما[4] و همکاران (۲۰۲۱) بیانگر آن است که با افزایش درک کارکنان از ریسک‌های امنیت اطلاعات، ترس آن ها از خطرات سایبری افزایش می یابد. این موضوع باعث می شود تا انگیزه بیشتری ، برای حفاظت از سیستم های اطلاعاتی داشته باشند.

بر اساس آن چه که درباره ارتباط میان ارزیابی تهدید از امنیت سیستم‌های اطلاعاتی و ترس کارکنان بیان شد، فرضیه دوم به صورت زیر نوشته می شود:

فرضیه دوم: ارزیابی کارکنان از تهدید امنیت سیستم‌های اطلاعاتی بر ترس آن ها از خطرات امنیتی تاثیر معنی داری دارد.

۴-۲- ترس کارکنان و انگیزه حفاظت از امنیت سیستم‌های اطلاعاتی

گانی و اسمیت (۲۰۲۴) معتقدند ترس کارکنان از خطرات حملات سایبری تاثیر معنی داری بر فرایندهای شناختی آن ها می گذارد و این موضوع می‌تواند به طور بالقوه بر اثربخشی اقدامات برای حفاظت از امنیت سیستم های اطلاعاتی تأثیر بگذارد. میلز و همکاران (۲۰۲۴) دریافتند تمایل به استفاده از سیستم هشدار امنیتی گوشی همراه تحت تأثیر ارزیابی افراد از یک تهدید اضطراری و درک آنها از نحوه استفاده از این سیستم برای مقابله مؤثر است. ترس و شدت تهدید درک شده، انگیزه های مهم استفاده از سیستم هشدار امنیتی گوشی همراه هستند. اما، زمانی که تأثیرات منفی نگرانی در مورد حفظ حریم خصوصی به اندازه کافی قوی باشد، افراد با وجود آگاهی از خطرات، استفاده از این سیستم هشدار منصرف می شوند.

فنگ (۲۰۱۷) معتقد است ترس به عنوان یک احساس قدرتمند و فراگیر انسانی، اجتناب و رویکرد را تشویق می کند و ممکن است بر طیف گسترده ای از رفتارهای سازمانی، از جمله ارتباطات، اشتراک دانش و استفاده از فناوری تأثیر بگذارد. بر اساس آن چه که گفته شده فرضیه سوم به صورت زیر نوشته می شود:

فرضیه سوم: ترس کارکنان از تهدیدهای امنیتی ، بر انگیزه آن ها از حفاظت از سیستم های اطلاعاتی حسابداری تاثیر معنی داری دارد.

۵-۲- پیشینه خارجی

وفایی زاده و همکاران (۲۰۲۴) دریافتند آسیب پذیری درک شده، نفوذ به حریم خصوصی و آگاهی از حریم خصوصی به طور قابل توجهی بر تهدیدات درک شده از خطرات سایبری تأثیر می گذارد، در حالی که دانش فنی بر تهدیدات مذکور تأثیر نمی گذارد. علاوه بر این، مشخص شد که اثربخشی واکنش و خودکارآمدی هر دو آگاهی امنیت سایبری را افزایش می‌دهند. در حالی که تهدیدات درک شده تأثیری بر آن ندارند. ژن[5] و همکاران (۲۰۲۴) تاثیر عوامل مختلف را به عنوان موانع پذیرش سیستم اطلاعاتی بررسی نمودند. آن ها این عوامل را به سه نوع عمده دسته بندی نمودند که شامل حملات خارجی (حملات فیشینگ و باج افزار)؛ عوامل انسانی، از جمله کمبود مهارت و موضوع سوء استفاده از اطلاعات؛ و عوامل فن آوری، از جمله پیچیدگی و آسیب پذیری. به عقیده آن ها حملات خارجی و عوامل فن‌آوری موانع اصلی پذیرش سیستم‌های اطلاعاتی هستند. اما عامل انسانی تأثیر قابل‌توجهی بر پذیرش سیستم‌های اطلاعاتی ندارد. تاکور[6] (۲۰۲۴) معتقد است که برای جلوی گیری از تهدیدهای امنیتی باید اقدامات پیشگیرانه ای از

[1] Xu
[2] Lestari
[3] Van Zoonen
[4] Sharma
[5] Zhan
[6] Thakur

جمله امنیت قوی شبکه، روش‌های کدگذاری ایمن، آموزش کاربر، رمزگذاری، کنترل‌های دسترسی انجام شود. با استفاده از راه حل های توصیه شده و ترویج فرهنگ آگاهی از امنیت سایبری، مردم و سازمان ها می توانند با اطمینان در عصر دیجیتال حرکت کنند و از خود در برابر محیط دائماً در حال تحول خطرات سایبری محافظت کنند. یزدان مهر و همکاران (۲۰۲۳) نشان دادند ترس از به امنیت اطلاعات، خودکارآمدی کارکنان و حمایت سازمانی از حفاظت از سیستم های اطلاعاتی را تحت تاثیر خود قرار می دهد. به عبارت دیگر مقابله متمرکز با مشکل نقض امنیت اطلاعات را کاهش می دهد. بالیکا[1] (۲۰۲۳) در پژوهشی نشان داد فناوری‌های دیجیتال تاثیر قابل توجهی بر بهبود سیستم اطلاعات حسابداری حامی فرآیندهای تصمیم‌گیری دارد. به عقیده او امکان استفاده از فناوری های دیجیتال در سیستم اطلاعات حسابداری، می تواند تحول در سیستم اطلاعات حسابداری ایجاد نماید. جرح[2] و همکاران (۲۰۲۳) طی مطالعه ای در اردن تأثیر سیستم کنترل داخلی در بانک های اسلامی بر رابطه بین سیستم اطلاعات حسابداری و عملکرد کارکنان را مورد بررسی قرار داد. آن ها دریافتند رابطه ای معنی دار میان یک کیفیت اطلاعات، کیفیت سیستم اطلاعات حسابداری و کیفیت خدمات و عملکرد کارکنان وجود دارد. آن ها نتیجه گیری می کنند که سیستم کنترل داخلی در بانک های اسلامی بر رابطه بین سیستم اطلاعات حسابداری و عملکرد کارکنان تاثیر معنی دار دارد. به عقیده توماس و سول[3] (۲۰۲۲) با گسترش فضای سایبری، خطرات بیشتری این فضا را تهدید می کند، زیرا تکنیک‌های حفاظتی سنتی ناکافی هستند و عموماً بر محیط سازمان تمرکز دارند. علاوه بر این، حملات سایبری هم چنان در پیچیدگی رشد می‌کنند و پیامدهای بزرگی را ایجاد می‌کنند. رویکردها و بهترین شیوه‌های امنیت سایبری موجود ، و استراتژی‌های پیاده‌سازی، با قدرت و تمرکز متفاوت، در سطوح مختلف جزئیات محدود هستند. لهنچک[4] و همکاران (۲۰۲۲) طی یک پژوهش پیشنهاد دادند حفاظت از اطلاعات حسابداری و پرهیز از حملات سایبری تنها در صورتی امکان‌پذیر است که اقدامات جامع و اقدامات مشترک مدیریت، حسابداری، حسابرسان و مؤسسات آموزشی در تربیت متخصصان مورد نیاز باید دنبال شود. به نظر آن ها، کنترل دسترسی غیرمجاز به سوابق حسابداری جزء مهم کنترل داخلی است. خط‌مشی‌های دسترسی و رمز عبور، رمزگذاری، امضای دیجیتال، قفل‌های دیسک و گواهی‌های دیجیتال نمونه‌هایی از کنترل‌هایی هستند که باید هنگام ارزیابی اثربخشی کنترل شناسایی، مستندسازی، برقراری ارتباط و آزمایش شوند.

۲-۶- پیشینه داخلی

رحمانیان کوشککی (۱۴۰۴) نشان دادند نرم افزارهای حسابداری مورد استفاده در شرکت های مورد بررسی، از نظر ویژگی های عمومی، سازگاری، انعطاف پذیری، کنترل های داخلی، آموزش و ساختار گزارش دهی دارای وضعیت مطلوبی بوده و این ویژگی ها در نرم افزارهای مورد استفاده لحاظ گردیده است. با توجه به رتبه بندی عوامل مؤثر در ارزیابی پیاده سازی نرم افزارهای حسابداری در شرکت ها، ساختار گزارش دهی دارای بیشترین اهمیت و کنترل داخلی از پایین ترین اهمیت در مقایسه با سایر عناصر برخوردار است. اخوان و همکاران (۱۴۰۳) طی پژوهشی با رویکرد فراترکیب مطالعات انجام شده در حوزه امنیت اطلاعات نشان داد که همسویی استراتژیک، مدیریت ریسک ، مدیریت منابع و اندازه گیری درست به درک صحیح حکمرانی امنیت سیستم های اطلاعاتی کمک می کند. فارسی و همکاران (۱۴۰۳) سیستم اطلاعات حسابداری مبتنی بر معماری بلاک چین به روش کیفی و تحلیل مضمون را مورد بررسی قرار دادند. نتایج آن ها نشان داد کدهای تضمین تعهدات، بهبود اقدامات مرکز عملیات امنیت و دسترسی دائمی بالاترین ضرایب اهمیت را در عوامل علی، تضاد با پلتفرم‌های موجود، مقیاس‌پذیری و فقدان خزانه استعداد در بخش عوامل مداخله‌گر، بهبود امنیت داده‌ها، امنیت سوابق و مدیریت هویت دیجیتال در بخش پیامدها دارای بیشترین ضریب اهمیت هستند. محمدی ارسی و ریاحی نیا(۱۴۰۲) امنیت اطلاعات کتابخانه های دیجیتال را مورد بررسی قرار دادند. یافته های آن ها نشان داد مؤلفه‌های سطح دسترسی، امنیت و فناوری، ارائهٔ خدمات و زیرساخت در وضعیت مناسب و مؤلفه‌های حفاظت اطلاعات و محرمانگی اطلاعات در وضعیت نامناسبی به لحاظ امنیت اطلاعات اینترنت اشیاء در کتابخانه‌های دیجیتال قرار دارند.آن ها نتیجه گیری می کنند امنیت یکی از چالش‌های کلیدی فناوری اطلاعات بوده و مسائل مربوط به امنیت اطلاعات در بستر اینترنت اشیاء در کتابخانه‌های دیجیتال بسیار حائز اهمیت است. گیلانی نیای صومعه سرایی و همکاران (۱۴۰۲) طی تحقیقی نشان دادند افزایش به کارگیری سیستم های اطلاعاتی حسابداری یکپارچه در سازمان‌های دولتی منجر به ارتقا مولفه های کیفیت اطلاعات، کیفیت خدمات، کیفیت آموزش، افزایش شفافیت، بهبود

[1] Balicka
[2] Jarah
[3] Thomas & Sule
[4] Lehenchuk

استراتژی و تسریع انجام وظایف می گردد و در نتیجه بهبود عملکرد سازمانی و کاهش تخلفات سازمانی را در پی دارد. رحیمی هلری و همکاران (۱۴۰۱) دریافتند تنوع در فرایندهای پردازشی، وجود اطلاعات متناقض و پیچیدگی اطلاعات در سازمان، تنوع در ابزارهای تحلیلی، خطر دستبرد اطلاعات و آسیب های ناشی از ویروس و خرابی نرم افزارها و سخت افزارها، وجود تنوع در سبک استفاده از مدیریت سیستم های اطلاعاتی حسابداری مدیریت، نیاز به ارزیابی عملکرد حوزه های مختلف، وجود ریسک سرمایه گذاری و انتخاب پروژه، امکان گزارش دهی و گزارشگری آسان، قابلیت سازگار کردن داده های متنوع، فراهم کردن اطلاعات کافی و گسترش دامنه اطلاعات در سازمان از جمله عوامل تاثیرگذار هوش تجاری بر سیستم های اطلاعاتی است. عزیزی و همکاران (۱۴۰۰) نشان دادند ویژگی‌های سیستم اطلاعات حسابداری بر عملکرد سیستم تأثیر دارد. همچنین آن ها دریافتند عدم تمرکز سازمانی، تأثیر ویژگی‌های سیستم اطلاعات حسابداری بر عملکرد سیستم را تعدیل می‌کند. در نهایت آن ها نتیجه گیری می کنند عدم‌اطمینان‌کاری، تأثیر ویژگی‌های سیستم اطلاعات حسابداری بر عملکرد سیستم را تعدیل می‌کند. محمد نژاد و همکاران (۱۳۹۹) نشان دادند انعطاف پذیری نرم افزارهای حسابداری بر پاسخگویی به ذی نفعان داخلی و خارجی شرکت تأثیرگذار است. رستمی مازویی و همکاران (۱۳۹۸) به بررسی اثرات کنشگران فنی و انسانی بر کارکردهای سیستم اطلاعاتی حسابداری مدیریت با استفاده از نظریه شبکه کنشگران پرداختند. نتایج حاصل از پژوهش آن ها نشان داد کنشگران فنی و انسانی نقش مؤثری در بهبود کارکردهای نظام حسابداری مدیریت ایفا می نمایند. برخلاف رویکرد سنتی متداول، در رویکرد کنشگری این بازیگران به عنوان مداخله گرانی که توانایی تأثیر و تغییر تصمیم های استراتژیک دارند . به عقیده آن ها الگوهای برنامه ریزی، کنترل و ارزیابی به عنوان وظایف حسابداری مدیریت فراتر از بخش های مالی تغییر و توسعه یافته است . صدری و همکاران (۱۳۹۷) دریافتند شاخص های رعایت اصول و قواعد، تأمین زیرساختها؛ منابع انسانی؛ اصول سیستمهای اطلاعاتی؛ رعایت اصول ایمنی و کنترل و تدوین ساختارهای مورد نیاز شاخصهای اولیه و کلی برای ارائه مدل ارتباط کنشگران در سیستمهای اطلاعاتی حسابداری می باشند. از میان این شاخص ها، شاخص رعایت اصول و قواعد، تأمین زیرساختها، تدوین ساختارهای مورد نیاز، اصول سیستمهای اطلاعاتی، رعایت اصول ایمنی و کنترل و منابع انسانی به ترتیب الویت قرار دارند. صالحی و نوروزی (۱۳۹۴) به بررسی مطالعه تجربی پذیرش نرم افزارهای حسابداری در میان دانشجویان پرداختند. نتایج نشان داد که سهولت مشاهده شده در استفاده از برنامه ها تأثیر مثبت بر تمایل به استفاده ندارد و تمایل به استفاده نیز دارای تأثیر مثبت بر استفاده حقیقی سیستمی از برنامه های حساب داری می باشد. چگونیان و همکاران (۱۳۹۲) به ارزیابی سیستم های اطلاعاتی حسابداری از دیدگاه کاربران پرداخته اند. نتایج نشان داد که پژوهش های متعددی در ارتباط با کیفیت سیستم های اطلاعاتی و رضایت مندی کاربران صورت می گیرد و هدف طراحان این سیستم ها، نیل به اهداف از پیش تعیین شده ای است که برای این سیستم ها در نظر گرفته اند، ضمن اینکه تاکید ویژه ای بر روی سیستم های تحت وب وجود دارد، لیکن دستیابی به این اطلاعات در ایران به سختی صورت می گیرد و گاهی غیر ممکن می شود. صالحی و حاجی زاده(۱۳۸۹) به بررسی سواد عمومی کامپیوتری کارکنان پرداختند. نتایج نشان داد که به طور کلی میزان سواد عمومی کامپیوتری تمامی زیرگروه ها پایین تر از حد متوسط می باشد. تمامی زیر گروه های سواد عمومی کامپیوتری پیش بینی کننده های معنی داری برای سواد کامپیوتری بودند. علیپور و همکاران (۱۳۸۹) به بررسی ارزیابی نرم افزارهای حسابداری بر اساس ویژگی های سیستم های اطلاعاتی حسابداری پرداختند. نتایج نشان داد که در خصوص شناخت میزان تأثیر برخی از متغیرهای مورد مطالعه، همگی به جز ساختار گزارش دهی دارای ویژگی های یک سیستم اطلاعاتی حسابداری مناسب می باشند. همچنین، کلیه فرضیه های پژوهش حاکی از عدم دلالت و تأثیر دو ویژگی کنترل و سازگاری در نوع فعالیت شرکت ها و انعطاف پذیری در تعداد نیروی انسانی را داشتند.

۳-روش‌شناسی پژوهش

مبانی‌نظری پژوهش بر اساس مطالعات کتابخانه‌ای و جمع‌آوری داده‌های تحقیق بر اساس روش پیمایشی و با استفاده از پرسش-نامه انجام شده‌است.اندازه گیری متغیرها بر اساس پرسش نامه برنز[1] و همکاران (۲۰۱۷) انجام شده است. جامعه آماری شامل کارشناسان حسابداری و مدیران مالی شاغل در شرکت های پذیرفته شده در بورس اوراق بهادار است. از این جامعه ، نمونه ای شامل ۴۰۷ نفر انتخاب گردید. برای تعیین حجم نمونه از فرمول کوکران به شرح زیر استفاده شده است:

$$n = \frac{Z_{\frac{\alpha}{2}}^2 pq}{d^2}$$

[1] Burns

در این فرمول:

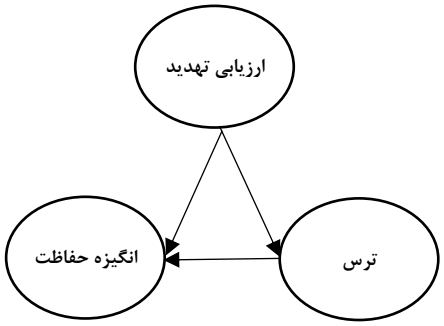
n =تعداد نمونه

$Z^{\frac{\alpha}{2}}$ =۱/۹۶ مقدار نرمال استاندارد یعنی

P=q=0/5

d=0/1

تعداد نمونه آماری به دست آمده مطابق با فرمول بالا ۹۶ می باشد که در این تحقیق تعداد ۴۵۰ پرسش نامه به صورت تصادفی میان مشارکت کنندگان توزیع و ۴۰۷ نسخه آن دریافت شد. آزمون فرضیه‌های پژوهش بر اساس معادلات ساختاری و با بکارگیری نرم افزار Smart PLS انجام شده‌است. مدل پژوهش نیز به صورت نمودار(۱) تدوین می‌گردد.



نمودار(۱) : مدل پژوهش

متغیر وابسته در این تحقیق انگیزه حفاظت از سیستم های اطلاعاتی حسابداری و متغیر مستقل و واسطه ای به ترتیب ارزیابی تهدید علیه سیستم اطلاعاتی حسابداری و ترس کارکنان از تهدید می باشد. پایایی متغیرهای پژوهش در جدول شماره ۱ آورده شده است. شواهد این جدول نشان می دهد که متغیرهای پژوهش از پایایی لازم برخوردار هستند.

جدول شماره ۱: روایی و پایایی متغیرهای پژوهش

	Cronbach'sAlpha	rho_A	CR	AVE
ارزیابی تهدید	۰/۸۴۸	۰/۸۵۷	۰/۹۱۳	۰/۵۴۵
ترس	۰/۸۱۶	۰/۸۱۳	۰/۸۹۸	۰/۵۳۷
انگیزه حفاظت	۰/۹۱۷	۰/۹۳۵	۰/۹۰۴	۰/۵۲۹

۴- یافته های پژوهش

۴-۱- آمار توصیفی

نتایج مربوط به آمار توصیفی در جدول شماره ۲ ارائه شده است. این جدول نشان می دهد که میانگین ارزیابی تهدید ۳۹/۱۴ می باشد. با توجه به این که مقدار بیشنه این متغیر ۶۰ است، میانگین مزبور بیشتر از حد متوسط آن است. میانگین ترس از خطرات تهدید کننده و انگیزه حفاظت از سیستم های حسابداری به ترتیب ۱۱/۴۷ و ۱۷/۶ بیشتر از حد متوسط آن و بالا است.

جدول شماره۲ : آمار توصیفی

متغیرها	میانگین	انحراف معیار	میانه	کمینه	بیشینه
ارزیابی تهدید	۳۹/۱۴	۴۰	۱۲/۶۷	۱۵	۶۰
ترس	۱۱/۴۷	۱۰	۳/۵۰۶	۴	۲۰
انگیزه حفاظت	۱۷/۶	۱۷	۱/۵۵۳	۱۴	۲۰

۴-۲- آزمون فرضیه ها

نتایج آزمون فرضیه ها در جدول ۳ نشان داده شده است. طبق شواهد این جدول از آن جایی که سطح معنی داری تمام مسیرها، کمتر از پنج درصد است، لذا با اطمینان ۹۵ درصد می توان نتیجه گرفت که تمام فرضیه ها تایید می شود. نتایج نشان می دهد هرگاه کارکنان به این نتیجه برسند که تهدید علیه سیستم های اطلاعاتی حسابداری جدی است ، در آن صورت انگیزه آن ها برای حفاظت از سیستم اطلاعاتی افزایش می یابد. هم چنین با افزایش ارزیابی تهدید علیه سیستم های اطلاعاتی حسابداری ، ترس کارکنان کاهش می یابد. در نهایت با افزایش ترس کارکنان ، انگیزه آن ها برای حفاظت از سیستم اطلاعاتی کاهش می یابد.

جدول ۳ . آزمون فرضیه ها

مسیر	ضریب مسیر	انحراف استاندارد	آماره t	سطح معنی داری	اندازه اثر
ارزیابی تهدید ← انگیزه حفاظت	۰/۰۲۷	۰/۰۸۱	۱۰۲/۲۱۳	۰/۰۰۰	۴/۳۲۹
ارزیابی تهدید ← ترس	-۰/۴۵۵	۰/۰۳۹	۱۱/۸۰۱	۰/۰۰۰	۰/۰۲۶۱
ترس ← انگیزه حفاظت	-۰/۳۲۷	۰/۰۶۰	۵/۴۶۸	۰/۰۰۰	۰/۰۹۶

۵- نتیجه گیری و پیشنهاد

بر اساس مفاهیم تئوری اثرگذاری[1] می‌توان گفت که تصمیات افراد، اغب تحت تاثیر وضعیت موقت یا زودگذر قرار دارد، هم‌چنین بر اساس نظریه انگیزه حفاظت[2] که یک مدل شناخت اجتماعی است بیان شده است که افراد ملزم به رفتار حفاظتی و مبتنی بر مراقبت هستند. این نظریه به ارزیابی پیامدهای کنش افراد می‌پردازد و آن‌ها را در دسته تهدید و مقابله دسته‌بندی می‌کند. لذا این تحقیق به دنبال آن است تا بر اساس نظریه روانشناسی مثبت گرا، روابط میان ارزیابی تهدید امنیت ، ترس و انگیزه حفاظت از سیستم‌های اطلاعاتی حسابداری را در حسابداران و مدیران مالی شرکت های پذیرفته شده در بورس اوراق بهادار مورد مطالعه و بررسی قرار دهد. شواهد این تحقیق نشان می‌دهد هرگاه کارکنان به این نتیجه برسند که تهدید علیه سیستم های اطلاعاتی حسابداری جدی است ، در آن صورت انگیزه آن‌ها برای حفاظت از سیستم اطلاعاتی افزایش می‌یابد. این یافته تحقیق حاضر با نتایج تحقیق سی پونن و همکاران (۲۰۱۴) مطابقت دارد. آن ها عقیده دارند هرگاه کارکنان به این نتیجه برسند که سیستم های اطلاعاتی شرکت با تهدید امنیتی روبرو است، تلاش می کنند تا با آن تهدیدات مقابله نمایند.

هم چنین نتایج آزمون فرضیه ها نشان داد که با افزایش ارزیابی تهدید علیه سیستم های اطلاعاتی حسابداری ، ترس کارکنان کاهش می یابد. این موضوع با نتایج تحقیق شی و همکاران (۲۰۲۴) و لزتاری و همکاران (۲۰۲۴) مطابقت ندارد. آن ها دریافتند با افزایش درک از تهدیدات امنیتی ، ترس کارکنان از پیامدهای نامطلوب آن تهدیدات افزایش می یابد. در فرضیه سوم نیز یافته ها نشان می دهد با افزایش ترس کارکنان ، انگیزه آن ها برای حفاظت از سیستم اطلاعاتی کاهش می یابد. این یافته نیز با نتایج تحقیق گانی و اسمیت (۲۰۲۴) همخوانی دارد. آن ها معتقدند ترس کارکنان از خطرات حملات امنیتی سیستم های اطلاعاتی تاثیر معنی داری بر فرایندهای شناختی آن ها می گذارد.

این تحقیق با استفاده از نظریه روانشناسی مثبت گرا نشان داد که ویژگی ها و قابلیت های کارکنان می تواند در بهبود حفاظت از سیستم های اطلاعاتی بسیار تاثیرگذار باشد. این موضوع می تواند موجب بسط تحقیقات رفتاری در حسابداری گردد. هم چنین، این مقاله از رویکرد مطالعات میان رشته ای استفاده می نماید. تحقیقات در حوزه های میان رشته ای در حسابداری می تواند شکاف های علمی میان رشته حسابداری و سایر رشته را تا حدودی برطرف نماید و فرصت هایی را برای دانشجویان و استادان رشته حسابداری فراهم می سازد تا با مفاهیم سایر رشته ها آشنا شوند. یافته های تحقیقات میان رشته ای امکان تحلیل بهتر مسائل مطرح در هر رشته را فراهم می نماید. هم‌چنین توسعه مطالعات میان رشته‌ای در حسابداری موجب بهبود توانمندی علمی استادان، دانشجویان، پژوهش‌گران و کاربردی تر شدن این رشته در کشور می‌شود. یافته های این تحقیق هم چنین می‌تواند به واحدهای تجاری و مدیران آن‌ها، اطلاعات سودمندی را درباره عوامل فردی و روانشناختی تاثیرگذار بر انگیزه حفاظت از سیستم های اطلاعاتی ارائه نماید.

از نوآوری‌های برجسته این تحقیق می‌توان به کاربرد روان‌شناسی مثبت‌گرا در امنیت اطلاعات اشاره کرد زیرا که تحقیقات قبلی عمدتا بر روی بازدارندگی و جذابیت‌های ترس برای ایجاد انگیزه در رفتار حفاظتی تمرکز داشته‌اند در صورتی که در این مطالعه دیدگاه جدیدی بر اساس تاکید بر نقاط قوت و مثبت محرک‌های مثبت ، برای انطباق امنیتی مطرح می‌شود. هم‌چنین این تحقیق با استفاده از کاربرد نظریه انگیزه حفاظت، به بررسی این موضوع می‌پردازد که چگونه ارزیابی تهدید و مکانیزم‌های مقابله، بر انگیزه‌های افراد برای محافظت از سیستم‌های اطلاعاتی اثرگذار است. این مطالعه با ترکیب ساختارهای روان‌شناسی مثبت‌گرا و نظریه انگیزه حفاظت

[1] Affect theory

[2] Protection Motivation Theory

چارچوب جامع‌تری را برای درک عوامل انگیزشی که موجب امنیت سیستم‌های اطلاعاتی می‌شود ارائه می‌دهد.

درک رابطه بین ارزیابی تهدید امنیتی، ترس و انگیزه برای محافظت از سیستم‌های اطلاعاتی حسابداری می‌تواند برای توسعه سیاست‌های امنیتی موثر، ضروری است. سازمان‌ها با بهره‌گیری از بینش‌های روان‌شناسی مثبت و نظریه‌هایی مانند نظریه انگیزه حفاظت، می‌توانند مداخلاتی را طراحی کنند که نه تنها به ارزیابی شناختی تهدیدات می‌پردازد، بلکه محیطی را ایجاد می‌کند که به طور ذاتی افراد را به انجام رفتارهای محافظتی برمی‌انگیزد.

یافته های این تحقیق نشان داد که انگیزه کارکنان از حفاظت از امنیت سیستم های اطلاعاتی تحت تاثیر عواملی چون ارزیابی کارکنان از میزان تهدید امنیتی و ترس آن ها از خطرات ناشی از آن تهدیدها می باشد. از این رو به مدیران شرکت های پذیرفته شده در بورس اوراق بهادار پیشنهاد می شود با تدوین دستورالعمل های تشویقی و یا برگزاری دوره های آموزشی و روانشناختی نسبت به بهبود انگیزه کارکنان از حفاظت از امنیت سیستم های اطلاعاتی اقدام نمایند.

محدودیت اصلی این تحقیق، مربوط به محدودیت ذاتی پرسش‌نامه در جمع‌آوری داده‌ها است. طبق این محدودیت، ممکن است پاسخ‌دهندگان در زمان پاسخ‌گویی به سوالات پرسش‌نامه دقت کافی نداشته باشند و یا این‌که شرایط، حالات و روحیات آن‌ها تحت تاثیر شرایط محیطی طوری تغییر کند که در نتیجه پاسخ‌ها را به درستی درک نکنند، این موارد خارج از کنترل محقق می‌باشد. محدودیت دیگر این تحقیق مربوط به نمونه‌گیری اتفاقی است که نمونه انتخاب شده به این روش ممکن است نتواند معرف واقعی جامعه باشد و نتایج حاصل از آن را به جامعه تعمیم داد.

فهرست منابع

اخوان فاطمه ،امین موسوی سید عبدالله ، سرآبادانی ابوالقاسم (۱۴۰۳) رویکردی جهت تجزیه و تحلیل فضای کسب و کار در راستای حکمرانی امنیت اطلاعات ، فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی، شماره ۲۹ صص ۲۲۳-۲۵۲

باغانی، الهه، الهی، شعبان، حسن زاده، علیرضا، و رجب زاده قطری، علی. (۱۴۰۳). مدیریت تکامل و تحول معماری سیستم های اطلاعاتی در محیط پویای سازمان با رویکرد عاملیت. کنفرانس بین المللی پژوهش های مدیریت و علوم انسانی در ایران

تجویدی، الناز، و احمدی، پریسا. (۱۳۹۹). تاثیر مکانیسم ارتباطی راهبری فناوری اطلاعات بر عملکرد سیستم اطلاعاتی حسابداری در جهت دستیابی به مزیت رقابتی. دانش حسابداری و حسابرسی مدیریت، ۹(۳۳)، ۱۰۵-۹۱

چگونیان، ایمان، سلطانی، اصغر، تعمت بخش،محمد علی(۱۳۹۲) ارزیابی سیستم اطالعات حسابداری از دیدگاه کاربران، پایان نامه کارشناسی ارشد دانشگاه آزاد اسالمی واحد مبارکه اصفهان.

رحمانیان کوشککی عبدالرضا (۱۴۰۴) ارزیابی و رتبه بندی عوامل مؤثر در استقرار نرم افزارهای حسابداری دانش حسابداری و حسابرسی مدیریت دوره ۱۴/ شماره ۲)پیاپی ۵ صص ۱۴۹-۱۶۴

رستمی مازویی نعمت ، رهنمای رودپشتی فریدون ، رئیس زاده سید محمدرضا، زهرا پورزمانی (۱۳۹۸) تبیین اثرات کنشگران فنی و انسانی بر کارکردهای سیستم اطلاعاتی حسابداری مدیریت با استفاده از نظریه شبکه کنشگران، دانش حسابداری و حسابرسی مدیریت ، شماره ۴۱ صص ۹۱-۱۱۰

رفاهی بخش سمانه، بنی مهد بهمن، خردیار سینا، اوشک سرائی مریم. عواطف فردی و رفتار مدیریت سود : آزمونی از نظریه روانشناسی مثبت گرا. دو فصلنامه حسابداری ارزشی و رفتاری. ۱۳۹۷; ۳ (۶) :۲۴۱-۲۵۳

رحیمی هلز بنفشه ، احمدی فائق ، خان محمدی محمد حامد ، رنجبر محمد حسین ، کردلویی حمیدرضا (۱۴۰۱) ارائه مدل سیستم اطالعات حسابداری مدیریت مبتنی بر هوش تجاری بر اساس نظریه زمینه بنیان ، دانش حسابداری و حسابرسی مدیریت ، شماره ۴۲ صص ۳۵۷ -۳۶۸

صالحی، مهدی، نوروزی، مهدی(۱۳۹۴). مطالعه تجربی پذیرش نرم افزارهای حسابداری در میان دانشجویان . حسابداری و منافع اجتماعی، ۵(۱):.۲۸-۱

صالحی، محمد، حاجی زاده، محمد(۱۳۸۹). بررسی سواد عمومی کامپیوتری کارکنان دانشگاه آزاد اسلامی استان مازندران، فصلنامه فناوری اطلاعات و ارتباطات در علوم تربیتی. سال اول، شماره اول، صص ۱-۱۵

صدری پروین، رهنمای رودپشتی فریدون ، پورزمانی زهرا ، نیکومرام هاشم (۱۳۹۷) فرا تحلیل ارتباطات درون شبکه کنشگران با یکدیگر و ارائه مدل ارتباطات بر اساس سیستم اطلاعات حسابداری ایران، دانش

حسابداری و حسابرسی مدیریت، شماره ۲۸ صص ۱۶۷-۱۸۵

علیپور، مهرداد، بدیعی، حسین، رمضانی، مرتضی.)۱۳۸۹ .) ارزیابی نرم افزارهای حسابداری بر اساس ویژگی های سیستم های اطلاعاتی حسابداری، مطالعه موردی شرکت های مستقر در استان زنجان . حسابداری مدیریت، ۴(۳) : ۶۶-۷۷

عزیزی فرهاد ؛ خان محمدی محمد حامد ؛ اسماعیل زاده علی؛ رهنمای رودپشتی فریدون (۱۴۰۰) ارائه الگویی از اثر ویژگی‌های سیستم‌های اطلاعاتی حسابداری بر عملکرد سیستم مبتنی بر نقش تعدیلی عدم‌اطمینان‌کاری و عدم تمرکز سازمانی، دانش حسابداری و حسابرسی مدیریت ، شماره ۳۷ صص ۹۷-۱۱۱

فارسی، محسن ؛ پاکمرام، عسکر ؛ رضایی، نادر ؛ جعفری علی (۱۴۰۳) سیستم اطلاعات حسابداری مبتنی بر معماری بلاک چین: طراحی مدل ، تحلیل بازار سرمایه ، شماره ۱۳ صص ۱۸۱-۲۱۰

گیلانی نیای صومعه سرائی، بهنام ؛ ربیعی؛ خدیجه ؛ فتوحی فشتمی ، حسن (۱۴۰۳) تدوین مدل سیستمهای اطلاعاتی حسابداری یکپارچه در سازمان‌های دولتی ایران در راستای بهبود عملکرد و کاهش تخلفات سازمانی ، دانش حسابداری و حسابرسی مدیریت دوره ۱۲، شماره ۴۶، صص 201-216

محمد نژاد، مهناز، جامی، مجید، مرادخانی مالل، بهنام(۱۳۹۹) بررسی ارزیابی نرم افزارهای حسابداری بر اساس ویژگی های سیستم های اطلاعاتی حسابداری مورد مطالعه (شرکتهای تولیدی واقع در شهرک صنعتی زاهدان . مطالعات اقتصاد، مدیریت مالی و حسابداری، ۶(۳): ۲۲-۳۰

موسوی پریسا، لگزیان محمد، ۱۳۹۷، مروری سیستماتیک بر رویکردهای سرمایه گذاری در امنیت اطلاعات، فصلنامه علمی-پژوهشی مطالعات مدیریت کسب و کار هوشمند- سال هفتم – شماره ۲۵.

واعظ سید علی ، احمدی رویا (۱۳۹۲) امنیت و تهدیدات امنیتی در سیستمهای اطلاعاتی حسابداری، پژوهش حسابداری ، شماره ۱۰ صص ۱-۲۰

Balicka, H. (2023). Digital technologies in the accounting information system supporting decision-making processes. *Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska*.

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209.

Fang, Y.H. (2017), Coping with fear and guilt using mobile social networking applications: knowledge hiding, loafing, and sharing", Telematics and Informatics, Vol. 34 No. 5, pp. 779-797.

Ganye, D. and Smith, K. (2024), Examining the effects of cognitive load on information systems security policy compliance", *Internet Research*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/INTR-04-2023-0329

Jarah, B. A. F., Zaqeeba, N., Al-Jarrah, M. F. M., Al Badarin, A. M., & Almatarneh, Z. (2023). The mediating effect of the internal control system on the relationship between the accounting information system and employee performance in Jordan Islamic banks. *Economies*, *11*(3), 77.

Li, X., Cheng, J., Shi, Z., Liu, J., Zhang, B., Xu, X., ... & Sheng, V. S. (2023). Blockchain security threats and collaborative defense: A literature review.

Lehenchuk, S. F., Vygivska, I. M., & Hryhorevska, O. O. (2022). Protection of accounting information in the conditions of cyber security.

Lestari, S., Adawiyah, W.R., Alhamidi, A.L., Prayogi, J. and Haryanto, R. (2024), "Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking", *Safer Communities*, Vol. 23 No. 4, pp. 444-464

Mills, A., Todorova, N. and Zhang, J. (2024), "The role of threat and coping appraisals in motivating the use of personalized mobile emergency alert systems", *Information Technology & People*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ITP-04-2021-0297

Sharma, K., Zhan, X., Nah, F.F.-H., Siau, K. and Cheng, M.X. (2021), "Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 1 No. 1, pp. 69-91. https://doi.org/10.1108/OCJ-03-2021-0009

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

Thompson, N., McGill, T., & Narula, N. (2024). " No point worrying"–The role of threat devaluation in information security behavior. *Computers & Security*, *143*, 103897.

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, *4*(1), 1-20.

Thomas, G. and Sule, M.-J. (2022), "A service lens on cybersecurity continuity and management for organizations' subsistence and growth", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 3 No. 1, pp. 18-40. https://doi.org/10.1108/OCJ-09-2021-0025

Van Zoonen, W., Treem, J.W. and Sivunen, A. (2022), "An analysis of fear factors predicting enterprise social media use in an era of communication visibility", *Internet Research*, Vol. 32 No. 7, pp. 354-375. https://doi.org/10.1108/INTR-05-2021-0341

Vafaei-Zadeh, A., Nikbin, D., Teoh, K.Y. and Hanifah, H. (2024), "Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia", *International Journal of Bank Marketing*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/IJBM-03-2024-0138

Xu, Y. W., Cai, R. R., & Gursoy, D. (2024). When disclosing the artificial intelligence (AI) technology integration into service delivery backfires: Roles of fear of AI, identity threat and existential threat. *International Journal of Hospitality Management*, *122*, 103829.

Yazdanmehr, A., Li, Y., & Wang, J. (2023). Employee responses to information security related stress: Coping and violation intention. *Information Systems Journal*, *33*(3), 598-639.

Zhan, Y., Ahmad, S. F., Irshad, M., Al-Razgan, M., Awwad, E. M., Ali, Y. A., & Ayassrah, A. Y. B. A. (2024). Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. *Heliyon*, *10*(1).

Accounting Knowledge & Management Auditing
Vol. 15/ No. 58/ Summer 2025

Explaining The Relationship Between Security Threat Assessment, Fear, and Motivation to Protect Accounting Information Systems: A Test of Positive Psychology Theory

Ali Tarchani Narenjbon
PhD Student in Accounting, Department of Accounting, Qazvin Branch, Islamic Azad University, Qazvin, Iran

Farzin Rezaei
Associate Professor, Department of Accounting, Qazvin Branch, Islamic Azad University, Qazvin, Iran
(Corresponding Author)
Farzin.rezaei@iau.ac.ir

Mehdi Beshkooh
Assistant Professor, Department of Accounting, Qazvin Branch, Islamic Azad University, Qazvin, Iran

Abstract
The main objective of this study is to study the relationships between security threat assessment, fear, and motivation to protect information systems among accountants and financial managers. The statistical population of the study includes accountants and financial managers working in companies listed on the Tehran Stock Exchange. From this population, a sample of 407 people was randomly selected. The research method is a library method to collect theoretical foundations of the research and a survey and questionnaire to collect research data. The findings of this study show that with increasing people's perception of the threat against accounting information systems, their motivation to protect the information system increases significantly. The research findings also confirm that with increasing people's perception of the threat assessment against accounting information systems, their fear decreases, and finally, with increasing people's fear, their motivation to protect the information system also decreases significantly.
Keywords: Information Systems, Security Threat, and Fear