مدیریت امنیت اطلاعات در کسب‌وکار هوشمند[1]

علی اکبر حدادی هرندی: دانش‌آموخته دکتری گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران؛
Email: aharandi@gmail.com
چنگیز والمحمدی*: دانشیار گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران؛
Email: valmohammadi@yahoo.com
جمشید صالحی صدقیانی: استاد گروه مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبایی، تهران، ایران؛
Email: P_DR_SS@yahoo.com

چکیده

در شرایط عدم اطمینان و ناپایدار فضای رقابتی عصر حاضر، مهم‌ترین وظیفه مدیران برای حفظ و افزایش سرمایه‌های فکری و دارایی مشهود کسب‌وکار و برتری از رقبایشان، تصمیم‌گیری صحیح و به‌موقع می‌باشد. پیاده‌سازی سیستم‌های کسب‌وکار هوشمند راهکاری فنی و اجتماعی برای تسهیل ارتباطات و تسریع دسترسی آسان به اطلاعات می‌باشد اما افزایش وابستگی کسب‌وکار به سیستم‌های اطلاعاتی؛ آسیب‌ها، تهدیدات و اقدامات فنی و غیرفنی برای نقض اصول امنیت اطلاعات کسب‌وکار را به دنبال داشته است که این مسئله اصلی سازمان‌ها و موضوع این مقاله می‌باشد. لذا هدف عمده این تحقیق بررسی تأثیر مدیریت امنیت اطلاعات بر پیاده‌سازی سیستم‌های هوشمند کسب‌وکار می‌باشد. در این مقاله با استفاده از ادبیات تحقیق و مدل بلوغ سیستم‌های هوشمند کسب‌وکار، مدلی تبیین و پرسشنامه‌ای طراحی و توسط ۳۰۵ نفر از مدیران، کارکنان دانشی و کارشناسان بخش حمل‌ونقل دولتی تکمیل شد. با استفاده از تحلیل عاملی تأییدی و تجزیه‌وتحلیل مسیر، سازه‌های مدل بررسی و داده‌های جمع‌آوری‌شده توسط نرم‌افزار AMOS تحلیل شدند. نتیجه حاصله حاکی از تأثیر مستقیم امنیت اطلاعات با ضریب رگرسیونی ۰/۳۸ بر هوشمندی کسب‌وکار می‌باشد؛ به‌عبارت‌دیگر امنیت اطلاعات باهدف تضمین تداوم عملیات و به حداقل رساندن آسیب‌ها و تهدیدات سایبری، باعث حفظ و ارتقاء اعتبار کسب‌وکار و به حداکثر رساندن فرصت‌های سرمایه‌گذاری از طریق توسعه بازارهای جدید می‌شود.

کلیدواژه: *مدیریت امنیت اطلاعات، سرمایه اطلاعاتی، هوشمندی کسب‌وکار، مدل‌سازی معادلات ساختاری*

Information Security Management in Business Intelligence

Ali Akbar Haddadi Harandi [1], Changiz Valmohammadi[2*] , Jamshid Salehi Sadaghiani[3]

Abstract

In the uncertain and unstable conditions of the competitive atmosphere of the present day, the most important task of managers to maintain and increase intellectual capital and assets of the business and excellence of their competitors is a timely and timely decision. The implementation of Business Intelligence systems is a technical and social solution to facilitate communications and accelerate easy access to information. but Increased business dependence on information systems; is resulting in technical, non-technical damage, threats and measures to violate business information security principles. This is the main issue for organizations and the subject of this article. Therefore, the main objective of this study is to examine the impact of information security management on the implementation of Business Intelligence systems. In this paper, a questionnaire was designed using an in-depth review of the relevant literature and maturity model of business intelligent systems and completed by 305 managers, knowledge workers and experts in the field of public transport. Using the confirmatory factor analysis and Structural Equation Modeling, the structures of the survey model and the data collected by AMOS software were analyzed. The obtained result indicates a direct impact of information security with the regression coefficient of 0.38 on business intelligence. In other words, information security aimed at ensuring the continuity of operations and reducing the cyber damages and threats will cause businesses to maintain and enhance the investment opportunities through development of new markets.

Keyword: *Information Security Management, Informational Capital, Business Intelligence, Structural Equation Modeling*

1 – Information Technology Management Department, Management Faculty, Islamic Azad University South Tehran Branch, Tehran Iran
2 – Department of Management and Accounting, Allameh Tabatabaee University, Tehran, Iran

مقدمه

هوشمندی کسب‌وکار مفهومی جامع است که سازمان باهدف کسب اطلاعات به هنگام و باکیفیت برای تصمیم‌گیری؛ تلاش می‌کند تا از سیستم‌های اطلاعاتی به مؤثرترین روش استفاده نموده و به مزیت رقابتی دست یابد [۱]. سیستم‌های هوشمند کسب‌وکار، سرمایه‌های اطلاعاتی سازمان (از قبیل اطلاعات کاربران، مشتریان، شرکت‌کنندگان فعال در فعالیت‌های تجاری، اطلاعاتی و اجتماعی وابسته، نقشه‌های تولید، استراتژی و نظایر آن) را به‌صورت خودکار و الکترونیکی جمع‌آوری و پردازش می‌کنند و سپس از طریق کشف الگوها و قوانین سودمند، تصمیم‌گیری در کسب‌وکار را تسهیل کرده و منجر به فعالیتی خاص و یا راه‌اندازی سرویسی ارزش‌افزوده می‌گردند که محیط کسب‌وکار را تحت تأثیر قرارمی‌دهند [۲]-[۴]. گسترش سیستم‌های اطلاعاتی، توسعه شبکه‌های اجتماعی و اینترنت اشیاء در محیط پیرامون کسب‌وکار باعث رشد تولید داده‌های متنوع و حجیم شده است. محققان از این پدیده به نام داده‌های بزرگ یا عظیم داده[۲] نام برده‌اند. داده‌های بزرگ اکنون یک دارایی است که می‌تواند مزیت رقابتی قابل‌توجهی را خلق نموده و نوآوری را هدایت کند، رقابت را افزایش دهد و تأثیر اجتماعی ایجاد کند [۵]. از سوی دیگر با توجه گسترش داده‌ها تحقیقات نگرانی‌های جدی در مورد حفظ حریم خصوصی و استفاده از داده‌های کاربر شخصی و حساس را گزارش کرده‌اند [۶]. نظام امنیت اطلاعات با تغیر ماهیت استفاده از اطلاعات برای اهداف تجاری، وابستگی کسب‌وکار به سیستم‌های اطلاعاتی، سناریوهای متفاوتی را برای کاهش ریسک و مقابله با تهدیدات سایبری ارائه می‌نماید [۷]. هدف اصلی این مقاله ارائه رویکردی جدید در بررسی کاربرد سرمایه اطلاعاتی و هوشمندی کسب‌وکار با پیش‌فرض رعایت اصول امنیت اطلاعات در حفظ یکپارچگی، دسترسی‌پذیری و اصالت اطلاعات برای خلق ارزش و حفظ اعتبار کسب‌وکار می‌باشد.

ساختار این مقاله بدین شرح است که ابتدا با مرور مبانی نظری و مرور تحقیقات پیشین، ضرورت و علت انجام و مسئله اصلی تحقیق تبیین خواهد شد. در بخش بعد با استفاده از مطالعات قبلی متدولوژی و روش تحقیق و ابزار تحلیل داده‌ها توضیح داده خواهد شد.

در بخش محاسبات، با ارائه تئوری‌های مورداستفاده در تحقیق، مدل مفهومی ترسیم و فرضیه مورد آزمون تدوین و تشریح می‌گردد سپس با آزمون داده‌های جمع‌آوری‌شده نتایج تحلیل‌های آماری به‌صورت مختصر و توضیحی گزارش می‌شود و با بررسی و مقایسه نتایج تحقیق با یافته‌های پژوهش‌های مرتبط جمع‌بندی و نتیجه‌گیری خواهد شد.

مبانی نظری

برخلاف وابستگی فعالیت‌های اقتصادی و اجتماعی به اطلاعات و داده‌ها در دهه‌های قبل، امروزه با روند فزاینده حجم، سرعت و تنوع داده‌ها و شکل‌گیری پدیده‌ای به نام کلان (عظیم) داده در حوزه‌های اقتصادی و اجتماعی، مواجه هستیم. این پدیده منجر به تغییر الگوی کسب‌وکارها به یک مدل اقتصادی -اجتماعی داده محور شده است [۸]. تحلیل و استفاده از داده‌های عظیم به‌عنوان یک عامل کلیدی موجب رشد مزیت رقابتی در کسب‌وکارها شده و محرک نوآوری، افزایش رقابت و اثرات مثبت اجتماعی به دنبال خواهد داشت [۹]. در این فضا برای خلق ثروت از داده‌های عظیم در کسب‌وکارها روش‌های زیر پیشنهاد شده است [۱۰]:

۱. شفاف‌سازی و قابل‌انتقال کردن اطلاعات به‌دفعات بسیار،
۲. تولید و ذخیره‌سازی داده‌های ناشی از تراکنش‌ها در اشکال دیجیتالی،
۳. طراحی دقیق‌تر محصولات و خدمات از طریق متمرکز شدن بر روی اطلاعات مشتریان،
۴. بهبود و تصمیم‌سازی پایدار از طریق تحلیل‌های پیچیده،
۵. بهبود و توسعه نسل جدید محصولات و خدمات.

قابلیت‌های ارزش‌افزای اشاره شده، سبب گردیده از اطلاعات به‌عنوان یک سرمایه برای کسب‌وکار نام‌برده شود. سرمایه اطلاعاتی در بستر فناوری اطلاعات و ارتباطات با تأخیر زمانی بر ساختار، اندازه، فرهنگ، یادگیری و روابط بین سازمانی نیز تأثیر خواهد گذاشت و منجر به توانمندسازی کارکنان، افزایش حیطه سازمان، افزایش کارایی، خلاقیت و نوآوری می‌شود [۱۱]. ازآنجاکه در فضای مجازی به‌کارگیری فرایند چرخه دانش، داده و اطلاعات را به سرمایه تبدیل می‌کند؛ بشر با وابستگی به فضای سایبری و دریافت و به‌کارگیری مداوم اطلاعات و ایده‌های نو در زندگی خود، به این فضا وابسته شده است و طبیعتاً بیشتر در معرض حمله بالقوه هکرها قرار می‌گیرد. لذا بهترین راه حصول اطمینان از محرمانه و امن بودن داده‌های حساس، سرمایه‌گذاری در یک راهکار امنیت سایبری است که تأمین‌کننده نیازهای فرد و سازمان باشد [۱۲]. امنیت سرمایه اطلاعاتی در کنار امنیت سرمایه‌های مالی و فیزیکی پشتوانه یکدیگر محسوب می‌شوند و رکن امنیت را در سازمان‌ها و کسب‌وکارها تشکیل می‌دهند [۱۳]. «انجمن جهانی مدیریت داده»[۳] با ارائه مؤلفه‌های دانش مدیریت داده (DMBOK)[۴] توصیه نموده است علاوه بر نیازمندی‌های نوینی که در عرصه تولید و پردازش و تحلیل داده، به وجود آمده است، نیازمندی‌های مدیریتی داده هم باید مدنظر کسب‌وکارها قرار گیرد تا بتوان یک سازمان کاملاً مکانیزه و هوشمند داشت [۱۴].

DMBOK در مؤلفه سوم به مدیریت امنیت اطلاعات پرداخته است و توصیه می‌کند کسب‌وکارها باید برای بحث امنیت داده، یک استراتژی درست راهبری داده داشته باشند. بطوریکه مشخص باشد چه افرادی، تحت چه شرایطی، در چه زمانی به کدامین داده‌ها دسترسی دارند. همچنین چگونه با حوادث داده‌ای مانند خرابی ذخیره‌سازها یا از کارافتادن شبکه، دزدی و هک شدن داده‌ها مواجه شوند.

محرک‌های بسیار پیچیده در زیرساخت فناوری اطلاعات، تهدیدات جدیدی را برای امنیت زیرساخت‌های مدیریت فناوری

شکل ۱: مؤلفه‌های دانش مدیریت داده. منبع: انجمن جهانی مدیریت داده، ۲۰۱۷

اطلاعات ایجاد می‌کند. این تهدیدات قابل پیش‌بینی نیست و در ابتدا، قابل‌شناسایی و قابل‌رفع نمی‌باشند. سازمان‌ها به علت عدم اطمینان‌هایی که ریشه در فناوری دارند، با مسائل امنیتی مختلف مواجه می‌شوند و اقدامات امنیتی آن‌ها، نیازمند تغییر در شرایط امنیتی و شناسایی عوامل مؤثر بر مدیریت امنیت فناوری اطلاعات می‌باشند [۱۵] و [۱۶]. جهت فهمیدن و درک سامانه‌ای تهدیدات و دسته‌بندی آن‌ها حداقل سه رویکرد متفاوت وجود دارد:

۱. مهاجم‌محور [۵]
۲. نرم‌افزارمحور [۶]
۳. دارایی‌محور [۷]

در رویکرد دارایی محور، تحلیل‌های محرمانگی [۸]، یکپارچگی [۹] و دسترسی‌پذیری [۱۰] (CIA) بر روی دارایی‌های اطلاعاتی اعمال می‌گردد. در رویکرد مهاجم محور، تحلیل‌های احراز اصالت [۱۱]، مجازشناسی [۱۲] و حسابرسی [۱۳] (AAA) بررسی می‌شوند. همچنین تهدیدات حریم خصوصی در این دسته ارزیابی می‌شوند. در رویکرد نرم‌افزار محور، نیز ریسک‌های احتمالی تحلیل می‌شوند [۱۷].

تضمین امنیت اطلاعات و حفظ حریم خصوصی افراد و پیاده‌سازی سیستم مدیریت امنیت اطلاعات به‌منظور حصول اطمینان از به‌کارگیری کنترل‌های امنیتی مناسب، در کسب‌وکارها ضروری و حیاتی است و یکی از مهم‌ترین عوامل در پذیرفتن فناوری‌های جدید اطلاعاتی به شمار می‌رود؛ زیرا علیرغم وابستگی روزافزون به سیستم‌های اطلاعاتی، تهدیدها در این سیستم‌ها نیز جدی‌تر می‌شود [۱۸].

سیستم‌های هوشمند کسب‌وکار، باهدف کسب اطلاعات به هنگام و باکیفیت برای تصمیم‌گیری؛ تلاش می‌کند تا از سیستم‌های اطلاعاتی به مؤثرترین روش استفاده نموده و به مزیت رقابتی دست یابد [۱]. اهداف اولیه این سیستم‌ها، بهبود کیفیت و به‌موقع بودن فرآیند تصمیم‌گیری است [۱۹]. قابلیت‌های هوش کسب‌وکار از مؤلفه‌های مهمی به‌شمار می‌روند که به یک سازمان یاری می‌رسانند تا بتواند به بهترین وجه، خودش را با تغییرات سازگار نماید و عملکردش را بهبود بخشد [۲۰]. این قابلیت‌ها ناشی از به‌کارگیری ابزارها و تکنیک‌های مبتنی بر سیستم پشتیبانی تصمیم، سیستم‌های اطلاعات اجرائی و انباره داده است و شامل اجزایی از قبیل پرس‌وجو، مصورسازی، گردش کار، تحقیق در عملیات و هوش مصنوعی کاربردی است [۲۱].

پژوهشگران در چند سال اخیر به میزان اهمیت امنیت فناوری اطلاعات در سازمان‌ها و شرکت‌های تجاری و غیرتجاری پی برده‌اند و بیش‌ازپیش به دنبال شناسایی عوامل مؤثر بر آن و کمک به مدیریت سازمان‌ها با ارائه راهکارهایی که امکان کنترل این عوامل را به حداکثر برساند، می‌باشند.

محمودزاده و رادرجبی (۱۳۸۵) با بررسی مدیریت امنیت در نظام‌های اطلاعاتی، مؤلفه **عدم آگاهی کاربران** را بالاترین تهدید برای امنیت اطلاعات نظام‌های رایانه‌ای برشمرده است.[۲۲] اسماعیل‌پور (۱۳۸۸) با بررسی شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود نظام مدیریت امنیت اطلاعات، نشان داده **عوامل حوزه فنی** (نظام‌های اطلاعاتی و به‌روزرسانی نظام‌ها) بر بهبود نظام مدیریت امنیت اطلاعات تأثیر دارند [۲۳]. نیارکی و عبدی (۱۳۹۵) با اشاره به نقش منحصربه‌فرد اطلاعات کسب‌وکارها در محیطی رقابت، استفاده و لزوم حفاظت از آن را امری اجتناب‌ناپذیر می‌داند؛ و **هم‌راستا بودن فعالیت‌های امنیت با نیازمندی‌های کسب‌وکار** و ایجاد وحدت و هماهنگی بین کارکرد تمام عوامل ایمن‌سازی را سبب افزایش موفقیت مدیریت امن‌یت برشمرده است [۲۴]. نتایج تحقیق پارسونز و همکاران (۲۰۱۴) بر روی ۵۲۲ کارمند استرالیایی نشان داد که روش‌ها و سیاست‌های دانشی نفوذ قوی‌تری نسبت به تعریف افراد از رفتار خود داشته است. این یافته‌ها بیانگر این است که **آموزش‌وپرورش** خیلی بیشتر ازآنچه انتظار می‌رود می‌تواند در ایجاد دانش مناسب برای استفاده از سیستم‌های اطلاعاتی و امنیت سیستم‌ها نگرش ایجاد نماید [۳]. باتس (۲۰۱۵) با بررسی مطالعات و تحقیقات پیشین، ویژگی‌ها و عوامل سازمانی اثرگذار بر اثربخشی امنیت سیستم‌های اطلاعاتی را استخراج نموده است. بر مبنای ارزیابی نظرات خبرگان، موضوع میزان اثرگذاری عوامل سازمانی بر سازه‌های واسط، تلاش‌های پیشگیرانه و بازدارنده، تعیین و مفروضات ارائه‌شده آزمون گردید. نتایج نشان می‌دهد که **حمایت مدیران ارشد** با اثرگذاری بر هر دو تلاش، بیشترین نقش را بر اثربخشی امنیت در سیستم‌های اطلاعاتی داراست. نوع کسب‌وکار و اندازه سازمان بر تلاش‌های پیشگیرانه و نوع کارکنان سازمان و سیاست‌های امنیتی بر تلاش‌های بازدارنده، اثرگذار است. عوامل سازمانی به‌واسطه این دو نوع تلاش بر اثربخشی سیستم‌های اطلاعاتی مؤثر است [۱۸].

موس و آتر [۱۵] (۲۰۰۳) در کتاب نقشه راه کسب‌وکار هوشمند **زیرساخت سازمانی مناسب** در کنار زیرساخت فنی و غیر فنی را ازجمله عوامل موفقیت هوشمندی کسب‌وکار برشمرده است. مؤلفه‌هایی چون سخت‌افزار، نرم‌افزار، میان‌افزار، سیستم‌های مدیریت پایگاه داده، سیستم‌عامل‌ها، زیرساخت‌های فنی را تشکیل می‌دهند و مؤلفه‌هایی مانند استانداردهای متادیتا، داده‌کاوی، مدل منطقی داده‌ها و متدولوژی‌ها، زیرساخت‌های غیرفنی را معین می‌کنند [۲۵]. سنگر و یاهد [۱۶] (۲۰۱۳) بر مبنای مطالعات قبلی و چرخه عمر پروژه، مدل فرآیندی سه مرحله‌ای

قبل، حین و بعد از پیاده‌سازی سیستم هوش کسب‌وکار را پیشنهاد داده‌انـد. مرحله اول، رویکرد پیاده‌سازی و اصول سازمانی نیز تعیین می‌شوند و تغییرات لازم را بـرای هـم‌تـرازی با استراتژی شرکت را فراهم می‌کند. مرحله دوم شامل طراحی، ترکیب و تست سیستم هوش کسب‌وکار است. مرحله سوم نیز شامل دو نوع فرآیند بهینه‌سازی سیستم و نگهداری سیستم می‌باشد [۲۶]. بروکس و همکاران [۱۷] (۲۰۱۵) معتقدند ابعاد هوشمندی کسب‌وکار فراتر از تکنولوژی است و شامل فهم تعامل جنبه‌های کلیدی سازمانی، فنی و فرآیند منابع انسانی می‌باشد. در پیاده‌سازی هوشمندی کسب‌وکار عناصر زیاد وجود دارد که باید در نظر گرفته شوند. این عناصر شامل فرآیندهای کسب‌وکار، فرهنگ سازمانی، افراد، منابع، تکنولوژی و محیط سازمانی می‌باشد[۱۹].

اولبریچ و همکاران [۱۸] (۲۰۱۲) پـروژه هوشمندی کسب‌وکار ابعاد رفـتاری و سازمانی فراگیری دارد که باید به‌درستی درک شود زیـرا این پـروژه مختص یک بخش نبوده و تمام سازمان را دربـر می‌گیرد و بـرای پیاده‌سازی موفق آن تعهد و پذیرش تمام اعضاء نیاز است. در این راستا عواملی مانند کیفیت منابع داده، تأمین مالی سرمایه‌گذاری، نـوع صنعت، سطح حمایت مدیران عالی و مهارت‌های تاکتیکی نقش مهمی در موفقیت پیاده‌سازی هوشمندی کسب‌وکار ایفا می‌کنند [۲۷].

در شرایـط عـدم اطمیـنان و نـاپایـدار فـضای رقـابـتی عصر حاضر مـدیـران بـدون داشتن سرمایه‌های اطلاعاتی مـورد نیاز، قـادر به رهبری سازمان و رسیدن به اهـداف از پیش تعیین‌شده نیستند، بنابراین مهم‌ترین وظیفه مدیران برای حفظ و افزایش سرمایه‌های فکری و دارایی مشهود کسب‌وکار و برتری از رقبایشان تصمیم‌گیری صحیح و به‌موقع می‌باشد. تحولات و رشد بی‌وقفه فـنـاوری اطلاعات و ارتـبـاطات باعث شده حجم تولید داده به شکل غیرقابل‌باوری افزایش یابد؛ بنابراین در این شرایط آگاهی از اینکه چه اطلاعاتی مفید است و در راستای کسب‌وکار می‌تواند ارزش‌آفـریـن باشد، به‌طوری‌که مدیران بتوانند به‌موقع و در هر مکانی اطلاعات مناسب را در اختیار داشته باشند، سؤالی است که با پیاده‌سازی سیستم‌های کسب‌وکار هوشمند می‌توان پاسخ آن را یافت. همان‌طور که اشاره شد به‌موازات تسهیل ارتباطات و تسریع دسترسی آسان به اطلاعات، آسیب‌ها، تهدیدات، رخنه‌ها و خرابکاری‌های آگاهانه و عامدانه اصول امنیت اطلاعات کسب‌وکار یعنی محرمانگی[۱۹] ، یکپارچگی[۲۰] و دسترسی‌پذیری[۲۱] را تهدید می‌کنند [۱۱]. لذا سؤال اصلی این مطالعه این است که امنیت اطلاعات چگونه و تا چه میزان می‌تواند بر پیاده‌سازی سیستم‌های هوشمند کسب‌وکار اثرگذار باشد؟

روش تحقیق و ابزارها

این تحقیق ازنظر هدف اکتشافی است و ازنظر نتایج تحقیق، کاربردی می‌باشد. ازنظر نوع ماهیت توصیفی، همبستگی و علی و معلولی است. توصیفی است زیرا به دنبال ارائه وضع موجود امنیت و هوش کسب‌وکار در بخش حمل‌ونقل دولتی است. همبستگی است زیرا به دنبال تبیین رابطه امنیت و هوش کسب‌وکار است. علی و معلولی است زیرا به دنبال تعیین جهت روابط بین متغیرها می‌باشد.

این تحقیق ازنظر فرایند اجرا، کمی است و ازآنجاکه جامعه آماری این تحقیق را مدیران، کارشناسان و کارکنان دانشی بخش حمل‌ونقل دولتی کشور تشکیل داده‌اند، در طبقه تحقیقات مطالعه موردی قرار خواهد گرفت. فرضیه تحقیق بر اساس یافته‌های مرور ادبیات موضوع مرتبط شکل گرفته و این روابط را می‌آزماید. برای گردآوری اطلاعات مورد نیاز از مطالعات کتابخانه‌ای و پرسشنامه الکترونیکی استفاده شده است و ۳۰۵ نفر نسبت به تکمیل و ارسال پرسشنامه تحقیق همکاری نموده‌اند.

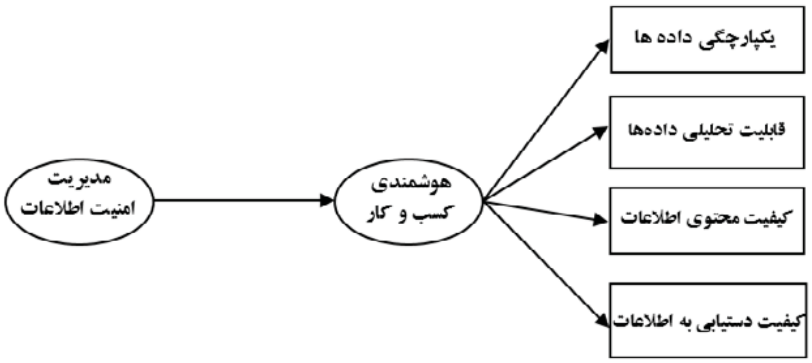
با توجه به حجم بالای نمونه جمع‌آوری و فرض نرمال بودن داده‌های جمع‌آوری‌شده، به‌منظور افزایش توانایی تبیین و کارایی در مدل‌سازی معادلات ساختاری، مدل اندازه‌گیری به تحلیل‌های عاملی تأییدی و رسیدن به مدل ساختاری و کشف روابط پنهان بین متغیرها کمک می‌کند. تحلیل عامل تأییدی، تعیین میزان توان مدل عاملی تحقیق هرندی و همکاران (۱۳۹۷) با داده‌های این مقاله را نشان می‌دهد و درصدد تبیین این مسئله است که آیا عامل‌ها با آنچه در تئوری هرندی و همکاران (۱۳۹۷) ارائه داده است انطباق دارد.

در این تحقیق به‌منظور تبیین و شناخت هر چه بهتر روابط علی و میزان تأثیرگذاری امنیت و هوش کسب‌وکار از روش همبستگی و به‌طور مشخص مبتنی بر مدل یابی معادلات ساختاری (SEM)[۲۲] ، توسط نرم‌افزار AMOS [۲۳] استفاده شده است.

با استفاده از تحلیل عاملی تأییدی پایایی و روایی سازه‌ای پرسش‌نامه انجام شده است. برای بررسی جنبه‌های پایایی (ثبات و سازگاری درونی) از روش‌های ضریب همبستگی پیرسون، ضریب همبستگی درون‌خوشه‌ای (ICC)، آزمون t-زوجی و ضریب آلفای کرونباخ و برای بررسی جنبه‌های متفاوت روایی سازه‌ای ازجمله روایـی همگرا و واگـرا از شاخص‌های پایایی سـازه‌ای [۲۴] (CR)، میانگین واریانس استخراجی [۲۵] (AVE)، حداکثر مجذور واریانس مشترک [۲۶] (MSV) و میانگین مجذور واریانس مشترک [۲۷] (ASV) استفاده شده است. با توجه به اینکه در مدل مفهومی تحقیق این سازه به‌صورت مرتبه دوم استفاده شده است، لذا روایی سازه‌ای مرتبه دوم مدل نیز سنجیده شده است.

تئوری و محاسبات

پرویچ و همکارانش [۲۸](۲۰۱۲) در تحقیقی به بررسی ارتباط بین ابعاد موفقیت سیستم‌های هوشمند کسب‌وکار و اثرات بلوغ سیستم‌های هوشمند کسب‌وکار و فرهنگ تصمیم‌گیری تحلیلی در استفاده از اطلاعات پرداخته‌اند. بر اساس داده‌هـای بررسی شده، یکپارچه‌سازی داده‌ها و قابلیت‌های تحلیلی را به‌عنوان دو بعد بلوغ سیستم‌های هوشمند کسب‌وکار به یکدیگر مرتبط می‌سازند. مطالعات آن‌ها نشان می‌دهد که یکپارچه‌سازی داده‌ها، نقطه شروعی برای پیاده‌سازی سیستم‌های هوشمند کسب‌وکار و تلاش برای رسیدن به سطوح بالاتر بلوغ سیستم‌های هوشمند کسب‌وکار در سازمان است. در این راستا ضرورت دارد ابتدا مسائل



شکل ۲: مدل مفهومی تحقیق

جدول ۱: بررسی ثبات سازه‌های مقیاس مدل تحقیق

نام سازه	نماد سازه	تعداد سؤالات	ضریب همبستگی پیرسون	ضریب همبستگی درونخوشهای (ICC)	p-value آزمون t-زوجی
هوش کسب‌وکار	BI	۱۷	۰/۷۰	۰/۷۲	۰/۳۸
امنیت اطلاعات	SIC	۹	۰/۸۵	۰/۸۹	۰/۴۱

یکپارچه‌سازی داده‌ها (مانند کیفیت داده‌ها و مسائل امنیتی، مسائل مدیریت فراداده، عدم وجود مهارت‌های یکپارچه‌سازی داده‌ها و تبدیل داده‌ها و مسائل مربوط به تجمیع داده‌ها) را که غالباً مانعی برای ارائه به‌موقع نتایج به کاربران است، حل شوند [۲۸]. با توجه به ادبیات موضوع و با توجه به اینکه تحقیقی مشاهده نشده که به بررسی ارتباط امنیت باهوش کسب‌وکار پرداخته باشد؛ در این تحقیق با استفاده از مدل پایه بلوغ هوشمندی کسب‌وکار پروبیچ و همکارانش و ادبیات موضوع حوزه امنیت اطلاعات یک مدل مفهومی ترسیم‌شده (شکل ۲) و به دنبال بررسی این فرضیه است که امنیت اطلاعات بر بلوغ کسب‌وکار هوشمند تأثیر مثبت و مستقیم دارد.

برای اجرای روش‌های آماری و محاسبه آماره آزمون مناسب بودن و استنتاج منطقی فرضیه تحقیق، آگاهی از توزیع داده‌ها از الویت اساسی برخوردار است. در این تحقیق با فرض نرمال بودن توزیع داده‌ها، آزمون کولموگروف اسیمرونوف انجام شد. با توجه به بالا بودن سطح معنی‌داری متغیرهای مستقل و وابسته آزمون از ۰/۰۵ و همچنین بزرگ‌تر بودن حجم نمونه از استاندارد قضیه حد مرکزی؛ پس فرض نرمال بودن توزیع داده‌ها تأیید می‌شود.

بحث و نتایج

برای بررسی ثبات هر یک از سازه‌های تحقیق، با استفاده از روش آزمون مجدد، تعداد ۳۰ آزمودنی با فاصله زمانی معین دومرتبه ارزیابی شدند. در ادامه با روش‌های ضریب همبستگی پیرسون، ضریب همبستگی درون‌خوشه‌ای (ICC) و آزمون t- زوجی ثبات هر یک از سازه‌های تحقیق مورد ارزیابی قرار گرفتند. نتایج در جدول ۱ آمده است.

جدول ۲: بررسی سازگاری درونی (پایایی)

نام سازه	نماد سازه	تعداد سؤالات	مقدار آلفای کرونباخ
هوش کسب‌وکار	BI	۱۷	۰/۹۴
امنیت اطلاعات	SIC	۹	۰/۹۲

همان‌طور که در جدول ۱ مشخص است، ضریب همبستگی پیرسون و همچنین ICC برای همه سازه‌ها بزرگ‌تر از ۰/۶۰ است که نشان از بالا بودن توافق پاسخگویی افراد به سازه‌ها دارد و همچنین مقدار p حاصل از آزمون t-زوجی نیز بزرگ‌تر از ۰/۰۵ است؛ که نشان‌دهنده عدم معنی‌داری میانگین نمره سازه‌ها در هر بار سنجش آزمودنی‌هاست.

در این بخش با استفاده از شاخص آلفای کرونباخ به بررسی پایایی سازه‌های مدل مفهومی می‌پردازیم. نتایج این تحلیل در جدول ۲ آمده است.

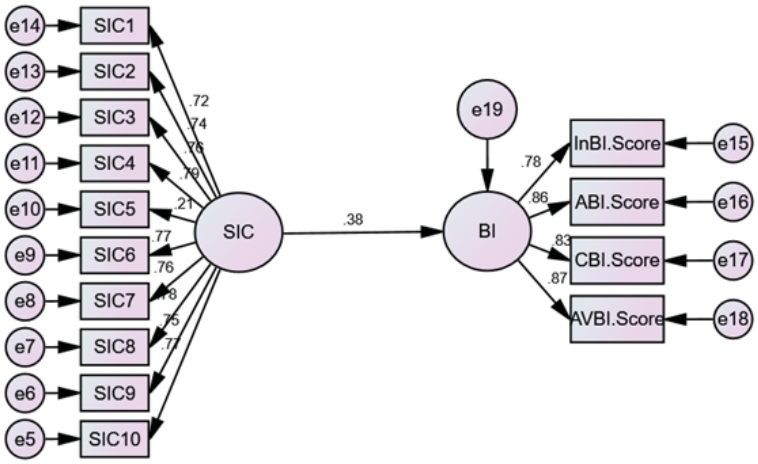
با توجه به مقادیر به‌دست‌آمده از آلفای کرونباخ در جدول شماره ۲ می‌توان نتیجه گرفت که هر یک از سازه‌های مقیاس مدل از سازگاری درونی مناسبی برخوردار می‌باشند. لذا در این مرحله پایایی این سازه پذیرفته می‌شود.

برای بررسی هدف و تأیید فرضیه تحقیق از آزمون‌های روایی استفاده شده است. یکی از موارد مهم در روایی ابزارهای پرسشنامه‌ای، روایی سازه‌ای است. روایی سازه‌ای خود شامل دو بخش مهم روایی همگرایی و روایی افتراقی می‌باشد. روش آماری مورداستفاده برای بررسی اعتبار سازه‌های مدل تحقیق، نیز تحلیل عاملی تأییدی است.

پس از بررسی نیکویی برازش، مدل تحلیل عاملی تأییدی سازه هوش کسب‌وکار و امنیت اطلاعات، شرط روایی همگرایی این است که [۲۹]:

جدول ۳: بررسی روایی سازهای مقیاس هوش کسب‌وکار و امنیت اطلاعات

شاخص‌ها	پایایی سازهای (CR)	میانگین واریانس استخراجی (AVE)	حداکثر مجذور واریانس مشترک (MSV)
هوش کسب‌وکار	۰/۸۶	۰/۶۱	۰/۵۳
امنیت اطلاعات	۰/۹۰	۰/۵۱	۰/۴۴



Model Froamt Show = Standardized estimates
Chi-Square =67.947[76] P-value =.733
Root mean square error of approximation (RMSEA) = .000
Comparative fit index (CFI) = 1.000
Normed fit index (NFI) = .972
Tucker-Lewis index (TLI) = 1.004
Goodness of fit index (GFI) = .970
Adjusted goodness of fit index (AGFI) = .958

شکل ۳: مدل نهایی تحقیق به همراه بارهای عاملی استاندارد

۱. پایایی سازه‌ای (CR) بزرگ‌تر از ۰/۷ باشد. به عبارتی CR> ۰/۷ باشد.
۲. بارهای عاملی معنی‌دار باشند. به عبارتی p-value< ۰/۰۵ باشد.
۳. بارهای عاملی استاندار بزرگ‌تر از ۰/۵ و در صورت امکان بزرگ‌تر از ۰/۷ باشند.
۴. پایایی سازه‌ای (CR) بزرگ‌تر از میانگین واریانس استخراجی (AVE) باشد. به عبارتی CR>AVE باشد.
۵. مقدار واریانس استخراجی (AVE) بزرگ‌تر از ۰/۵ باشد. به عبارتی AVE> ۰/۵ باشد.

همچنین شرط روایی واگرایی (افتراقی) نیز به این صورت است که میانگین واریانس استخراجی (AVE) بزرگ‌تر از حداکثر مجذور واریانس مشترک (MSV) باشد. به عبارتی AVE>MSV باشد.

روایی همگرایی با استفاده تحلیل عاملی تأییدی هر یک سازه‌های تحقیق بررسی می‌شود و روایی واگرایی با استفاده از مدل تحلیل عاملی تأییدی کل سازه‌ها در کنار یکدیگر صورت می‌پذیرد. نتایج بررسی روایی واگرایی سازه‌های تحقیق در جدول شماره ۳ آمده است که می‌توان نتیجه گرفت این سازه دارای روایی همگرایی و روایی افتراقی می‌باشد.

در شکل ۳ این مدل را به همراه بارهای عاملی استاندارد نشان داده شده است و در جدول ۴، نیز شاخص‌های نیکویی برازش مشاهده می‌گردد. همچنین در جدول ۵ بارهای عاملی غیراستاندارد به همراه معنی‌داری آن‌ها ذکر شده است.

با توجه به مقادیر مربوط به شاخص‌های نیکویی برازش، این مدل ازلحاظ همه شاخص‌های نیکویی برازش و با توجه به داده‌های این پژوهش در سطح خوب قرار دارد. مقادیر شاخص‌های برازندگی مدل بیانگر برازش مدل با توجه به تمام شاخص‌های برازندگی مدل با داده‌ها قلمداد می‌شود. لذا مدل برای مدل‌بندی معادلات ساختاری مورد تأیید است [۲۹].

بار عاملی در حقیقت یک ضریب همبستگی بین متغیرهای مکنون و متغیرهای آشکار در یک مدل اندازه‌گیری است. این ضریب تعیین می‌کند که متغیر مکنون چقدر از واریانس متغیرهای آشکار را تبیین می‌کند و ازآنجاکه یک ضریب همبستگی است باید ازنظر آماری معنادار باشد. معناداری بار عاملی با آماره‌های T VALUE و P VALUE بررسی می‌شود.

جدول ۴: شاخص‌های نیکویی برازش مدل تحقیق

نوع شاخص نیکویی برازش	حدود شاخص برای برازش موردقبول	حدود شاخص برای برازش خوب	شاخص نیکویی برازش مشاهده‌شده	نتیجه
مقدار آماره X^2(df)	نسبت آماره X^2 به درجه آزادی کمتر از ۵	نسبت آماره X^2 به درجه آزادی ۳	(۷۶)۶۷/۹۵	برازش خوب
P-value آزمون X^2			۰/۷۳	برازش خوب
نسبت آماره X^2 به درجه آزادی			۰/۸۹	برازش خوب
RMSEA	کمتر از ۰/۰۸	کمتر از ۰/۰۵	۰/۰۱	برازش خوب
P(RMSEA<0.05)	بیشتر از ۰/۰۵	بیشتر از ۰/۱	۰/۹۹	برازش خوب
CFI	بیشتر از ۰/۹۰	بیشتر از ۰/۹۵	۰/۹۹	برازش خوب
NNFI	بیشتر از ۰/۹۰	بیشتر از ۰/۹۵	۰/۹۹	برازش خوب
GFI	بیشتر از ۰/۸۵	بیشتر از ۰/۹۰	۰/۹۷	برازش خوب
AGFI	بیشتر از ۰/۸۵	بیشتر از ۰/۹۰	۰/۹۵	برازش خوب

جدول ۵: بررسی معنی‌داری بارهای عاملی

مسیر			بار عاملی غیراستاندارد	بار عاملی استاندارد	خطای برآورد	آماره t	p-value
BI	→	**SIC**	**۰/۶۷**	**۰/۳۸**	**۰/۱۱**	**۵/۹۲**	**<۰/۰۵**
SIC10	→	SIC	۱/۰۰	۰/۷۷	۰/۰۸	۱۲/۵۷	<۰/۰۵
SIC9	→	SIC	۰/۹۱	۰/۷۵	۰/۰۷	۱۳/۶۰	<۰/۰۵
SIC8	→	SIC	۰/۹۵	۰/۷۸	۰/۰۷	۱۴/۱۶	<۰/۰۵
SIC7	→	SIC	۰/۹۳	۰/۷۶	۰/۰۷	۱۳/۷۶	<۰/۰۵
SIC6	→	SIC	۱/۱۲	۰/۷۷	۰/۰۸	۱۳/۹۶	<۰/۰۵
SIC5	→	SIC	۰/۳۰	۰/۲۱	۰/۰۹	۳/۵۱	<۰/۰۵
SIC4	→	SIC	۰/۹۹	۰/۷۹	۰/۰۷	۱۴/۳۵	<۰/۰۵
SIC3	→	SIC	۰/۹۳	۰/۷۶	۰/۰۷	۱۳/۷۱	<۰/۰۵
SIC2	→	SIC	۰/۹۵	۰/۷۴	۰/۰۷	۱۳/۲۹	<۰/۰۵
SIC1	→	SIC	۰/۹۴	۰/۷۲	۰/۰۷	۱۳/۰۳	<۰/۰۵
InBI.Score	→	BI	۱/۰۰	۰/۷۸	۰/۱۴	۱۴/۲۱	<۰/۰۵
ABI.Score	→	BI	۲/۳۷	۰/۸۶	۰/۱۵	۱۶/۰۹	<۰/۰۵
CBI.Score	→	BI	۲/۸۱	۰/۸۴	۰/۱۸	۱۵/۵۸	<۰/۰۵
AVBI.Score	→	BI	۲/۱۷	۰/۸۷	۰/۱۳	۱۶/۲۹	<۰/۰۵

با توجه به نتیجه مدل‌بندی معادلات ساختاری برای مدل مفهومی تأثیر امنیت اطلاعات (SIC) بر هوش کسب‌وکار (BI) معنی-دار و مستقیم است (p<۰/۰۵) و فرضیه تحقیق تأیید می‌گردد. به عبارتی با افزایش هوشمندی کسب‌وکار به‌طور معنی‌داری نیاز به مدیریت امنیت اطلاعات افزایش می‌یابد.

نتیجه‌گیری

با تأیید فرضیه تحقیق، تحلیل داده‌های این تحقیق با تئوری پرویچ و همکارانش[۲۹] (۲۰۱۲) مبنی بر رعایت مسائل امنیتی در پیاده‌سازی هوشمندی کسب‌وکار مطابقت دارد. نتایج به‌دست‌آمده همچنین با نتایج مطالعات پارسونز و همکاران (۲۰۱۴)، باتس (۲۰۱۵) و بروکس و همکاران (۲۰۱۵) که بر رعایت همه‌جانبه ابعاد سیستم‌های اطلاعاتی و هوشمندی کسب‌وکار به‌ویژه امنیت اطلاعات تأکید دارند، یکسان است.

سازمان در فضای سایبری هرروزه نقش پررنگ‌تری را ایفا می‌کنند و بدون تکنولوژی مدیریت و تحلیل کلان داده تجاری تعیین مسیر حرکت یک کسب‌وکار عملاً ناممکن است. داده‌ها به‌طور فزاینده‌ای در حال افزایش هستند و این داده‌ها هم‌اکنون به یکی از موارد باارزش برای نفوذگران و هکرهای تبدیل شده است که با سرقت هر چه بیشتر بتواند به اهداف مخرب خود دست‌یافته و از آن‌ها سوءاستفاده کنند. سازمان‌ها برای مقابله با افزایش خطر آسیب‌پذیری نیاز باید در سیاست‌گذاری خود در قبال داده‌های فعلی و خاص سازمان و کاربرانشان تغییر رویه دهند [۳۰].

به‌طورکلی تغییرات سریع فناوری و نوآوری‌های کسب‌وکار و تولید انبوه داده‌های ساختاریافته و بدون ساختار توسط شبکه‌های اجتماعی و تجهیزات هوشمند، باعث شده است چرخه عمر محصولات و خدمات در محیط رقابتی کسب‌وکارها کاهش یابد. در این فضا شناخت و درک هرچه بیشتر پدیده‌های نو و تصمیم‌گیری در شرایط عدم اطمینان از اهمیت بالایی برخوردار

است که از توان شخصی افراد خارج است لذا هوشمند سازی کسب‌وکار اجتناب‌ناپذیر است. امنیت اطلاعات (محرمانگی، جامعیت و دسترسی‌پذیری) باهدف تضمین تداوم عملیاتی و به حداقل رساندن خسارت‌های باعث حفظ اعتبار کسب‌وکار و به حداکثر رساندن فرصت‌های سرمایه‌گذاری از توسعه بازارهای جدید می‌شود. بدین مفهوم که حفاظت از سرمایه اطلاعاتی و حفظ حریم خصوصی افراد و آگاهی از صدمات ناشی از نقض امنیت به همراه کاهش مخاطرات محیطی می‌تواند ضامن استمرار کسب‌وکار، بازگشت سرمایه و ایجاد فرصت‌های تجاری جدید برای سازمان‌ها باشد. در راستای ایمن‌سازی فضای تبادل اطلاعات و از سال ۱۹۹۵ استانداردهای مدیریتی و گزارش‌های فنی زیادی ازجمله BS 13335، BS7799، ISO/IEC 27001، ISO/IEC TR 13335، ISO/IEC TR7799 و ISO/IEC17799 تدوین شده‌اند اما آنچه حائز اهمیت است، این است که هر سازمان باید بر اساس روش شناسی مشخص و برنامه‌ریزی‌شده متناسب بافرهنگ و راهبردهای خود به کنترل و نظارت بر اطلاعات و تبادلات اطلاعات بپردازد.

پی‌نوشت

۱. این مقاله از بخشی از رساله دکتری استخراج شده است.

2. Big Data
3. DAMA - the Data Management Association International
4. Data Management Body of Knowledge
5. Attacker-centric
6. Software-centric
7. Asset-centric
8. Confidentiality
9. Integrity
10. Availability
11. Authentication
12. Authorization
13. Accounting
14. Bates
15. Moss & Atre
16. Sangar & lahad
17. Brooks et al
18. Olbrich et al
19. Confidentiality
20. Integrity
21. Availability
22. Structural Equation Modeling
23. Analysis of Moment Structures
24. Construct validity
25. Average Variance extracted
26. Maximum shared squared variance
27. Average shared squared variance
28. Popovič et al
29. Popovič et al

منابع

[1] B. Hočevar and ;Melamin plc Kočevje, "Assessing Benefits of Business Intelligence Systems – A Case Study," J. Contemp. Manag., vol. 15, no. 1, 2010.

[2] L. Belli, S. Cirani, L. Davoli, G. Ferrari, L. Melegari, and M. Picone, "Applying Security to a Big Stream Cloud Architecture for the Internet of Things," Int. J. Distrib. Syst. Technol., vol. 7, no. 1, p. 22, 2016.

[3] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Comput. Secur., vol. 42, pp. 165–176, May 2014.

[4] J. SathishKumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," Int. J. Comput. Appl., vol. 90, no. 11, pp. 20–26, Mar. 2014.

[5] L. Uden and P. Del Vecchio, "Transforming the stakeholders' Big Data for intellectual capital management," Meditari Account. Res., vol. 26, no. 3, pp. 420–442, Aug. 2018.

[6] M. La Torre, J. Dumay, and M. A. Rea, "Breaching intellectual capital: critical reflections on Big Data security," Meditari Account. Res., vol. 26, no. 3, pp. 463–482, Aug. 2018.

[7] A. Narain Singh, M. P. Gupta, and A. Ojha, "Identifying factors of 'organizational information security management,'" J. Enterp. Inf. Manag., vol. 27, no. 5, pp. 644–667, Sep. 2014.

[8] V. Charles and T. Gherman, "Achieving Competitive Advantage Through Big Data. Strategic Implications," Middle-East J. Sci. Res., vol. 16 (8), pp. 1069–1074, 2013.

[۹] ع. ا. انصاری, "تحلیل بر ضرورت تعیین راهبردها و راهکارهای ملی داده‌های عظیم با رویکرد توسعه اقتصادی," اولین همایش داده‌های عظیم, ۱۳۹۴ ص ۶۴-۶۹

[10] M. James et al., "Big data: The next frontier for innovation, competition, and productivity," McKinsey Global Institute, 2011.

[۱۱] ع. ا. ح. هرندی, "ارائه مدل سنجش سرمایه فکری و هوش کسب‌وکار با استفاده از رویکرد سیستم داینامیک," دانشگاه آزاد اسلامی واحد تهران جنوب, ۱۳۹۷.

[12] A. A. H. Harandi, M. Safdari, and S. Esmaeili, "IPv6;

A Critical Threat Reduction Strategy," in he First Cyber Defense Conference, 2016.

[13] R. von Solms, "Information security management: The second generation," Comput. Secur., vol. 15, no. 4, pp. 281–288, Jan. 1996.

[14] D. International, DAMA-DMBOK : Data Management Body of Kn owledge (2nd Edition). Technics Publications, 2017.

[15] A. Narain Singh, M. P. Gupta, and A. Ojha, "Identifying factors of 'organizational information security management,'" J. Enterp. Inf. Manag., vol. 27, no. 5, pp. 644–667, Sep. 2014.

[16] H. Abbas, C. Magnusson, L. Yngstrom, and A. Hemani, "Addressing dynamic issues in information security management," Inf. Manag. Comput. Secur., vol. 19, no. 1, pp. 5–24, Mar. 2011.

[17] H. R. K. A. Hamidreza Arkian, Atefeh Pourkhalili, "Security and Privacy in the Internet of Things," Biannu. J. Monadi Cybersp. Secur., vol. 4, no. 2, pp. 13–35, 2016.

[18] Marcia J. Bates, "The information professions: knowledge, memory, heritage," Inf. Res., vol. 20, no. 1, 2015.

[19] P. Brooks, O. El-Gayar, and S. Sarnikar, "A Framework for Developing a Domain Specific Business Intelligence Maturity Model: Application to Healthcare.," Int. J. Inf. Manage., no. 35, pp. 337–345, 2015.

[20] Ö. Işık, M. Jones, and A. Sidorova, "Business Intelligence Success: An Empirical Evaluation of the Role of BI Capabilities and the Decision Environment.," BI Congress II: Pre-ICIS. 2010.

[21] I. A. Jamaludin and Z. Mansor, "Review on Business Intelligence (BI) Success Determinants in Project Implementation," Int. J. Comput. Appl., vol. 33, no. 8, pp. 24–27, 2011.

[۲۲] م. محمودزاده و ا. رادرجبی،، "مدیریت امنیت در سیستم‌های اطلاعاتی،" فصلنامه علوم مدیریت ایران. سال اول شماره ۴ ص ۷۸-۱۱۲، ۱۳۸۵

[۲۳] ح. اسماعیل‌پور، "شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود سیستم مدیریت امنیت اطلاعات،" پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.، ۱۳۸۸.

[۲۴] ف. ر. نیارکی و ب. عبدی، "ارائه راهکارهایی برای مدیریت امنیت اطلاعات با رویکرد مدیریت استراتژیک فناوری اطلاعات."، دومین کنفرانس بین‌المللی پارادایم‌های نوین مدیریت نوآوری و کارآفرینی. تهران، ۱۳۹۵.

[25] L. T. Moss and S. Atre, Business Intelligence Roadmap: The Complete Project Lifecycle for Decision-Support Applications. Addison-Wesley Professional, 2003.

[26] A. B. Sangar and N. B. A.Iahad, "Critical Factors That Affect The Success Of Business Intelligence Systems (BIS) Implementation In An Organization," Int. J. Sci. Technol. Res., vol. 2, no. 2, pp. 176–180, 2013.

[27] S. Olbrich, J. Pöppelbuß, and B. Niehaves, "Critical Contextual Success Factors for Business Intelligence: A Delphi Study on Their Relevance, Variability, and Controllability," in 45th Hawaii International Conference on System Sciences, 2012, pp. 4148–4157.

[28] A. Popovič, R. Hackney, P. S. Coelho, and J. Jaklič, "Towards Business Intelligence Systems Success: Effects of Maturity and Culture on Analytical Decision Making.," Decis. Support Syst., vol. 54, no. 2012, pp. 729–739, 2012.

[29] C. Valmohammadi and M. S. Mazaheri, "Clarification of factors affecting the decision to use cloud computing among IRIB employees based on a Technology Acceptance Model," IT Management Studies., vol. 5, no. 19, pp. 105–124, Apr. 2017.

[30] A. PourEbrahimi, M. B. Nia, and A. A. H. Harandi, "Architectural design The safety system is a macro security data management to manage the defenses and advanced threats to organizations," Era Inf. Technol., vol. 11, no. 113, pp. 113–120, 2016.