کاربست الگوی ساختاری - تفسیری مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد هنری-اسلامی

چکیده

امروزه اطلاعات، عامل اصلی کسب قدرت است و تسلط واقعی، تسلط اطلاعاتی است. مدیریت امنیت اطاعات مدلی را به‌منظور حفاظت از دارایی‌های اطلاعاتی سازمان ارائه می‌کند که در نتیجهٔ آن احتمال دسترسی غیرمجاز به این دارایی‌های حساس به حداقل می‌رسد. اجرای سیاست‌ها و برنامه‌های مدیریت امنیت اطلاعات می‌تواند در جهت بالابردن اخلاق کاری کارکنان کمک کند و همچنین با افزایش رعایت اخلاق کاری می‌توان مدیریت امنیت اطلاعات را در سازمان افزایش داد. مدیریت امنیت اطلاعات بنابه دلایلی که در این پژوهش در پی شناسایی آن هستیم تاکنون به‌درستی محقق نشده است، پژوهش حاضر با هدف غایی«کاربست الگوی ساختاری - تفسیری مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد هنری- اسلامی» و با استفاده از روش تحقیق نظریه داده‌بنیاد، روش جمع‌آوری داده مصاحبه، نمونه‌گیری نظری و گلوله برفی انجام و با ۱۷ مصاحبه اشباع نظری آن حاصل شد. مجموعه‌ای از مضامین اولیه طی فرآیند کدگذاری باز، گردآوری و از دل آن‌ها مقوله‌هایی استخراج گردید. سپس در مرحله کدگذاری محوری، پیوند میان این مقوله‌ها ذیل عناوین شرایط علی، مقوله محوری، راهبردها، بستر، شرایط مداخله‌گر و پیامدها در قالب پارادایم کدگذاری تعیین شدند. بعد از پژوهش کیفی براساس مدل به‌دست آمده، پرسش‌نامه‌ای تنظیم و از ۳۸۴ نفر از مدیران و کارشناسان آشنا و مرتبط با حوزه مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران، پاسخ‌ها جمع‌آوری و مورد تجزیه‌وتحلیل قرار گرفت. نتایج به‌دست آمده از تجزیه‌وتحلیل داده‌ها کلیات مدل استخراج شده از داده‌های کیفی را مورد تأیید قرار داد و براساس آن پیشنهاداتی ارائه گردید.

اهداف پژوهش:

۱. بررسی رویکرد هنری و اسلامی در مدیریت امنیت اطلاعات سازمانی.

۲. بررسی چارچوب و ساختار تفسیری امنیت اطلاعات سازمان‌های ایران.

سؤالات پژوهش:

۱. رویکرد هنری- اسلامی در مدیریت امنیت اطلاعات سازمانی چه تأثیری دارد؟

۲. چارچوب و ساختار تفسیری امنیت اطلاعات سازمان‌های ایران به چه شکل باشد؟

کلیدواژه‌ها: مدیریت امنیت اطلاعات، الگوی ساختاری-تفسیری، رویکرد اسلامی، رویکرد هنری.

مقدمه

اطلاعات مهم‌ترین گنجینه سازمان‌ها و اشخاص می‌باشد که از بین رفتن و حتی کوچک‌ترین آسیب به آن، نیازمند صرف زمان، هزینه و نیروی کار تصورناپذیری برای جبران است و در برخی مواقع اصول کاری و موجودیت یک سازمان را تهدید می‌کند (موسوی، ۱۳۹۴). حیات سازمان‌ها ارتباط نزدیکی با سیستم اطلاعاتی آن‌ها دارد (تاج‌فر، ۱۳۹۳) و این اهمیت تا جایی است که عده‌ای آن را به خونی در رگ‌های سازمان تشبیه کرده و آن را عامل حیات‌بخش سازمان می‌دانند (مسکل[۱] و همکاران، ۲۰۱۵). چون سازمان‌ها، بسیاری از منابع و امتیازاتشان را از محیط اطراف کسب می‌کنند، چنانچه نتوانند امنیت اطلاعات سازمان و یا افراد مرتبط با سازمان را حفظ نمایند به تدریج جایگاه و اعتبارشان را از دست داده و دیگر نمی‌توانند موفق باشند. مهم‌ترین مطلبی که در مورد امنیت باید موردتوجه قرار گیرد این است که بُعد انسانی و رفتار انسانی در این مقوله مهم و حیاتی می‌باشد، زیرا این انسان‌ها هستند که از سیستم‌ها و اطلاعات استفاده کرده و می‌توانند خواسته یا ناخواسته امنیت اطلاعات را زیر سوال ببرند (صالحی، ۱۳۹۶).

مدیریت امنیت اطلاعات به دو بخش عمده فنی و مدیریتی تقسیم می‌شود که ادغام این دو جنبه کارایی امنیت اطلاعات را تضمین خواهد کرد (یانگ[۲]، ۲۰۱۴)؛ لیکن برخی از پژوهشگران حوزه امنیت معتقدند طی سال‌های اخیر مسلم شده است که امنیت اطلاعات دیگر یک موضوع فنی نیست، بلکه مسئله‌ای مدیریتی محسوب می‌شود (نادری، ۱۳۹۶). در یکی از تحقیقات (بهاتاچاریا[۳]، ۲۰۱۱) عامل انسانی به‌عنوان پاشنه آشیل امنیت اطلاعات معرفی شده است. امروزه به‌نظر می‌رسد موفقیت امنیت اطلاعات تا حد زیادی به رفتار اثربخش کارکنان و مدیران وابسته است (هاگن، ۲۰۱۱). امروزه اطلاعات عامل اصلی کسب قدرت است و تسلط واقعی، تسلط اطلاعاتی است. جنگ میان کشورهای غنی و فقیر درواقع جنگ اطلاعاتی است و کشورهای سلطه‌گر که خواستار استمرار بهره‌جویی خود از منابع و ثروت کشورهای عقب مانده هستند، علاقه‌ای به ایجاد زیربناهای اطلاعاتی در این کشورها ندارند (جهرمی، ۱۳۹۶).

محمدی و همکاران (۱۳۹۸)، به مقایسه الگوریتم‌های بیمار محور برای امنیت اطلاعات سلامت در شبکه‌های اجتماعی سلامت و محیط ابر پرداختند. در این پژوهش، جست‌وجو مقالات در فاصلهٔ زمانی ۲۰۰۹-۲۰۱۹ انتخاب شده‌اند. ۲۹ مقاله برای حل مسئله لغو کاربر و ۷ مقاله برای حل مسئله کنترل دسترسی انتخاب شده است. به‌منظور حفظ محرمانگی اطلاعات بیماران، روش رمزنگاری قبل از به اشتراک‌گذاری پیشنهاد شده است. این راه حل مشکل لغو کاربر را دارد. برای حل این مشکل روش‌های مختلفی ارائه شده است. این راه‌حل‌ها از جنبه‌های مختلف کوتاه بودن زمان لغو، به‌روزرسانی متن رمز شده، آزادبودن محیط ابر، تناوب در به‌روزرسانی کلید و لغو فوری متفاوت هستند. همچنین روش‌هایی برای کنترل دسترسی اطلاعات توسط بیمار ارائه شده است. مسائل مربوط به امنیت اطلاعات سلامت باعث می‌شود بیماران نسبت به ارسال اطلاعات حساس لامت خود و اشتراک آن با ارائه‌دهندگان خدمات سلامت مردد باشند. در این پژوهش، الگوریتم‌ها و روش‌های امنیت اطلاعات سلامت مقایسه شده‌اند. اکثر راه‌حل‌های لغو کاربر به رمزنگاری مجدد نیاز دارند. همچنین راه‌حل‌های کنترل دسترسی انعطاف‌پذیری لازم ندارند. از این‌رو در آینده باید روش‌های بهتری ارائه شوند.

---

[۱] Meskel
[۲] Yang
[۳] Bhattacharya

امینی و همکاران (۱۳۹۸)، در پژوهشی به شناسایی عوامل مؤثر بر مدیریت امنیت اطلاعات کتابخانه‌ها و مراکز اطلاع رسانی دانشگاه علوم پزشکب همدان پرداختند. براساس نتایج مطالعه، سازه اجرایی با میانگین ۴۶/۴ در رتبه اول و با بیشترین اثرگذاری در سیستم مدیریت امنیت اطلاعات و سازه نیروی‌انسانی با میانگین ۵۶/۳ در رتبه هفتم و با کم‌ترین اثرگذاری شناسایی شد. برای ارتقاء سطح امنیت اطلاعات ضروری است که مدیران ارشد با مشخص‌نمودن اهداف امنیتی مرتبط با سازمان، ایجاد مدیریتی جامع و یکپارچه، تلاش برای رعایت قوانین و استانداردهای امنیتی، در دست داشتن منابع و بودجه کافی و ایجاد انگیزه در بین کتابداران و اطلاع‌رسانان، بستر مناسبی را فراهم آورند تا ارائه خدمات مطلوب‌تر گردد و همچنین بتوانند گامی مؤثر در جهت افزایش تولیدات علمی دانشگاهی داشته باشند. حدادی هرندی و همکاران (۱۳۹۸) به بررسی مدیریت امنیت اطلاعات در کسب و کار هوشمند پرداختند. در این پژوهش با استفاده از ادبیات تحقیق و مدل بلوغ سیستم‌های هوشمند کسب و کار، مدلی تبیین و پرسش‌نامه‌ای طراحی و توسط ۳۰۵ نفر از مدیران، کارکنان دانشی و کارشناسان بخش حمل‌ونقل دولتی تکمیل شده است. با استفاده از تحلیل عاملی تأییدی و تجزیه‌وتحلیل مسیر، سازه‌های مدل بررسی و داده‌های جمع‌آوری شده توسط نرم‌افزار AMOS تحلیل شدند. نتایج نشان می‌دهد که امنیت اطلاعات با ضریب رگرسیونی ۰/۳۸ تأثیر مستقیم بر امنیت اطلاعات درد. به عبارت دیگر، امنیت اطلاعات با هدف تضمین تداوم و به حداقل رساندن آسیب‌ها و تهدیدات سایبری، باعث حفظ و ارتقاء کسب و کار و به حداکثر رساندن فرصت‌های سرمایه‌گذاری از طریق توسعه بازارهای جدید می‌شود.

دهقانی و همکاران (۱۳۹۸) به بررسی آگاهی، نگرش و عملکرد کارکنان بخش مدیریت اطلاعات سلامت بیمارستان‌های ایران نسبت به امنیت اطلاعات سلامت پرداختند. این مطالعه توصیفی- تحلیلی در سال ۱۳۹۷ برروی ۳۶۷ نفر از کارکنان بخش مدیریت اطلاعات سلامت بیمارستان‌های ایران انجام شده است. میانگین امتیازات آگاهی، نگرش و عملکرد شرکت‌کنندگان در زمینهٔ مدیریت امنیت اطلاعات به ترتیب ۰/۶۷ ، ۳/۵۳ و ۱/۴۷ به‌دست آمده است. همچنین رابطهٔ مستقیم و معناداری بین نمره کسب شده در هر یک از این سه بعد با سن، سابقه کار، مقطع تحصیلی و رشته تحصیلی وجود دارد. باتوجه‌به وضعیت آگاهی، نگرش و عملکرد کارکنان، می‌توان با برگزاری دوره‌های آموزشی و ضمن خدمت، وضعیت امنیت اطلاعات سلامت در بیمارستان‌ها را ارتقا داد.

رضوانی، شهلا (۱۳۹۷) در پژوهشی با عنوان «طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی» دریافت که سیستم‌ها و معماری‌های سازمانی و ممیزی کمک شایانی به استقرار سیستم‌های امنیت در سازمان‌ها خواهند نمود. پایه‌ریزی تحقیقات دربارهٔ سیستم‌های سازمانی و معماری‌های مختلف، یکی از نیازمندی‌های ضروری محسوب می‌شود و لازم است محققان قدم‌های اساسی در این جهت بردارند. پیاده‌سازی سیستم‌های بهینه تعریف شده، نیاز اعتمادسازی در سازمان‌ها و ارائه منابع تحقیقات به سازمان‌ها، در پذیرش این معماری تأثیرگذار خواهند بود.

رضایی، علی و همکاران (۱۳۹۷) در پژوهشی با عنوان «عوامل مؤثر بر اثربخشی سیستم مدیریت امنیت اطلاعات» دریافتند که شاخص‌های نقش مدیریت، آگاهی از سیستم امنیت اطلاعات و انطباق با آموزش، امنیت سیستم اطلاعات کسب و کار و ارزیابی ریسک امنیت سیستم اطلاعات بر اثربخشی سیستم مدیریت امنیت اطلاعات تأثیرگذار می‌باشد.

پارک[۴] و همکاران (۲۰۱۷)، نقش آموزش امنیت اطلاعات و عوامل فردی در افشای اطلاعات سلامت بیماران را بر گسترش امنیت اطلاعات بررسی کردند. باتوجه‌به بیشتر شدن اهمیت اجابت مقررات و سیاست‌های امنیت اطلاعات

---

[۴] - Park

به‌وسیلهٔ کارکنانی که در صنعت مراقبت‌های بهداشتی کار می‌کنند، بحث امنیت اطلاعات در مراکز درمانی از اهمیت بیشتری برخوردار شده است. همچنین یافته‌های این پژوهش نشان دادند امنیت اطلاعات و ارزش‌های شخصی در آموزش پرستاری و تلاش صنعت مراقبت‌های بهداشتی برای حفاظت از اطلاعات سلامت بیماران نقش جالب توجهی دارند.

وایگا و مارتینز[۵] (۲۰۱۷)، در پژوهش بهبود فرهنگ امنیتی اطلاعات از طریق اقدامات نظارت و پیاده‌سازی که بین ۵۱۲ نفر از کارکنان در آفریقای جنوبی انجام دادند، به این نتیجه رسیدند که ابزار ارزیابی فرهنگ امنیت اطلاعات می‌تواند در سازمان‌ها به‌طور موفقیت‌آمیزی بر فرهنگ امنیت اطلاعات تأثیر بگذارد. همچنین آموزش امنیت اطلاعات و آگاهی عاملی مهم در تأثیرگذاری مثبت بر فرهنگ امنیت اطلاعات است. آن‌ها نشان دادند فرهنگ و خرده‌فرهنگ‌های امنیتی اطلاعات غالب در طول زمان پس از اجرای مداخلات هدفمند به یک فرهنگ امنیتی اطلاعاتی مثبت‌تر بهبود یافته است. پارسونز[۶] و همکاران (۲۰۱۴)، در پژوهش خود که بر روی ۵۵۲ کارمند استرالیایی انجام شده است، نشان دادند که روش‌ها و سیاست‌های دانشی نفوذ قوی‌تری نسبت به تعریف افراد از رفتار خود داشته است. این یافته‌ها بیانگر این است که آموزش و پرورش خیلی بیشتر از آنچه انتظار می‌رود می‌تواند در ایجاد دانش مناسب برای استفاده از سیستم‌های اطلاعاتی و امنیت سیستم‌ها، نگرش ایجاد نماید.

نتیجه‌گیری

وجود استانداردهای گوناگون مدیریت امنیت اطلاعات در جهان و ملزم‌کردن سازمان‌ها و نهادهای داخلی به اجرای آن، هرچند به‌صورت نمادین امکان‌پذیر است لیکن پیاده‌سازی و اجرایی‌کردن دستورالعمل‌های واقعی مندرج در آن، باید در قالب مدل معینی در اختیار سازمان‌ها قرار گیرد. پذیرش مدیریت امنیت اطلاعات مستلزم شناسایی موانع و مشکلات آن و در نهایت شناسایی راهبردهایی برای پذیرش و به‌کارگیری آن است. در راستای نیل به اهداف و نیز پاسخ به پرسش پژوهش، پس از اجرای راهبرد پژوهشی کیفی نظریه‌پردازی داده‌بنیاد، طراحی و تبیین الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد اسلامی با اجزای آن استخراج گردید. در روش نظریه‌پردازی داده‌بنیاد پاسخ به پرسش پژوهش، همان الگوی به‌دست آمده و عناصر آن می‌باشد. در حقیقت، یافته‌های پژوهش؛ مقوله‌ها و مؤلفه‌های آن می‌باشند که در این پژوهش، در قالب الگو بیان شده‌اند (دانایی‌فرد و امامی، ۱۳۸۶). از آنجا که در روش داده‌بنیاد، نظریهٔ جدیدی به‌وجود آمده است لذا همه یافته‌ها قابل مقایسه با ادبیات پیشین نبوده و برای بررسی کامل، بایستی در پژوهش‌های آتی مورد بررسی بیشتر و ارزیابی قرار گیرند. الگوی مدیریت امنیت اطلاعات دارای مزایای مختلفی از قبیل بهبود اعتماد سازمانی، تقویت امنیت ملی، تعالی جامعه، امنیت فیزیکی و تقویت امنیت ملی و ... است. این امر میسر نمی‌شود مگر اینکه قبل از آن مدیریت امنیت اطلاعات مورد پذیرش واقع شود. مهم‌ترین مطلبی که در مورد مدیریت امنیت اطلاعات باید موردتوجه قرار گیرد این است که بُعد انسانی و رفتار انسانی در این مقوله بسیار مهم و حیاتی می‌باشد، زیرا این انسان‌ها هستند که از سیستم‌ها و اطلاعات استفاده کرده و می‌توانند خواسته یا ناخواسته امنیت اطلاعات را زیر سؤال ببرند. باید توجه داشت که در دنیای امروز چیزی به‌عنوان امنیت مطلق و کامل نمی‌تواند وجود داشته باشد، امروزه چه دنیای واقعی و چه دنیای مجازی مانند زندان شیشه‌ای هستند که همیشه احتمال نشر و گسترش اطلاعات به‌صورت ناخواسته و غیرمجاز در آن وجود خواهد

---

۵ Veiga. & Martins
۶ Parsons

داشت اما می‌توان با رعایت برخی مسائل احتمال وقوع این اتفاقات را به مقدار قابل‌ملاحظه‌ای کاهش داد. همان‌طور که قبلاً بیان شد نظام مدیریت امنیت اطاعات به‌عنوان یک راهکار جامع مدیریتی و فنی برای مقابله با مخاطرات امنیتی پذیرفته شده است. لیکن پیاده‌سازی آن نیازمند وجود یک الگوی جامع است (نقیان فشارکی، ۱۳۹۳).

فهرست منابع و مآخذ:

آرام، محمدرضا. (۱۳۸۸). «بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات شرکت گاز پارس جنوبی». پایان‌نامه کارشناسی ارشد دانشگاه شهید بهشتی.

امینی، معصومه؛ وکیلی مفرد، حسین؛ صابری محمدکریم. (۱۳۹۸). «شناسایی عوامل موثر بر مدیریت امنیت اطلاعات کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان». تحقیقات کتابداری و اطلاع‌رسانی دانشگاهی، ۳، ۵۳.

حدادی هرندی، علی‌اکبر؛ والمحمدی، چنگیز و صالحی صدقیانی، جمشید. (۱۳۹۸). «مدیریت امنیت اطلاعات در کسب و کار هوشمند». علمی پژوهشی مدیریت بحران ۸، (ویژه‌نامه هوشمندسازی)، ۲۵-۳۳.

دانایی‌فرد، حسن؛ ابدالی، رقیه؛ محمودی کوچکسرایی، علی‌اصغر. (۱۳۹۹). «پژوهش‌های فساد و سلامت اداری در ایران: مرور دامنه‌ای (حیطه‌ای)»، دانش حسابرسی،۲۰(۷۹)، ۲۰۱-۲۱۸.

دانایی‌فرد، حسن؛ رجب‌زاده، علی؛ حصیری، اسد. (۱۳۸۸). «ارتقا اعتماد درون سازمانی در بخش دولتی: بررسی نقش شایستگی مدیریتی مدیران». پژوهش‌های مدیریت، شماره چهارم، ۵۹-۹۰.

دهقانی، محمد؛ رحمت‌پسند فتیده، زری؛ آراسته، زهرا؛ شکری‌زاده بزنجانی و کبری، آگاهی. (۱۳۹۸). «نگرش و عملکرد کارکنان بخش مدیریت اطلاعات سلامت بیمارستان‌های ایران نسبت به امنیت اطلاعات سلامت». مجله مدیریت اطلاعات سلامت، شماره اول، ۹-۳.

شمس، شهاب‌الدین؛ اسفندیاری مقدم، امیر. (۱۳۹۴). «ارتباط ابعاد مختلف اعتماد سازمانی با رضایت شغلی کارکنان». مطالعات مدیریت (بهبود و تحول)، شماره ۷۷، ۱۷۱- ۱۸۵.

عاشوری‌زاده، سهیلا. (۱۳۹۱). «رابطه فرهنگ سازمانی با مدیریت امنیت اطلاعات در بانک ملی ایران». پایان‌نامه کارشناسی ارشد. دانشگاه علامه طباطبایی.

محمدی، مهین؛ شیخ ظاهری، عباس؛ کرمانی، فرزانه. (۱۳۹۸). «مقایسه الگوریتم‌های بیمار محور برای امنیت اطلاعات سلامت در شبکه‌های اجتماعی سلامت و محیط ابر». مجله اطلاع‌رسانی پزشکی نوین، دوره پنجم، شماره دوم، ۶۸-۷۹.

میوالد، اریک. (۱۳۸۵). مبانی امنیت شبکه. ترجمه: گروه پژوهشی فناوری اطلاعات جهاد دانشگاهی صنعتی شریف. تهران: انتشارات انستیتو ایز ایزان.

Boritz, J. E. (۲۰۰٤). *Managing enterprise information integrity: security, control, and audit issues*. Isaca.

Chang. E. (۲۰۰۷). An Investigation of Organizational Culture on Information Security Management. Academy of Management Journal, ۳۵: ٤۲۱-٤۳۸.

Chathoth, P. K., Mak, B., Sim, J., Jauhari, V., & Manaktola, K. (٢٠١١). Assessing dimensions of organizational trust across cultures: A comparative analysis of US and Indian full service hotels. *International Journal of Hospitality Management*, *30* (٢), ٢٣٣-٢٤٢.

Hansche, S. (٢٠٠١). Designing a security awareness program: Part ١. *Information systems security*, *9* (٦), ١-٩.

Heidari, S., & Mohammadi, S. (٢٠١٢). A New Model for Information Security Management in Service-Oriented Enterprise Architecture. *American Journal of Scientific Research*, (٧٦), ١١٤-١٣٢.

Ho, S. M. (٢٠٠٨). A Framework of Coordinated Defense. In *Proceedings of the Second International Conference on Computational Cultural Dynamics* (pp. ٣٩-٤٤).

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (٢٠٠٣). An integrated system theory of information security management. *Information Management & Computer Security*.

Kadam, A. W. (٢٠٠٧). Information security policy development and implementation. *Information Systems Security*, *16* (٥), ٢٤٦-٢٥٦.

Kambwiri, L. (٢٠١٢). An Appraisal of Information Security Management at Chancellor College, University of Malawi.

Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S., & Ramanauskaite, S. (٢٠١٧). High-level self-sustaining information security management framework. *Baltic Journal of Modern Computing*, *5* (١), ١٠٧.

Kline, R. B. (٢٠١١). Principles and practice of structural equation modeling: Guilford press.

Kim, S., Kim, S., & Lee, G. (٢٠٠٩). Structure design and test of enterprise security management system with advanced internal security. *Future Generation Computer Systems*, ٢٥(٣), ٣٥٨-٣٦٣.

Mitchell, R. C., Marcella, R., & Baxter, G. (١٩٩٩). Corporate information security management. *New Library World*.

Park, E. H., Kim, J., & Park, Y. S. (٢٠١٧). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, *65*, ٦٤-٧٦.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (٢٠١٤). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, ١٦٥-١٧٦.

Veiga. A. & Martins, N. (٢٠١٧) "Defining and Identifying Dominant Information Security Cultures and Subcultures." Computers & Security, ٧٠: ٧٢-٩٤.

Vermeulen, C., & Von Solms, R. (٢٠٠٢). The information security management toolbox–taking the pain out of security management. *Information management & computer security*.

Whitener, E. M. (٢٠٠١). Do "high commitment" human resource practices affect employee commitment? A cross-level analysis using hierarchical linear modeling. *Journal of management*, *27* (٥), ٥١٥-٥٣٥.

Whitener, E. M., Brodt, S. E., Korsgaard, M. A., & Werner, J. M. (١٩٩٨). Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior. *Academy of management review*, *23* (٣), ٥١٣-٥٣٠.

Whitley, R. (١٩٩٩). *Divergent capitalisms: The social structuring and change of business systems*. OUP Oxford.

Whitman, M. E., & Mattord, H. J. (٢٠١١). *Principles of information security*. Cengage Learning.