

چکیده

در دنیای کنونی، مباحث مرتبط با امنیت اطلاعات، تبدیل به یکی از مشکلات بخش‌های دولتی و خصوصی در همه کشورها شده است. با توجه به تفاوت‌های فرهنگی و میزان اهمیت و توجه به احترام به حریم خصوصی افراد، پیاده‌سازی سیستم‌های امنیت اطلاعات در کشورهای مختلف می‌تواند تفاوت‌هایی را در برداشته باشد. مقاله حاضر در رابطه با شناسایی عوامل شکست پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در کشورهای در حال توسعه و با بررسی موردی بر سازمان‌های ایرانی است. مفهوم کلیدی ISMS برای سازماندهی، طراحی، پیاده‌سازی و نگهداری مجموعه‌ای منسجم از فرآیندها و سیستم‌ها به منظور مدیریت کردن دستیابی‌پذیری اطلاعات بطور موثر است. در این مقاله ابتدا تحقیقات مختلف که به برخی از موانع پیاده‌سازی ISMS اشاره کرده بودند، با مطالعات کتابخانه‌ای جمع‌آوری شد و این عوامل استخراج گردید. سپس این موانع از طریق روش دلفی تکمیل و نهایی گردید. در فرآیند دلفی از نظرات ۱۹ صاحب‌نظر استفاده شد که این افراد از بین اساتید هیئت علمی دانشگاه‌های مختلف که دارای تحصیلات، تخصص و تجربه در زمینه امنیت اطلاعات بودند و همچنین محققان و مجریان در زمینه ISMS انتخاب شدند. در نهایت به دلیل امکان دسترسی محققین به سازمان‌های ایرانی، ۱۸ عامل در طی ۴ مرحله به عنوان موانع پیاده‌سازی ISMS در سازمان‌های ایرانی شناسایی شدند.

واژگان کلیدی: ISMS، مدیریت امنیت اطلاعات، امنیت اطلاعات، سیاست امنیت، کشورهای در حال توسعه.....

استخراج عوامل شکست پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در کشورهای در حال توسعه (با تمرکز بر سازمان‌های ایرانی)

مجتبی امیری

دانشیار دانشکده مدیریت دانشگاه تهران

mamiry@ut.ac.ir

خدیدجه روزبهانی

دانشکده مدیریت دانشگاه تهران

rrouzbehani@ut.ac.ir

مصطفی زمانیان

دانشکده مدیریت دانشگاه تهران

zamanyan@ut.ac.ir

مقدمه

ظهور فناوری ارتباطات و اینترنت امکان «اشتراک اطلاعات» و «تبادل آسان اطلاعات» بین سیستم‌های رایانه‌ای را به وجود آورده است. این فناوری‌های نوین با غلبه بر فاصله‌ها و محدودیت‌های فیزیکی و کاهش محسوس زمان، معماری و ساختار ارائه خدمات در سیستم‌ها را به شدت تحت تاثیر قرار داده‌اند. بدیهی است که در این شرایط روش‌های حفاظت فیزیکی به تهایی قادر به تامین امنیت نخواهند بود. بنابراین سازمان‌ها مجبور به استفاده از روش‌های جدید حفاظت اطلاعات و کنترل دسترسی‌ها به منابع سازمان شوند.

در چنین شرایطی بسیاری از سازمان‌ها به پذیرش استانداردهای مدیریت امنیتی منتشرشده اقدام نموده‌اند. Lin و Fung ، Farn سال ۲۰۰۳ در رابطه با استفاده از استانداردها بیان کرده‌اند که با کمک استانداردها، می‌توان مشکلات ناشی از اطلاعات ناقص را کاهش داد. همچنین می‌توان فرآیندهای تصمیم‌گیری مرتبط با عرضه و تقاضای قابل اطمینان را ساده نمود [۸].

همچنین استانداردها، امری مناسب برای اطمینان از رعایت امنیت اطلاعات در سازمان‌ها محسوب می‌گردند و از آنجا که در دنیای امروز و با توجه به پدیده‌هایی مانند تجارت الکترونیک، دیگر امنیت اطلاعات مسئله‌ای داخلی (domestic issue) محسوب نمی‌شود و روی شرکای هر سازمان اثر می‌گذارد، استانداردها ابزار خوبی برای اطمینان از سطح قابل قبولی از امنیت در سازمان‌ها هستند [۱۶]. بدین ترتیب به منظور جلوگیری از نفوذهای ناخواسته امنیتی لازم است که استاندارد مدیریت امنیت اطلاعات مناسبی به کار گرفته شود تا به پیاده‌سازی سیستم مدیریت امنیت اطلاعات (Information Security Management System) در سازمان کمک نماید.

از سوی دیگر عموماً فرض بر این بوده که پیشرفته‌ترین فناوری مورد استفاده در کشورهای توسعه یافته را می‌توان با [حداکثر] کارایی و سهولت در کشورهای در حال توسعه نیز مورد استفاده قرار داد. در اوایل دهه ۱۹۷۰ ضرورت انتقال مستقیم و انبوه فناوری پیشرفته به کشورهای در حال توسعه به صورت گسترده‌ای مورد بحث قرار گرفت. از آن پس رفته‌رفته مشخص شد که عرضه عملکردهای بسیار پیچیده و سرمایه‌بر، به جای حل مسئله باعث افزایش مشکلات می‌گردد [۱۳].

«سونیلسن» درباره راهبرد انتقال فناوری در کشورهای در حال توسعه اظهار می‌دارد: «برای پایه‌گذاری فناوری نوین در کشورهای در حال توسعه باید نظام‌های اجتماعی و گرایش‌های انسانی، دانش و مهارت‌های انسانی و ابزارهای فیزیکی که فن‌آوری در قالب آن‌ها عینیت می‌یابد را تغییر دهیم.» [۶]. به این ترتیب هر کشوری باید در پی ایجاد فرآیند بومی تولید علم باشد. زیرا شکاف عمیق و فزاینده بین استانداردهای زندگی در کشورهای توسعه یافته و در حال توسعه، ناشی از فاصله علمی و فنی بین آن‌هاست. در واقع چیزی که ملت‌های غنی را از فقیر متمایز می‌کند، نه تنها تولید ثروت‌های مادی بلکه میزان تولید علمی و دستیابی به دانش بهره‌گیری مناسب از منابع موجود است [۲].

با توجه به تفاوت‌های فرهنگی و درجه احترام و حفظ حریم خصوصی افراد در کشورهای توسعه یافته و کشورهای در حال توسعه، کپی‌برداری در پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات به نظر مشکل‌ساز می‌آید. ذکر برخی از این تفاوت‌ها می‌تواند به شناخت و اهمیت این تفاوت کمک کند. در کشورهای توسعه یافته احترام به حریم خصوصی افراد بسیار اهمیت دارد. برای مثال پرسیدن اطلاعات شخصی افراد از قبیل میزان حقوق دریافتی فرد امری ناپسند است، در صورتی که در کشوری مانند ایران سوال در مورد حقوق دریافتی فرد حتی در حضور جمع، امری عادی و پذیرفته است و یا می‌دانیم که رمز کارت‌های اعتباری در کشورهای توسعه یافته بسیار محرمانه تلقی می‌شود و حتی هنگام خرید و پرداخت با کارت اعتباری، فروشنده در هنگامی که خریدار می‌خواهد رمزش را وارد دستگاه کند، رویش را بر می‌گرداند تا خریدار مطمئن شود که رمز او را نمی‌بیند. ولی در ایران فروشنده در حضور دیگران از خریدار می‌خواهد تا رمز کارتش را با صدای بلند بگوید تا فروشنده خودش آن را وارد دستگاه کند و این امر موضوعی عادی و پذیرفته شده است و افراد به راحتی رمز کارت‌های خود را در

اختیار یکدیگر قرار می‌دهند.

از این روست که به نظر می‌رسد کپی‌برداری از کشورهای توسعه‌یافته در پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات در کشورهای در حال توسعه نیاز به بازنگری دارد. لازم است تا پژوهش‌هایی در این زمینه صورت گیرد تا مشکلات پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات در کشورهای در حال توسعه را با توجه به تفاوت‌های ذکر شده مورد مطالعه قرار دهند.

این مقاله به دنبال پاسخ به یک پرسش اصلی است: چگونه می‌توان با استفاده از تکنیک دلفی عوامل شکست پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) را در میان کشورهای در حال توسعه (با مطالعه موردی بر سازمان‌های ایرانی) استخراج نمود؟ بر مبنای دانش محققین این پژوهش، در رابطه با موانعی که بطور کلی پیش‌روی پیاده‌سازی سیستم مدیریت امنیت اطلاعات وجود دارد، پژوهش جامع و کاملی انجام نشده است. اما برخی از پژوهشگران بصورت جسته و گریخته در مقالات مختلف به پاره‌ای از این موانع اشاره نموده‌اند.

مثلاً Dhillon در سال ۲۰۰۱، عدم تبادل نظر مدیران سازمان به هنگام اتخاذ تصمیمات مرتبط با امنیت اطلاعات با سایر پرسنل سازمانی را به عنوان یکی از موانع پیاده‌سازی ISMS مطرح نمود. همچنین به عقیده او در سازمانی که هم‌راستایی میان سیاست‌های امنیتی با فلسفه سازمانی وجود نداشته باشد، پیاده‌سازی ISMS با مشکل مواجه می‌گردد [۴]. در پژوهشی دیگر که در سال ۲۰۰۸ توسط Fomin صورت پذیرفت، این نتیجه حاصل گشت که ممکن است که هزینه‌های بالای مالی و زمانی پیاده‌سازی سیستم مدیریت امنیت اطلاعات، به ایجاد مقاومت در قبول ISMS بینجامد. این مقاومت ممکن است که از سوی متخصصان IT (مثل CIOها، مشاوران IT و ...) در مراحل مختلف پیاده‌سازی سیستم مدیریت امنیت اطلاعات و به دلایل مختلف باشد.

همچنین به عقیده Fomin برون‌سپاری خدمات IT در موافقی می‌تواند پیاده‌سازی سیستم مدیریت امنیت اطلاعات را دشوار نماید [۷]. Smith و Kritzingr نیز در سال ۲۰۰۸ یکی از موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات را در عدم وجود دانش کافی در رابطه با تهدیدات امنیت اطلاعات می‌دانند. در ادامه، به بررسی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات در پژوهش حاضر می‌پردازیم.

۲- روش پژوهش

در گردآوری اطلاعات از هر دو منبع اطلاعات اولیه و ثانویه بهره گرفته شده است. اطلاعات ثانویه برگرفته از مطالعات کتابخانه‌ای، جستجو در اینترنت، مطالعه مقالات، کتب، مجلات، پایان‌نامه‌ها و سایر پایگاه‌های علمی معتبر است. همچنین از آنجایی که در بسیاری از موارد برای تصمیم‌گیری، اطلاعات کامل و دقیقی از گذشته در دست نیست و یا محیط به گونه‌ای آشفته است که نمی‌توان اطلاعات گذشته را ملاک پیش‌بینی آینده و تصمیم‌گیری قرار داد، در چنین شرایطی تحلیل‌گر برای پیش‌بینی آینده به روش‌های کیفی متوسل می‌شود [۱]. در این پژوهش نیز از آنجایی که چارچوبی از پیش تعیین شده مانند نظریه یا مدل در شناسایی موانع سیستم مدیریت امنیت اطلاعات وجود ندارد، محققین از روش دلفی جهت شناسایی موانع مربوطه بهره جستند.

همچنین از آنجا که امکان دسترسی به اطلاعات کلیه کشورهای در حال توسعه برای محقق میسر نیست و با توجه به در دسترس بودن اطلاعات سازمان‌های ایرانی، شرکت‌های ایرانی برای این پژوهش انتخاب شده‌اند. علاوه بر این، با توجه به تشابهات فراوان مشکلات اقتصادی، اجتماعی، فرهنگی و بحران‌های سیاسی و مدیریتی نتایج این پژوهش را در سایر کشورهای در حال توسعه نیز می‌توان مفروض دانست. پژوهشگران بعدی نیز می‌توانند به تست این فرضیات در سایر کشورهای در حال توسعه بپردازند.

۲-۱- روش دلفی

روش دلفی (Delphi method) که به وسیله شرکت راند برای پیش‌بینی‌های کیفی پیشنهاد شده، روشی است که بر اساس نظر یک گروه از متخصصان و یک نفر هماهنگ‌کننده شکل می‌گیرد. همچنین هیچ عضوی از گروه از سایر اعضای آن خبر ندارد، بلکه همه ارتباطات از طریق هماهنگ‌کننده اصلی انجام می‌گیرد [۱].

۲-۱-۱- نحوه اجرای روش دلفی

به منظور اجرای روش دلفی در این پژوهش، در ابتدا به بررسی مقالات مختلف که در زمینه «موانع پیاده‌سازی ISMS» در سایر کشورها صورت پذیرفته بود پرداخته شد. سپس عواملی که به عنوان موانع پیاده‌سازی این استاندارد در هر یک از مقالات اشاره شده بود استخراج گردید. پس از آن این عوامل دسته‌بندی شده و در قالب پرسشنامه‌ای طراحی گردید. بر همین اساس

پرسشنامه‌ای در دو قسمت طراحی گردید.

قسمت اول پرسشنامه فهرستی از موانعی را شامل می‌شد که از پژوهش‌های پیشین استخراج شده بود. هدف از بیان این موانع تعیین میزان اهمیتشان در سازمان‌های ایرانی در مقیاس ۱ (کمترین میزان اهمیت) تا ۵ (بیشترین میزان اهمیت) بود. در قسمت دوم از افراد خواسته شد تا چنانچه عواملی علاوه بر عوامل مطرح شده را به عنوان موانع پیاده‌سازی ISMS در سازمان‌های ایرانی می‌شناسند بیان نمایند. در مرحله تهیه پرسشنامه موانع مطرح شده از جهت واژه‌پردازی و عدم ابهام مورد آزمایش قرار گرفت و از افرادی خارج از حیطه تحقیق خواسته شد تا برداشت‌های خود را از هر عبارت مطرح نمایند.

موانعی که در تدوین پرسشنامه مورد استفاده واقع شد، عبارتند از:

- ۱- عدم تبادل نظر مدیران سازمان به هنگام اخذ تصمیمات مرتبط با امنیت اطلاعات با سایر پرسنل سازمانی [۴].
- ۲- ترس از بروز تغییرات در تشکیلات سازمانی [۱۰].
- ۳- ترس از بروز تغییرات در فرآیندهای کسب و کار [۱۷].
- ۴- هزینه های بالای مالی پیاده‌سازی استاندارد [۷].
- ۵- صرف زمان زیاد جهت پیاده‌سازی استاندارد [۷].
- ۶- مقاومت و خودداری متخصصان IT (مثل CIOها، مشاوران IT و ...) در مراحل مختلف پیاده‌سازی استاندارد [۷].
- ۷- برون‌سپاری خدمات IT [۷].
- ۸- عدم درک صحیح شروط و مفاد مربوط به استاندارد [۱۰].
- ۹- عدم وجود سازگاری (تطابق) با رویه های سازمانی موجود [۱۰].
- ۱۰- عدم وجود دانش کافی در رابطه با تهدیدات امنیت اطلاعات [۵] و [۹].
- ۱۱- عدم وجود حمایت مستمر مدیریت ارشد [۳] و [۱۱].
- ۱۲- عدم ارتقاء دانش و آگاهی کافی در رابطه با استاندارد [۳] و [۱۵].
- ۱۳- عدم به روزرسانی مستمر مستندات استاندارد [۳].
- ۱۴- عدم تخصیص صحیح مسئولیتهای کاربران در حوزه امنیت اطلاعات [۴].
- ۱۵- عدم وجود تکنولوژی اطلاعاتی مناسب در سازمان [۴].
- ۱۶- عدم تشخیص صحیح فرآیندهای سازمانی [۳].
- ۱۷- فقدان منبع قدرتمندی به منظور نظارت صحیح بر مراحل پیاده‌سازی استاندارد [۱۱].
- ۱۸- تجزیه و تحلیل نادرست ریسکهای مرتبط با امنیت اطلاعات [۱۱].
- ۱۹- عدم اجرای رویه های کنترلی مناسب در دسترسی شبکه [۱۱].
- ۲۰- وظایف به ظاهر کلان [۱۴].
- ۲۱- عدم وجود نظارت کافی بر رفتار کارکنان در رابطه با امنیت اطلاعات [۴].
- ۲۲- وجود پراکندگی جغرافیایی سازمان (که اعمال کنترل های استاندارد را دشوار می سازد [۴].
- ۲۳- عدم وجود سیاست های امنیتی که به طور کامل همراستا با فلسفه سازمانی باشد [۴].

با توجه به هدف پژوهش، جامعه آماری شامل خبرگان و متخصصین در زمینه امنیت اطلاعات و سیستم مدیریت امنیت اطلاعات بود. در این پژوهش جهت انتخاب افراد از نمونه‌گیری قضاوتی و گلوله برفی استفاده گردید.

روش قضاوتی بر این فرض استوار است که دانش پژوهشگر درباره جامعه برای دستچین کردن اعضای پانل قابل استفاده است و روش گلوله برفی در صورتی استفاده می شود که پژوهشگر، خود تمام افراد مناسب را برای عضویت در پانل شناسد. در این روش، پژوهشگر کار تعیین اعضا را با شناسایی فرد یا گروهی از افراد آگاه، آغاز می‌نماید. سپس از این طریق به دیگر افراد مناسب برای کار دست می‌یابد.

در پژوهش حاضر، اعضای پانل دلفی دارای یک یا هر دو ویژگی زیر بودند:

الف - عضو هیات علمی دانشگاه در زمینه امنیت اطلاعات

ب - محقق و مجری در زمینه سیستم مدیریت امنیت اطلاعات

لازم به توضیح است که تعداد اعضا ۱۹ نفر بوده و طی ۴ راند دلفی نتیجه حاصل گشت.

۲-۱-۲- آنالیز نتایج در دلفی

در دلفی، اطلاعات کیفی و کمی جمع آوری شده ولی متاسفانه روش مورد نظر برای آنالیز و چگونگی مدیریت اطلاعات تولید شده تعریف نگردیده است. روش‌های آنالیز بر اساس هدف دلفی، ساختار راندها، نوع سوالات و تعداد شرکت‌کنندگان

تعیین می‌شود. آمارهای اصلی استفاده شده در مطالعات دلفی اندازه‌های مرکزی (میانگین، میانه و نما) و شاخص پراکندگی (انحراف معیار و محدوده میان چارکی) است [۱۲].

در هیچ یک از کتب و مقالات ارائه شده پیرامون دلفی، روش مشخص و ثابتی برای آنالیز نتایج ارائه نشده است. از این رو محققین از توصیه اساتید و متخصصان این حوزه استفاده کرده و شاخص میانگین را جهت محاسبات انتخاب نموده است. همچنین با بالا رفتن درصد اجماع، نتایج به دست آمده از اعتبار بالاتری برخوردار است. به این دلیل و با توجه به پیشنهاد خبرگان، در این پژوهش میزان اجماع نظر بر اساس چارک سوم ۷۵٪ در نظر گرفته شد.

۳-۱-۲- مراحل اجرایی دلفی

۱-۳-۱-۲- مرحله اول دلفی

در این مرحله با تمام اعضای گروه خبرگان بصورت حضوری تماس گرفته شد. آنها از اهداف، طبیعت کار و مدت زمان احتمالی برای ادامه فرآیند مطلع شدند و برای هرکدام تعریفی از اهداف پژوهش ارائه شد. همچنین به سوالات آنها پاسخ داده شد. در انتها پرسشنامه دور اول به آنها ارائه شد و از آنان خواسته شد تا پاسخ‌های خود را ارائه نمایند.

۲-۳-۱-۲- مرحله دوم دلفی

با جمع‌آوری پرسشنامه‌ها، دور اول فرآیند دلفی به پایان رسید. روش محاسبه بر این مبنا بود که عواملی که حداقل ۷۵٪ افراد به آنها رتبه ۴ و یا ۵ داده بودند به عنوان موانع پیاده‌سازی ISMS پذیرفته شدند. همچنین مقرر شد آنهایی که حداقل ۷۵٪ افراد به آنها رتبه ۱، ۲ و یا ۳ داده بودند حذف گردند. از آنجایی که در این مرحله هیچ یک از عوامل به اتفاق نظر ۷۵٪ نرسیدند، عامل حذف‌شده‌ای وجود نداشت.

عوامل پیشنهادی توسط خبرگان نیز سازماندهی شده، نظرات مشابه ترکیب و موضوعات تکراری حذف گردید. همچنین تلاش شد عوامل مطرح‌شده تا حد امکان به صورت جملاتی واضح و کوتاه بیان گردد. به این ترتیب پرسشنامه دور دوم تهیه شد. این پرسشنامه مجدداً بین خبرگان توزیع گردید تا خبرگان مولفه‌های نظرات دیگران را ببینند و اگر آن مولفه مورد تایید آنها بود، آن را انتخاب نمایند.

۳-۳-۱-۲- مرحله سوم دلفی

در این مرحله فرم‌های مرحله ۲ جمع‌آوری گردید. پس از تجزیه و تحلیل پاسخ‌های برگشتی، عواملی که ۷۵٪ افراد به آنها رتبه ۲، ۱ و یا ۳ داده بودند حذف گردیده و عواملی که ۷۵٪ افراد به آنها رتبه ۴ و یا ۵ داده بودند انتخاب گردیدند. همچنین مولفه‌هایی که از نظر معانی در یک گروه بودند، با هم تلفیق شدند. مجدداً پرسشنامه دور سوم که حاوی مولفه‌هایی با توافق بیشتر خبرگان بود، تهیه شده و بین خبرگان توزیع گردید تا مولفه‌ای که از نظرشان از اهمیت بالاتری برخوردار باشد، انتخاب گردد.

۴-۳-۱-۲- مرحله چهارم دلفی

پس از دریافت فرم‌های مرحله قبل، کلیه فرم‌ها مورد تجزیه و تحلیل قرار گرفت. بدین ترتیب پرسشنامه دور چهارم طراحی شده و در اختیار خبرگان قرار گرفت. پس از جمع‌آوری پرسشنامه و تجزیه و تحلیل پاسخ‌ها، از آنجایی که تمامی عوامل مورد توافق نظر خبرگان واقع گشت، فرآیند دلفی به پایان رسیده و عوامل نهایی استخراج شد.

۳- نتیجه مراحل دلفی

در ادامه نتایج هر یک از راندهای دلفی ارائه شده است:

۱-۳- نتیجه راند اول دلفی: شاخص‌های پیشنهاد شده از سوی اعضای پانل دلفی در راند اول عبارتند از:

- عدم وجود تجربه کافی در زمینه پیاده‌سازی موفق ISMS در ایران
- تمرکز بیش از اندازه بر روی مباحث فنی (که نتیجه آن نادیده گرفتن مباحث مدیریتی استاندارد است)
- داشتن انتظارات غیر واقعی (خارج از چارچوب ISMS و استاندارد) مدیران و کارشناسان فنی از پیاده‌سازی ISMS
- مقاومت در استفاده از متخصص امنیت کارآمد در سازمان جهت نگهداری و بهبود سیستم پیاده‌سازی شده
- باور نادرست در زمینه توان پیاده‌سازی ISMS با نیروهای فعلی سازمان
- تغییر ناصحیح الزمات استاندارد توسط مدیران (به اصطلاح بومی کردن آن برای سازمان)
- قوی نبودن کمیته راهبری امنیت اطلاعات در سازمان‌ها از نظر قدرت اجرایی تصمیمات
- تعیین اشتباه حوزه عملکرد و دامنه، جهت پیاده‌سازی ISMS در سازمان
- طبقه بندی نادرست دارایی‌های اطلاعاتی

- تغییرات زیاد مدیریتی در سازمانهای ایرانی
- عدم استقرار سیاستها و روشهای اجرایی امنیتی در پایان فاز طراحی ISMS
- عدم توجه به بعد سیستمی ISMS
- کم‌رنگ و ضعیف بودن موسسات و مشاوران پیاده‌سازی ISMS در ایران
- عدم آگاهی و شناخت کافی مدیران ایرانی از ISMS
- عدم اختصاص بودجه و هزینه مناسب به انجام اینکار

۲-۳- نتیجه راند دوم دلفی

کلیه نتایج راند اول دلفی به راند دوم منتقل گردید. در راند دوم پس از بررسی نظرات خبرگان و با استفاده از منطق چارک سوم، شاخص‌های زیر به اجماع نظر ۷۵٪ مبنی بر توافق نظر خبرگان به عنوان موانع پیاده‌سازی ISMS رسیدند. سایر عوامل که به اجماع نظر ۷۵٪ نرسیده بودند، به پرسشنامه راند سوم منتقل شده تا مجدداً مورد ارزیابی خبرگان قرار گیرند:

- ترس از بروز تغییرات در تشکیلات سازمانی
- هزینه‌های بالای مالی پیاده‌سازی استاندارد
- عدم درک صحیح شروط و مفاد مربوط به استاندارد توسط مجریان پیاده‌سازی ISMS
- عدم وجود دانش کافی در رابطه با تهدیدات امنیت اطلاعات
- عدم وجود حمایت مستمر مدیریت ارشد
- عدم ارتقاء دانش و آگاهی کافی سازمانی در رابطه با استاندارد
- عدم تشخیص صحیح فرآیندهای سازمانی
- فقدان منبع قدرتمندی به منظور نظارت صحیح بر مراحل پیاده‌سازی استاندارد
- قوی نبودن کمیته راهبری امنیت اطلاعات در سازمان‌ها از نظر قدرت اجرایی تصمیمات
- تغییرات زیاد مدیریتی در سازمانهای ایرانی
- عدم آگاهی و شناخت کافی مدیران ایرانی از ISMS

۳-۳- نتیجه راند سوم دلفی

در راند سوم نیز پس از بررسی نظرات اعضاء پانل دلفی، شاخص‌های زیر به اجماع نظر ۷۵٪ مبنی بر توافق نظر خبرگان به عنوان موانع پیاده‌سازی ISMS رسیدند. سایر عوامل که به اجماع نظر ۷۵٪ نرسیده بودند، به پرسشنامه راند چهارم منتقل شده تا مجدداً مورد ارزیابی خبرگان قرار گیرند:

- عدم تبادل نظر مدیران سازمان به هنگام اخذ تصمیمات مرتبط با امنیت اطلاعات با سایر پرسنل سازمانی
- عدم وجود سازگاری (تطابق) با رویه‌های سازمانی موجود
- عدم تخصیص صحیح مسئولیت‌های کاربران در حوزه امنیت اطلاعات
- عدم وجود سیاست‌های امنیتی که به طور کامل همراستا با فلسفه سازمانی باشد
- عدم وجود تجربه کافی در زمینه پیاده‌سازی موفق ISMS در ایران
- تمرکز بیش از اندازه بر روی مباحث فنی (که نتیجه آن نادیده گرفتن مباحث مدیریتی استاندارد است)
- تغییر ناصحیح الزامات استاندارد توسط مدیران (به اصطلاح بومی کردن آن برای سازمان)

۴-۳- نتیجه راند چهارم دلفی

در این راند، سایر مولفه‌هایی که به اجماع نظر ۷۵٪ در رابطه با عدم پذیرش مولفه‌های مذکور به عنوان موانع پیاده‌سازی ISMS رسیده بودند، مجدداً مورد ارزیابی قرار گرفتند. سپس نتیجه راند سوم تکرار شده و هیچ یک از مولفه‌ها به عنوان موانع پیاده‌سازی ISMS مورد قبول خبرگان واقع نشدند. لذا فرآیند دلفی در این مرحله به پایان رسید.

۴- یافته‌های پژوهش

با توجه به هدف پژوهش که استخراج عوامل شکست پیاده‌سازی ISMS در کشورهای در حال توسعه، با بهره‌گیری از اطلاعات سازمان‌های ایرانی و با استفاده از تکنیک دلفی است، پس از اجرای ۴ راند دلفی، این عوامل شکست به شرح زیر شناسایی شدند:

- ۱- عدم تبادل نظر مدیران سازمان به هنگام اخذ تصمیمات مرتبط با امنیت اطلاعات با سایر پرسنل سازمانی
- ۲- عدم آگاهی و شناخت کافی مدیران از ISMS
- ۳- تغییرات زیاد مدیریتی

- ۴- عدم وجود حمایت مستمر مدیریت ارشد
- ۵- تغییر ناصحیح الزامات استاندارد توسط مدیران (به اصطلاح بومی کردن آن برای سازمان)
- ۶- فقدان منبع قدرتمندی به منظور نظارت صحیح بر مراحل پیاده‌سازی استاندارد
- ۷- قوی نبودن کمیته راهبری امنیت اطلاعات در سازمان‌ها از نظر قدرت اجرایی تصمیمات
- ۸- ترس از بروز تغییرات در تشکیلات سازمانی
- ۹- هزینه‌های بالای مالی پیاده‌سازی استاندارد
- ۱۰- عدم درک صحیح شروط و مفاد مربوط به استاندارد توسط مجریان پیاده‌سازی ISMS
- ۱۱- عدم وجود سازگاری (تطابق) بخش‌های مختلف استاندارد با رویه‌های سازمانی موجود
- ۱۲- عدم وجود دانش کافی در رابطه با تهدیدات امنیت اطلاعات
- ۱۳- عدم ارتقاء دانش و آگاهی کافی سازمانی در رابطه با استاندارد
- ۱۴- عدم تخصیص صحیح مسئولیت‌های کاربران در حوزه امنیت اطلاعات
- ۱۵- عدم تشخیص صحیح فرآیندهای سازمانی
- ۱۶- عدم وجود سیاست‌های امنیتی که به طور کامل همراستا با فلسفه سازمانی باشد
- ۱۷- عدم وجود تجربه کافی در زمینه پیاده‌سازی موفق ISMS
- ۱۸- تمرکز بیش از اندازه بر روی مباحث فنی (که نتیجه آن نادیده گرفتن مباحث مدیریتی استاندارد است)

با توجه به نتایج حاصل از پژوهش، لازم است موارد زیر در پیاده‌سازی سیستم مدیریت امنیت اطلاعات مدنظر قرار گیرد:

- ۱- لازم است مدیران ارشد در کشورهای در حال توسعه در راستای شناسایی دقیق این استاندارد و اهداف آن تلاش بیشتری نمایند. همچنین از طریق حمایت گسترده تر و درگیر شدن بیشتر با مباحث استاندارد، سعی نمایند تا با دانش بیشتر در پیاده‌سازی موفق این استاندارد امنیتی موثر باشند.
 - ۲- به منظور عملیاتی سازی ISMS در سازمان، لازم است شناخت دقیق و کاملی از پروسه‌ها و فرآیندهای سازمانی صورت پذیرد. سپس کلیه این فرآیندها مستند شده و مورد تجزیه و تحلیل قرار گیرند. همچنین با بررسی بندهای مختلف استاندارد، سازگاری منطقی میان بخش‌های استاندارد و رویه‌های سازمانی، برقرار گردد.
 - ۳- برای تدوین برنامه‌های عملیاتی لازم است کمیته‌ای که مسئولیت راهبری امنیت اطلاعات را عهده دار است، با تخصیص مسئولیت‌ها و اختیارات بیشتری در اجرایی نمودن برنامه‌های عملیاتی کوشا باشد.
 - ۴- شناسایی ریسک‌های امنیت اطلاعات و به روز نمودن اطلاعات در این رابطه به منظور شناسایی تهدیدات جدید امنیتی، می‌تواند در پیاده‌سازی موفق تر ISMS تاثیرگذار باشد.
 - ۵- یکی از وجوه مهم سیستم مدیریت امنیت اطلاعات، تدوین استراتژی و سیاست امنیتی است که همراستا با فلسفه سازمانی موجود باشد. این استراتژی می‌بایست در بلندمدت با اهداف و چشم انداز سازمانی تطابق داشته باشد. از این رو دقت در تدوین استراتژی امنیتی از جمله موارد بسیار مهمی است که توجه به آن ضروری به نظر می‌رسد.
 - ۶- این مسئله که سیستم مدیریت امنیت اطلاعات، استاندارد است که هر دو جنبه فنی و مدیریتی را دار بوده و توجه به هر دو جنبه آن به یک اندازه ضروری است، از جمله مسائل بسیار مهمی است که می‌بایست مورد توجه قرار گیرد. زیرا در شرایط کنونی، بیشتر نگاه‌ها به ISMS به عنوان یک استاندارد فنی معطوف است. لذا جنبه مدیریتی آن نادیده انگاشته می‌شود که این امر خود به ایجاد مشکلات بیشتر می‌انجامد.
 - ۷- موفقیت و اثربخشی در طرح‌های امنیت اطلاعات، متکی بر پشتیبانی مدیریتی ارشد و همچنین دخیل نمودن پرسنل سازمانی در تصمیمات مرتبط با امنیت است. از آنجایی که کارکنان در هر سازمان، از نزدیک با موارد اجرایی روبه رو می‌باشند، می‌توانند با ارائه پیشنهادات عملیاتی تر، در پیش بردن هرچه بیشتر فرآیند پیاده‌سازی ISMS موثر باشند.
- از آنجایی که کارکنان یک سازمان در سیستم مدیریت امنیت اطلاعات دارای نقش کلیدی هستند، لازم است نسبت به نقش خویش در این سیستم آگاهی کافی داشته باشند. این مهم تنها از طریق برنامه‌های آموزشی، اطلاع رسانی و ابلاغیه‌هایی از سوی مدیریت امنیت اطلاعات تحقق می‌پذیرد. هرچند نوع این آموزش‌ها برای افراد مختلف متفاوت است، ولی هدف از تمام این آموزش‌ها، انتقال درک و بینشی واحد برای امنیت و مسائل مربوط به آن، به تمام نیروهای انسانی یک سازمان است.

در این بخش به منظور توسعه تحقیقات آینده، چندین پیشنهاد به محققین و کسانی که علاقه مند به انجام پژوهش در زمینه سیستم مدیریت امنیت اطلاعات می‌باشند، ارائه می‌شود:

- استفاده از روش مطالعه صنعت به منظور استخراج موانع پیاده‌سازی ISMS.
- بررسی این که هر یک از موانع ISMS در کدام یک از مراحل چرخه PDCA قرار دارند.
- طراحی مدل موانع پیش روی پیاده‌سازی ISMS در کشورهای در حال توسعه.
- مقایسه موانع موجود در پیاده‌سازی ISMS میان سازمان‌های دولتی و خصوصی.
- مقایسه موانع موجود در پیاده‌سازی ISMS میان سازمان‌های تولیدی و خدماتی.

۵- محدودیت‌های پژوهش

تعداد متخصصان در حوزه سیستم مدیریت امنیت اطلاعات در کشورهای در حال توسعه محدود بوده و دسترسی به این افراد

نیز به سختی امکان پذیر است. همچنین اطلاعات، مدارک، مراجع و منابع مورد نیاز و همچنین case های عملی انجام شده در رابطه با موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات در کشورهای درحال توسعه محدود است. علاوه بر این دسترسی به موارد عملی انجام شده در کشورهای توسعه یافته به لحاظ نو و جدید بودن موضوع تحقیق، تا حدی دشوار است. با توجه به محدودیت‌های ذکر شده می‌توان گفت که نتایج حاصل از پژوهش حاضر، قابل تعمیم برای کلیه سازمان‌هایی است که به پیاده‌سازی ISMS در کشورهای درحال توسعه پرداخته‌اند.

۶- نتیجه‌گیری

با توجه به نتایج حاصل از پژوهش دیده می‌شود که در کشورهای در حال توسعه به دلیل مشکلات اقتصادی، اجتماعی و... فراوان مشکلات بسیار دست به گریبان توسعه و همگانی شدن شبکه ارتباطی و تکنولوژی آن است. پیاده‌سازی سیستم‌های امنیت اطلاعات در کشورهای مختلف می‌تواند تفاوت‌هایی را در برداشته باشد. همانطور که پیش از این اشاره شد، بحث‌های مرتبط با امنیت اطلاعات و حریم خصوصی در کشورهای در حال توسعه مانند ایران از اهمیت پایینی برخوردار است. حال آنکه در کشورهای توسعه یافته به مسایل پیرامون امنیت اطلاعات و سیستم‌های اطلاعاتی بسیار پرداخته شده و برنامه‌ریزی‌های بسیار برای این مقوله در نظر گرفته می‌شود. نتایج مستخرج از مشاهدات، مطالعات اسناد و سپس روش دلفی گواه آن است که این امر می‌تواند ناشی از وجود مواردی نظیر عدم مدیریت صحیح، نبود شناخت دقیق فرآیندهای سازمانی، عدم اطلاع از ریسک‌های امنیت اطلاعات، نبود استراتژی امنیتی همراستا با فلسفه سازمانی، عدم پشتیبانی مدیریت ارشد، اختصاص بودجه مناسب، عدم درک صحیح فرآیندهای سازمانی، تخصیص نا به جای مسئولیتها بین کاربران شبکه، فقدان دانش و تجربه در حوزه امنیت اطلاعات و تمرکز بیش از حد بر روی مسائل فنی و غفلت از مسائل مدیریتی باشد. لازم به ذکر است که شناسایی موانع مربوطه در پژوهش حاضر، می‌تواند به درک صحیحی از سیستم مدیریت امنیت اطلاعات در کشورهای در حال توسعه کمک کرده و به بهبود فرآیندهای موجود در هنگام پیاده‌سازی بینجامد.

۷- پیشنهادات

از آنجا که یافته‌های پژوهش از سازمانهای ایرانی استخراج گردیده، توصیه می‌شود به منظور جامعیت بخشیدن به شناسایی عوامل در کشورهای در حال توسعه، از مطالعات کتابخانه‌یی گسترده‌تر و مشاهدات و بررسی اسناد در سایر کشورهای در حال توسعه به منظور شناسایی عوامل بیشتری استفاده شود. در این پژوهش امکان مصاحبه با متخصصین بیشتر در روش دلفی وجود نداشت چرا که هماهنگی با خبرگان برای مصاحبه و گفتگو امری بسیار پیچیده بود. لذا به پژوهشگران بعدی توصیه می‌شود از نظرات متخصصین بیشتری بهره‌مند شوند تا جامعیت نتایج مصاحبه‌ها افزایش یابد.

منابع

- آذر، عادل و مومنی، منصور (۱۳۸۷)، آمار و کاربرد آن در مدیریت (تحلیل آماری)، جلد دوم، چاپ یازدهم، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- رحیمی سجاسی، مریم (۱۳۸۵)، «بررسی عوامل هنجاری و سازمانی مؤثر بر میزان تولید علمی اعضای هیأت علمی جامعه‌ی دانشگاهی و پژوهشی»، از: <http://www.zmatris.blogspot.com>
- Bellone, J., (۲۰۰۸), "A practiced approach to information security management system implementation", Information Management & Computer Security, Vol. ۱۶, No. ۱, pp. ۵۷-۴۹.
- Dhillon, G. (۲۰۰۱), Information security management: global challenges in the new millennium, IGI Global, ۱۹۲pp.
- Elaine, H., (۲۰۰۹), Information processing system to security standard compliance measurement: A quantitative approach using pathfinder networks (pfnets), Candidate for Degree of Doctor of Philosophy, Mississippi State University.
- Eves, Beth K., (۱۹۸۱), 'Transfer of information technology to less developed countries: a system approach' Journal of the American Society for Information Science, p. ۸۷.
- Fomin, et al. (۲۰۰۸), "ISO/IEC ۲۷۰۰۱ Information systems security management standards: Exploring the reasons for low adoption", RSM Erasmus University, ۱۳pp.
- Fung, A., Farn, K., Lin, A., (۲۰۰۳), "Paper: a study on the certification of the information security management systems", Computer Standards & Interfaces, Vol. ۲۵, pp. ۴۶۱-۴۴۷.
- Kritzinger, E., Smith, E., (۲۰۰۸), "Information security management: An information security retrieval and awareness model for industry", Computers & Security, Vol. ۲۷, pp. ۲۳۱-۲۲۴.
- Ku, et al., (۲۰۰۹), "National information security policy and its implementation: A case study in Taiwan", Telecommunications Policy, Vol. ۳۲, pp. ۲۸۴-۲۷۱.
- Kwok, L., Longley, D., (۱۹۹۹), "Information security management and modelling", Information Management & Computer Security, Vol. ۷, No. ۱, pp. ۳۹-۳۰.
- McKenna H, Hasson F, Smith M., (۲۰۰۲), "A Delphi survey of midwives and midwifery students to identify non-midwifery duties, Midwifery" Dec; (۴): ۱۸ ۲۲-۳۱۴.
- Munn, Robert F., (۱۹۷۸), 'Appropriate technology and information services in developing countries', International Library Review. ۱۰, pp. ۲۷-۲۳.
- Posthumus, S., Von Solms, R., (۲۰۰۴), A framework for the governance of information security, Computers & Security, ۲۳, ۱۴۶-۱۳۸.
- Siponen, M., Willison, R., (۲۰۰۹), "Information security management standards: Problems and solutions", Information & Management, Vol. ۴۶, pp. ۲۷۰-۲۶۷.
- Von Solms, R., (۱۹۹۹), Information security management: why standards are important, Information Management & Computer Security, ۵۷±۵۰, ۱/۷.
- Williams, P., (۲۰۰۸), "In a 'trusting' environment, everyone is responsible for information security", Information Security Technical Report, Vol. ۱۳, pp. -۲۰۷ ۲۱۵.