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

خدیجه روزبهانی
دانشکده مدیریت دانشگاه تهران
rrouzbehani@ut.ac.ir

مصطفی زمانیان
دانشکده مدیریت دانشگاه تهران
zamanyan@ut.ac.ir

مقدمه

ظهـور فنـاوری ارتباطـات و اینترنـت امـکان «اشـتراک اطلاعـات» و «تبـادل آسـان اطلاعـات» بیـن سیسـتم‌های رایانـه‌ای را بـه وجـود آورده اسـت. ایـن فناوری‌هـای نویـن بـا غلبـه بـر فاصله‌هـا و محدودیت‌هـای فیزیکـی و کاهـش محسـوس زمـان، معـماری و سـاختار ارائـه خدمـات در سیسـتم‌ها را بـه شـدت تحـت تاثیـر قـرار داده‌انـد. بدیهـی اسـت کـه در ایـن شرایـط روش‌هـای حفاظـت فیزیکـی بـه تنهایـی قـادر بـه تامیـن امنیـت نخواهنـد بـود. بنابرایـن سـازمان‌ها مجبـور بـه اسـتفاده از روش‌هـای جدیـد حفاظـت اطلاعـات و کنـترل دسترسـی‌ها بـه منابـع سـازمان شـوند.

در چنیـن شرایطـی بسـیاری از سـازمان‌ها بـه پذیـرش اسـتانداردهای مدیریـت امنیتـی منتشرشـده اقـدام نمـوده‌انـد. Farn ، Fung و Lin در سـال ۲۰۰۳ در رابطـه بـا اسـتفاده از اسـتانداردها بیـان کرده‌انـد کـه بـا کمـک اسـتانداردها، می‌تـوان مشـکلات ناشـی از اطلاعـات ناقـص را کاهـش داد. همچنیـن می‌تـوان فرآیندهـای تصمیم‌گیـری مرتبـط بـا عرضـه و تقاضـای قابـل اطمینـان را سـاده نمـود [۸].

همچنیـن اسـتانداردها، امـری مناسـب بـرای اطمینـان از رعایـت امنیـت اطلاعـات در سـازمان‌ها محسـوب می‌گردنـد و از آنجـا کـه در دنیـای امـروز و بـا توجـه بـه پدیده‌هایـی ماننـد تجـارت الکترونیـک، دیگـر امنیـت اطلاعـات مسـئله‌ای داخلـی (domestic issue) محسـوب نمی‌شـود و روی شرکای هـر سـازمان اثـر می‌گـذارد، اسـتانداردها ابـزار خوبـی بـرای اطمینـان از سـطح قابـل قبولـی از امنیـت در سـازمان‌ها هسـتند [۱۶].بدیـن ترتیـب بـه منظـور جلوگیـری از نفوذهـای ناخواسـته امنیتـی لازم اسـت کـه اسـتاندارد مدیریـت امنیـت اطلاعـات مناسـبی بـه کار گرفتـه شـود تـا بـه پیاده‌سـازی سیسـتم مدیریـت امنیـت اطلاعـات (Information Security Management System) در سـازمان کمـک نمایـد.

از سـوی دیگـر عمومـاً فـرض بـر ایـن بـوده کـه پیشرفته‌تریـن فنـاوری مـورد اسـتفاده در کشـورهای توسـعه یافتـه را مـی تـوان بـا [حداکـثر] کارایـی و سـهولت در کشـورهای در حـال توسـعه نیـز مـورد اسـتفاده قـرار داد. در اوایـل دهـه ۱۹۷۰ ضرورت انتقـال مسـتقیم و انبـوه فنـاوری پیشرفتـه بـه کشـورهای در حـال توسـعه بـه صـورت گسـترده‌ای مـورد بحـث قـرار گرفـت. از آن پـس رفته‌رفتـه مشـخص شـد کـه عرضـه عملکردهـای بسـیار پیچیـده و سرمایـه بـر، بـه جـای حـل مسـئله باعـث افزایـش مشـکلات می‌گـردد [۱۳].

«سونیلسـن» دربـاره راهـبرد انتقـال فنـاوری در کشـورهای در حـال توسـعه اظهـار مـی‌دارد: «بـرای پایه‌گـذاری فنـاوری نویـن در کشـورهای در حـال توسـعه بایـد نظام‌هـای اجتماعـی و گرایش‌هـای انسـانی، دانـش و مهارت‌هـای انسـانی و ابزارهـای فیزیکـی کـه فـن‌آوری در قالـب آن‌هـا عینیـت می‌یابـد را تغییـر دهیـم.» [۶]. بـه ایـن ترتیـب هـر کشـوری بایـد در پـی ایجـاد فرآینـد بومـی تولیـد علـم باشـد. زیـرا شـکاف عمیـق و فزاینـده بیـن اسـتانداردهای زندگـی در کشـورهای توسـعه یافتـه و در حـال توسـعه، ناشـی از فاصلـهٔ علمـی و فنـی بیـن آن‌هاسـت. در واقـع چیـزی کـه ملت‌هـای غنـی را از فقیـر متمایـز می‌کنـد، نـه تنهـا تولیـد ثروت‌هـای مـادی بلکـه میـزان تولیـد علمـی و دسـتیابی بـه دانـش بهره‌گیـری مناسـب از منابـع موجـود اسـت [۲].

بـا توجـه بـه تفاوت‌هـای فرهنگـی و درجـه احـترام و حفـظ حریـم خصوصـی افـراد در کشـورهای توسـعه‌یافته و کشـورهای درحـال توسـعه، کپی‌بـرداری در پیاده‌سـازی سیسـتم‌های مدیریـت امنیـت اطلاعـات بـه نظـر مشکل‌سـاز می‌آیـد. ذکـر برخـی از ایـن تفاوت‌هـا می‌توانـد بـه شـناخت و اهمیـت ایـن تفـاوت کمـک کنـد. در کشـورهای توسـعه‌یافته احـترام بـه حریـم خصوصـی افـراد بسـیار اهمیـت دارد. بـرای مثـال پرسـیدن اطلاعـات شـخصی افـراد از قبیـل میـزان حقـوق دریافتـی فـرد امـری ناپسـند اسـت، در صورتی‌کـه در کشـوری ماننـد ایـران سـوال در مـورد حقـوق دریافتـی فـرد حتـی در حضـور جمـع، امـری عـادی و پذیرفتـه اسـت و یـا مـی دانیـم کـه رمـز کارت‌هـای اعتبـاری در کشـورهای توسـعه یافتـه بسـیار محرمانـه تلقـی می‌شـود و حتـی هنـگام خریـد و پرداخـت بـا کارت اعتبـاری، فروشـنده در هنگامـی کـه خریـدار می‌خواهـد رمـزش را وارد دسـتگاه کنـد، رویـش را بـر می‌گردانـد تـا خریـدار مطمـئن شـود کـه رمـز او را نمی‌بینـد. ولـی در ایـران فروشـنده در حضـور دیگـران از خریـدار می‌خواهـد تـا رمـز کارتـش را بـا صـدای بلنـد بگویـد تـا فروشـنده خـودش آن را وارد دسـتگاه کنـد و ایـن امـر موضوعـی عـادی و پذیرفتـه شـده اسـت و افـراد بـه راحتـی رمـز کارت‌هـای خـود 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 سیستم های 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 سازمان های 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 اخذ 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 سیاست های امنیتی با فلسفه سازمانی وجود نداشته باشد، پیاده‌سازی ISMS با مشکل مواجه می گردد[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 مواقعی می‌تواند پیاده‌سازی سیستم مدیریت امنیت اطلاعات را دشوار نماید[۷]. Kritzinger و Smith 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 می شود [۱]. در این پژوهش نیز از آنجایی که چارچوبی از پیش تعیین‌شده 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 درسایر کشورهای درحال 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 اولِ 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 مطرح‌شده 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[٤].
۲- ترس از بروز تغییرات در تشکیلات سازمانی[۱۰].
۳- ترس از بروز تغییرات در فرآیندهای کسب و کار [۱۷].
٤- هزینه های بالای مالی پیاده‌سازی استاندارد [۷].
۵- صرف زمان زیاد جهت پیاده‌سازی استاندارد [۷].
٦- 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].
۱٤- عدم تخصیص صحیح مسئولیتهای کاربران در حوزه امنیت اطلاعات [٤]
۱۵- عدم وجود تکنولوژی اطلاعاتی مناسب در سازمان [٤].
۱٦- 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 [۱٤].
۲۱- عدم وجود نظارت کافی بر رفتار کارکنان در رابطه با امنیت اطلاعات [٤].
۲۲- وجود پراکندگی جغرافیایی سازمان (که اعمال کنترل های استاندارد را دشوار می سازد [٤].
۲۳- عدم وجود سیاست های امنیتی که به طور کامل همراستا با فلسفه سازمانی باشد [٤].

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 استواراست 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 نشناسد. 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 ٤ 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.

۲-۱-۳- مراحل اجرایی دلفی

۲-۱-۳-۱- 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.

۲-۱-۳-۲- مرحله دوم دلفی

با جمع‌آوری پرسشنامه‌ها، دور اول فرایند 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.

۲-۱-۳-۳- مرحله سوم دلفی

در این مرحله فرم‌های مرحله ۲ جمع‌آوری گردید. پس از تجزیه و تحلیل پاسخ های 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 مولفه هایی 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.

۲-۱-۳-٤- 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 جمع آوری 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 هریک از راندهای دلفی ارائه شده است:

۳-۱- 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 درایران
- 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 واستاندارد) 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 الزامات استاندارد توسط مدیران (به اصطلاح بومی کردن آن برای سازمان)
- قوی نبودن کمیته راهبری امنیت اطلاعات در سازمان ها از نظر قدرت اجرایی تصمیمات
- تعیین اشتباه حوزه عملکرد و دامنه، جهت پیاده‌سازی ISMS در سازمان
- طبقه بندی نادرست دارایی های 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

۳-۲- 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، شاخص های 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
- هزینه های 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 سازمان ها 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 رویه های سازمانی موجود
- عدم تخصیص صحیح مسئولیت‌های کاربران در حوزه امنیت اطلاعات
- عدم وجود سیاست های امنیتی که به طور کامل همراستا با فلسفه سازمانی باشد
- عدم وجود تجربه کافی در زمینه پیاده‌سازی موفق ISMS درایران
- 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)

۳-٤- نتیجه راند چهارم دلفی

در این راند، سایر مولفه‌هایی که به اجماع نظر ۷۵٪ در رابطه با عدم پذیرش مولفه های 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.

٤- یافته های 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

٤- عدم وجود حمایت مستمر مدیریت ارشد
٥- تغییر ناصحیح الزامات استاندارد توسط مدیران (به اصطلاح بومی کردن آن برای سازمان)
٦- فقدان منبع قدرتمندی به منظور نظارت صحیح بر مراحل پیاده‌سازی استاندارد
٧- قوی نبودن کمیته راهبری امنیت اطلاعات در سازمان‌ها از نظر قدرت اجرایی تصمیمات
٨- ترس از بروز تغییرات در تشکیلات سازمانی
٩- هزینه‌های بالای مالی پیاده‌سازی استاندارد
١٠- عدم درک صحیح شروط و مفاد مربوط به استاندارد توسط مجریان پیاده‌سازی ISMS
١١- عدم وجود سازگاری (تطابق) بخش‌های مختلف استاندارد با رویه‌های سازمانی موجود
١٢- عدم وجود دانش کافی در رابطه با تهدیدات امنیت اطلاعات
١٣- عدم ارتقاء دانش و آگاهی کافی سازمانی در رابطه با استاندارد
١٤- عدم تخصیص صحیح مسئولیت های کاربران در حوزه امنیت اطلاعات
١٥- عدم تشخیص صحیح فرآیندهای سازمانی
١٦- عدم وجود سیاست های امنیتی که به طور کامل همراستا با فلسفه سازمانی باشد
١٧- عدم وجود تجربه کافی در زمینه پیاده‌سازی موفق ISMS
١٨- 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:

١- 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.
٢- به منظور عملیاتی سازی ISMS در سازمان، لازم است شناخت دقیق و کاملی از پروسه ها 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 بخش های استاندارد و رویه های سازمانی، برقرار گردد.
٣- برای تدوین برنامه‌های عملیاتی لازم است کمیته ای که مسئولیت راهبری امنیت اطلاعات را عهده دار است، با تخصیص مسئولیت ها و اختیارات بیشتری در اجرایی نمودن برنامه های عملیاتی کوشا باشد.
٤- شناسایی ریسک های امنیت اطلاعات و به روز نمودن اطلاعات در این رابطه به منظور شناسایی تهدیدات جدید امنیتی، می تواند در پیاده‌سازی موفق تر ISMS تاثیرگذار باشد.
٥- یکی از وجوه مهم سیستم مدیریت امنیت اطلاعات، تدوین استراتژی و سیاست امنیتی است که همراستا با فلسفه سازمانی موجود باشد. این استراتژی می بایست 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 می رسد.
٦- این مسئله که سیستم مدیریت امنیت اطلاعات، استانداردی است که هر دو جنبه فنی و مدیریتی را دار بوده و توجه به هر دوجنبه آن به یک اندازه ضروری است، از جمله مسائل بسیار مهمی است که می بایست مورد توجه قرار گیرد. زیرا در شرایط کنونی، بیشتر نگاه ها به ISMS به عنوان یک استاندارد فنی معطوف است. لذا جنبه مدیریتی آن نادیده انگاشته می شود که این امر خود به ایجاد مشکلات بیشتر می انجامد.
٧- موفقیت و اثربخشی در طرح های امنیت اطلاعات، متکی بر پشتیبانی مدیریت 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 می باشند، می توانند 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 برنامه های آموزشی، اطلاع رسانی و ابلاغیه هایی از سوی مدیریت امنیت اطلاعات تحقق می پذیرد. هرچند نوع این آموزش ها برای افراد مختلف متفاوت است، ولی هدف از تمام این آموزش ها، 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 محققیق و کسانی که علاقه مند به انجام پژوهش در زمینه سیستم مدیریت امنیت اطلاعات می باشند، ارایه می شود:

- استفاده از روش مطالعه صنعت به منظور استخراج موانع پیاده‌سازی ISMS.
- بررسی این که هریک 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 سازمان های دولتی و خصوصی.
- مقایسه موانع موجود در پیاده‌سازی ISMS میان سازمان های تولیدی و خدماتی.

٥- محدودیت‌های پژوهش

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

نیز به سختی امکان پذیر است. همپنین 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 می توان گفت که نتایج حاصل از پژوهش حاضر، قابل تعمیم برای کلیه سازمان هایی است که به پیاده‌سازی ISMS در کشورهای درحال توسعه پرداخته اند.

٦- نتیجه گیری

با توجه به نتایج حاصل از پژوهش دیده می شود 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 سیستم های امنیت اطلاعات در کشورهای مختلف می تواند تفاوت هایی را در برداشته باشد. همانطور که پیش از این اشاره شد، بحث های 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 سیستم های اطلاعاتی بسیار پرداخته شده و برنامه ریزی های بسیار برای این مقوله در نظر گرفته می شود. نتایج مستخرج از مشاهدات ،مطالعات اسناد و سپس روش دلفی گواه آن است که این امر می تواند ناشی از وجود مواردی نظیر عدم مدیریت صحیح، نبود شناخت دقیق فرآیندهای سازمانی، عدم اطلاع از ریسک های امنیت اطلاعات، نبود استراتژی امنیتی همراستا با فلسفه سازمانی، عدم پشتیبانی مدیریت ارشد، عدم 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، می تواند به درک صحیحی از سیستم مدیریت امنیت اطلاعات درکشورهای در حال توسعه کمک کرده و به بهبود فرآیندهای موجود در هنگام پیاده‌سازی بینجامد.

٧- پیشنهادات

از آنجا که یافته های پژوهش از سازمانهای ایرانی استخراج گردیده ، توصیه میشود به منظور جامعیت بخشیدن به شناسایی عوامل در کشورهای در حال توسعه ،از مطالعات کتابخانه یی گسترده تر و مشاهدات و بررسی اسناد در سایر کشورهای در حال توسعه به منظورشناسایی 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 بهره مند شوند تا جامعیت نتایج مصاحبه ها افزایش یابد.

منابع

١. آذر، عادل و مومنی، منصور (١٣٨٧)، آمار و کاربرد آن در مدیریت (تحلیل آماری)، جلد دوم، چاپ یازدهم، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه ها (سمت).

٢. رحیمی سجاسی، مریم (١٣٨٥)، «بررسی عوامل هنجاری و سازمانی مؤثر بر میزان تولید علمی اعضای هیأت علمی جامعه¬ی دانشگاهی و پژوهشی»، از: http://www.matris.blogsky.com/٢٠٠٧/٠١/٢٠((

٣. Bellone, J., (٢٠٠٨), "A practiced approach to information security management system implementation", Information Management & Computer Security, Vol. ١٦, No. ١, pp. ٥٧-٤٩.

٤. Dhillon, G. (٢٠٠١), Information security management: global challenges in the new millennium, IGI Global, ١٩٢pp.

٥. Elaine, H., (٢٠٠٩), 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.

٦. Eves، Beth K., (١٩٨١), 'Transfer of information technology to less developed countries: a system approach' Journal of the American Society for Inforamtion Science, p .٩٧.

٧. Fomin, et al. (٢٠٠٨), "ISO/IEC ٢٧٠٠١ Information systems security management standards: Exploring the reasons for low adoption", RSM Erasmus University, ١٣pp.

٨. Fung, A., Farn, K., Lin, A., (٢٠٠٣), "Paper: a study on the certification of the information security management systems", Computer Standards & Interfaces, Vol. ٢٥, pp. ٤٦١-٤٤٧.

٩. Kritzinger, E., Smith, E., (٢٠٠٨), "Information security management: An information security retrieval and awareness model for industry", Computers & Security, Vol. ٢٧, pp. ٢٣١-٢٢٤.

١٠. Ku, et al., (٢٠٠٩), "National information security policy and its implementation: A case study in Taiwan", Telecommunications Policy, Vol. ٣٣, pp. ٣٨٤-٣٧١.

١١. Kwok, L., Longley, D., (١٩٩٩), "Information security management and modelling", Information Management & Computer Security, Vol. ٧, No. ١, pp. ٣٩-٣٠.

١٢. McKenna H, Hasson F, Smith M., (٢٠٠٢), "A Delphi survey of midwives and midwifery students to identify non-midwifery duties, Midwifery" Dec; :(٤) ١٨ ٢٢-٣١٤.

١٣. Munn، Robert F., (١٩٧٨), 'Appropriate technology and information services in developing countries', International Library Review. ١٠,pp.٢٧-٣٣.

١٤. Posthumus, S., Von Solms, R., (٢٠٠٤), A framework for the governance of information security, Computers & Security, ٦٤٦-٦٣٨ ,٢٣.

١٥. Siponen, M., Willison, R., (٢٠٠٩), "Information security management standards: Problems and solutions", Information & Management, Vol. ٤٦, pp. ٢٧٠-٢٦٧.

١٦. Von Solms, R, (١٩٩٩), Information security management: why standards are Important, Information Management & Computer Security, ٥٧±٥٠ ,١/٧.

١٧. Williams, P., (٢٠٠٨), "In a 'trusting' environment, everyone is responsible for information security", Information Security Technical Report, Vol. ١٣, pp. -٢٠٧ ٢١٥.