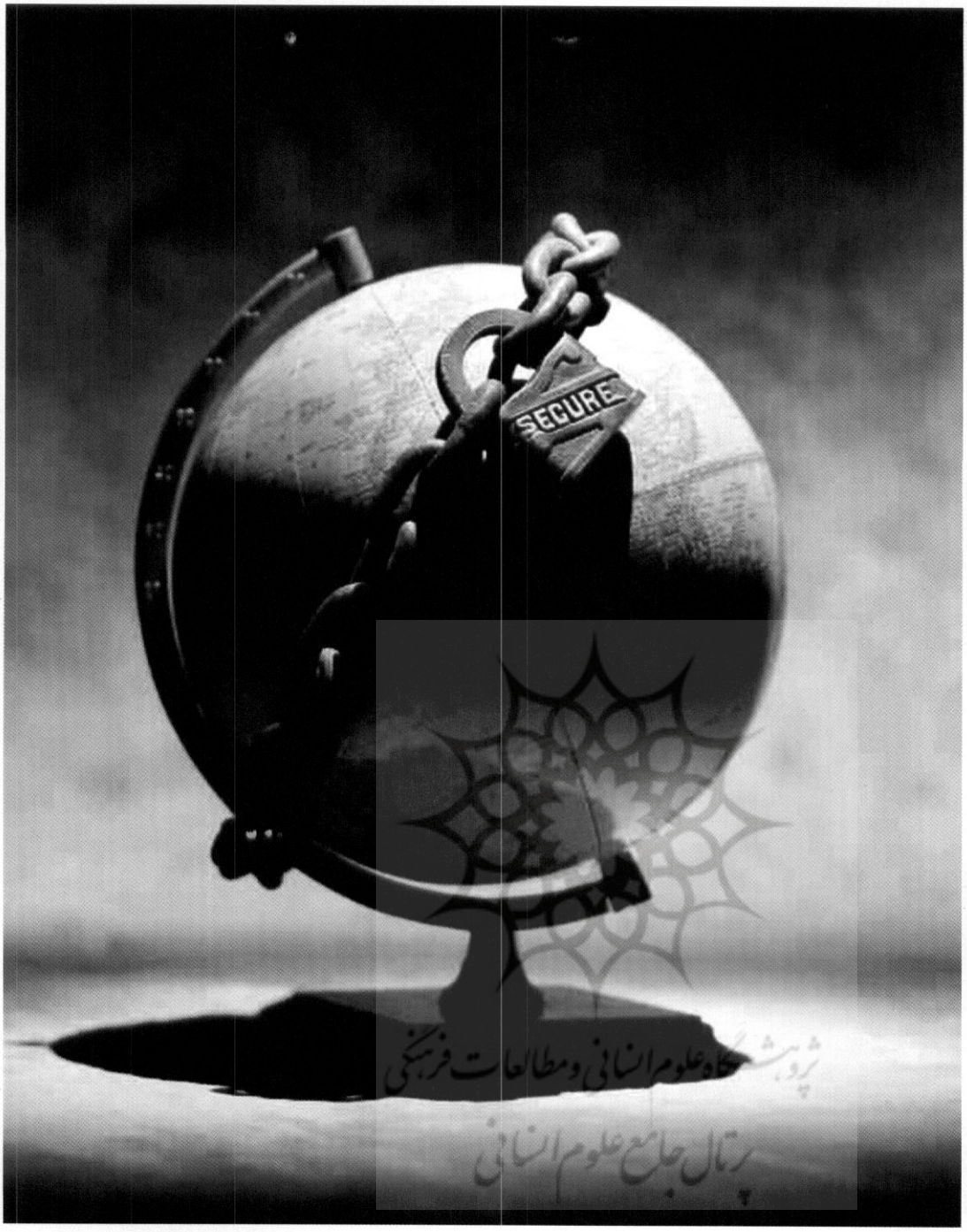
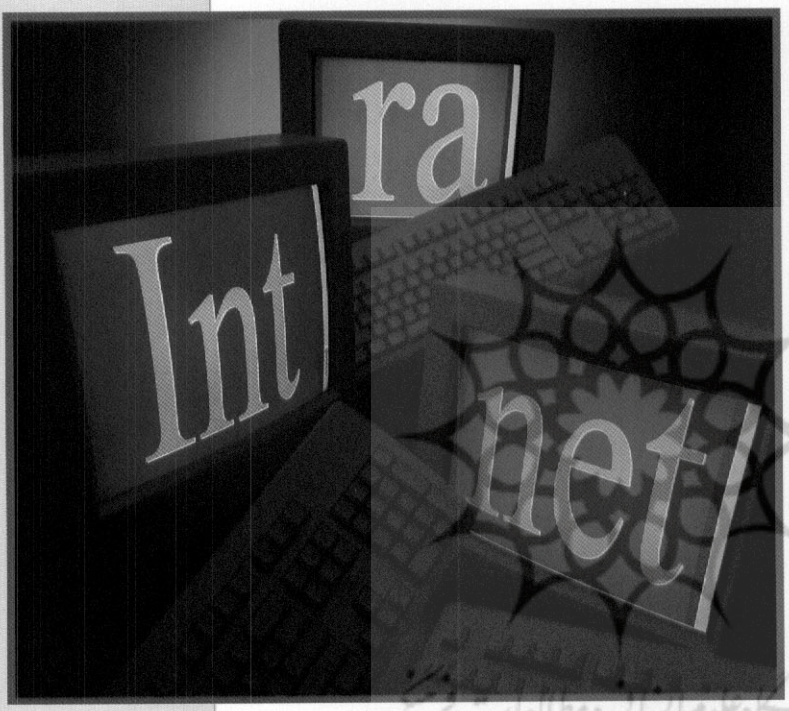


مدیریت امنیت اطلاعات در بنگاه‌های اقتصادی

نام ایران در فهرست کشورهای دارای گواهی‌نامه مدیریت امنیت اطلاعات نیست

مهندس بابک باقرزادگان

کسب اطلاعات تجاری و آگاهی از موقعیت رقبا در دنیای تجارت آنچنان مهم است که شرکت‌های بزرگ برای دستیابی به آنها مبالغ هنگفتی هزینه می‌کنند، اما مهم‌تر از آن حفظ و مراقبت از اطلاعات تجاری است که غالباً از طریق کنترل‌های امنیتی صورت می‌گیرد. اهمیت و حساسیت مدیریت امنیت اطلاعات ISMS تا آن حد است که همانند بحث مدیریت کیفیت برای آن استانداردهایی تعریف شده است. با وجود آن که بیشترین کشورهایی که موفق به اخذ این گواهی‌نامه شده‌اند در قاره آسیا قرار دارند متأسفانه کشور ما به دلایل مختلف نامی در فهرست جهانی دارندگان سیستم فوق ندارد و از این نظر از صحنه رقابت بین‌المللی دور است.



اگر شما بخواهید به عنوان یک کارآفرین یا سرمایه‌گذار با یکی از شرکای تجاری خود روابط کاری ایجاد کنید، قطعا مایلید این رابطه، رابطه‌ای محکم و کم نقص باشد. مواردی مانند نحوه ارتباط با شرکای کاری، تحلیل قیمت تمام شده، برنامه‌ریزی و نگهداری اطلاعات مشتریان، موارد مهم، حساس و استراتژیکی هستند که هر یک از رقبای شما از به دست آوردن تمام یا حتی بخشی از آنها خوشحال می‌شوند. هر کسی که با اطلاعات مشتری سر و کار دارد، خیلی زود در می‌یابد که باید به خوبی از اطلاعات موجود محافظت کند. نه تنها شما بلکه تامین‌کنندگانتان نیز باید چنین سیاستی را در کار خود داشته باشند. می‌توانید بخشی از فعالیت‌های ICT خود را برون‌سپاری کنید، اما آیا اشخاص ثالث و پیمانکاران شما نیز به اندازه شما در محافظت از اطلاعات بنگاهتان وسواس لازم را دارند؟

موارد فوق تنها بخشی از نگرانی‌های صاحبان و مدیران بنگاه‌های اقتصادی برای حفاظت از اطلاعات به عنوان مهم‌ترین دارایی بنگاه‌هشان است. در سالهای اخیر فضای فعالیت‌های اقتصادی در سرتاسر جهان به شدت رقابتی شده است و یکی از دلایل عمده این تحول، رشد سرعت و کیفیت ارتباطات و متولد شدن فناوری اطلاعات است. از دیگر نتایج ظهور فناوری اطلاعات، تسهیل انتقال اطلاعات از مکانی به مکانی دیگر است که به همان اندازه که مفید است، ریسک خروج اطلاعات از سازمان و سوءاستفاده از آن را نیز افزایش می‌دهد. بنابراین بهره‌مندی از مزایای آن مستلزم مدیریت کاربری و ایجاد کنترل‌های امنیتی لازم است. به منظور پیاده‌سازی امنیت اطلاعات و تضمین آن، در سال ۱۹۹۵ اولین استاندارد مدیریت امنیت اطلاعات با نگرشی سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. و از آن سال بر تعداد شرکت‌ها و بنگاه‌های اقتصادی که لزوم رعایت استانداردهای امنیت اطلاعات را درک کرده و گواهینامه‌های ملی یا بین‌المللی این استاندارد را دریافت می‌کنند افزوده می‌شود.

در جدول ۱ تعداد گواهینامه‌های ISMS* دریافت شده توسط کشورهای مختلف در آگوست سال ۲۰۰۵ دیده می‌شود. همانطور که مشاهده می‌کنید، کشور ژاپن به دلیل داشتن زمینه‌های مساعد و توانایی‌های منحصر بفرد خود در پیاده‌سازی استانداردهای مختلف، به تنهایی ۹۶۷ گواهینامه ISMS دریافت کرده است. بیشتر کشورهای دارنده این گواهینامه، کشورهای پیشرفته صنعتی و تعدادی از کشورهای در حال توسعه هستند. اما وجود نام کشورهایی مانند مصر، ترکیه و مراکش نشان از این دارد که تمایل، یا بهتر بگوییم، نیاز به مدیریت امنیت اطلاعات در شرکت‌های کوچک کشورهای در حال توسعه خاور میانه و شمال آفریقا نیز احساس شده است.

در جدول شماره ۲ جدیدترین رده‌بندی را که در ماه می‌سال جاری میلادی منتشر شده، مشاهده می‌کنید. باز هم کشور ژاپن در صدر جدول قرار دارد و فاصله خود را با کشورهای دیگر به شدت افزایش داده است. به جرات می‌توان گفت بنگاه‌های ژاپنی مانند تمام مدل‌های استاندارد و در بیشتر عرصه‌ها، در اینجا نیز الگوی تمام عیاری برای تمامی‌شرکت‌ها و بنگاه‌های کشورهای دیگر هستند. علت موفقیت شرکت‌های ژاپنی در دریافت این گواهینامه، فراهم بودن بستر آن و چه بسا عمل به کنترل‌های اشاره شده در استاندارد پیش از رجوع به آن است. شرکت‌های موفق خود به خود تجربه کنترل‌های لازم در زمینه امنیت اطلاعات و مدیریت آن را در درون خود به دست آورده‌اند.

جدول ۱- تعداد گواهینامه‌های ISMS صادر شده برای کشورهای مختلف (آگوست ۲۰۰۵)

Japan	967	Czech Republic	5	Egypt	1
UK	208	Poland	5	France	1
India	118	Switzerland	5	Kuwait	1
Taiwan	55	Greece	4	Lebanon	1
Germany	38	Iceland	4	Lithuania	1
Korea	32	Brazil	3	Luxemburg	1
Italy	25	Mexico	3	Macau	1
Netherlands	21	Saudi Arabia	3	Macedonia	1
USA	20	Spain	3	Morocco	1
Hong Kong	17	UAE	3	Qatar	1
Finland	14	Argentina	2	Romania	1
Hungary	13	Belgium	2	Russian Federation	1
China	12	Canada	2	Slovenia	1
Australia	11	Denmark	2	South Africa	1
Singapore	11	Isle of Man	2	Turkey	1
Ireland	11	Malaysia	2	Relative Total	1672
Norway	10	Slovak Republic	2	**Absolute Total**	**1660***
Austria	8	Chile	1		
Sweden	7	Colombia	1		

جدول ۲- تعداد گواهینامه‌های ISMS صادر شده برای کشورهای مختلف (می۲۰۰۷)

Japan	2148	Turkey	11	Denmark	2
UK	316	Spain	10	Lithuania	2
India	294	Philippines	9	Oman	2
Taiwan	125	Saudi Arabia	9	Slovak Republic	2
Germany	70	Sweden	8	South Africa	2
China	58	UAE	8	Sri Lanka	2
Hungary	56	Iceland	7	Armenia	1
Korea	52	Kuwait	6	Bulgaria	1
USA	50	Russian Federation	6	Egypt	1
Australia	44	Greece	5	Gibraltar	1
Italy	43	Bahrain	4	Lebanon	1
Netherlands	31	Canada	4	Luxemburg	1
Hong Kong	29	Indonesia	4	Macedonia	1
Czech Republic	25	Slovenia	4	Moldova	1
Singapore	25	Thailand	4	Morocco	1
Malaysia	20	Argentina	3	New Zealand	1
Brazil	17	France	3	Peru	1
Ireland	17	Isle of Man	3	Qatar	1
Poland	16	Macau	3	Ukraine	1
Austria	15	Pakistan	3	Uruguay	1
Finland	14	Romania	3	Vietnam	1
Norway	14	Belgium	2	Yugoslavia	1
Mexico	12	Colombia	2	Relative Total	3664
Switzerland	11	Croatia	2	**Absolute Total**	**3653***

حال به مقایسه ارقام جداول فوق می‌پردازیم. بر اساس این دو جدول، جدول‌های دیگری بر اساس گواهینامه‌های صادر شده در هر قاره ایجاد شده است. در جدول‌های شماره ۳ و ٤ ملاحظه می‌کنید که تعداد کشورهای دارنده گواهی‌نامه ISMS در قاره آسیا بسیار بیشتر از سایر قاره‌ها است. هر چند علت عمده این تفاوت مربوط به کشور ژاپن است، اما سایر کشورهای آسیایی مانند هند، چین، کره و تایوان نیز وضعیت کاملا قابل قبولی در رده‌بندی جهانی دارند. رتبه این کشورها در جدول‌های شماره ۱ و ۲ ارتباط نزدیکی با سهم آنها از تولید و کاربری نرم‌افزار و محصولات دیجیتال، ضریب نفوذ فناوری اطلاعات در صنایع و ارتباط فعال آنها با بازارهای جهانی (عضویت در سازمان جهانی تجارت و ...) دارد.

در جدول شماره ۵ رشد نسبی تعداد گواهینامه‌های ISMS را در هر قاره در فاصله آگوست ۲۰۰۵ تا می۲۰۰۷ مشاهده می‌کنید.

از نظر سرعت رشد، بعد از اقیانوسیه، خاورمیانه با رشدی معادل ۲۵۰ درصد قرار دارد که رقم قابل توجهی است. کشورهای عربستان سعودی، امارات متحده، بحرین، کویت، لبنان و حتی کشور عمان هر یک چند گواهینامه ISMS دریافت کرده‌اند. این آمار نشان‌دهنده عزم این کشورها برای رقابت با سایر کشورها و اشتیاق آنها برای راهیابی به بازارهای جهانی است. ضمن اینکه بستر مساعدی برای پیاده‌سازی این استاندارد داشته‌اند یا دست به فراهم کردن آن زده‌اند.

در این میان سهم کشور ما و شرکت‌های ایرانی چقدر است؟ در جداول فوق که اثری از نام ایران نبود. اما واقعیت این است که احتمالاً تا کنون به جز یکی دو شرکت هیچ شرکت ایرانی برای پیاده‌سازی این استاندارد و دریافت گواهینامه آن اقدامی نکرده است. علت چیست؟

در بند ۱,۱ استاندارد BS۹۹۷۷-۲-۲۰۰۲ در مورد علت طراحی این استاندارد چنین آمده است:

جدول ۳- تعداد گواهینامه‌های صادر شده در هر قاره تا آگوست سال ۲۰۰۵

نام قاره	آسیا	اروپا	آمریکا	خاورمیانه	اقیانوسیه
تعداد گواهینامه‌ها	۱۲۱۴	۳۹۷	۳۲	۱۰	۱۲

جدول ٤- تعداد گواهینامه‌های صادر شده در هر قاره تا می سال ۲۰۰۷

نام قاره	آسیا	اروپا	آمریکا	خاورمیانه	اقیانوسیه
تعداد گواهینامه‌ها	۲۷۷۱	۷۰۶	۹۰	۳۵	۴۸

جدول ۵- رشد نسبی تعداد گواهینامه‌ها در هر قاره در فاصله آگوست ۲۰۰۵ تا می۲۰۰۷

نام قاره	آسیا	اروپا	آمریکا	خاورمیانه	اقیانوسیه
تعداد گواهینامه‌ها	٪۱۲۸	٪۷۸	٪۱۸۱	٪۲۵۰	٪۳۰۰

«...تضمین کنترل‌های امنیتی مناسب که به صورتی جامع از **اموال اطلاعاتی** محافظت کند و از این حیث به مشتریان و سایر گروه‌های ذینفع اطمینان دهد...». بعبارتی، هدف از طراحی ISMS حفاظت از دارایی‌های مهم سازمان و در راس آن اموال اطلاعاتی است. علت حفاظت از دارایی‌های مهم عبارتند از:

۱.الزامات کسب و کار (تضمین تداوم کسب و کار) شامل:

- مشتریان/ سهامداران
- بازاریابی
- به دست آوردن اعتماد مشتریان و شرکا
- داشتن ابزار مدیریتی داخلی

۲.پایداری سازمان: تمرکز روی نیازها و انتظارات مشتریان

۳. الزامات قانونی: رعایت قوانین ملی و بین‌المللی در حفاظت از اموال اطلاعاتی شامل داده‌های مشتریان، نرم افزارهای اشخاص ثالث و ....

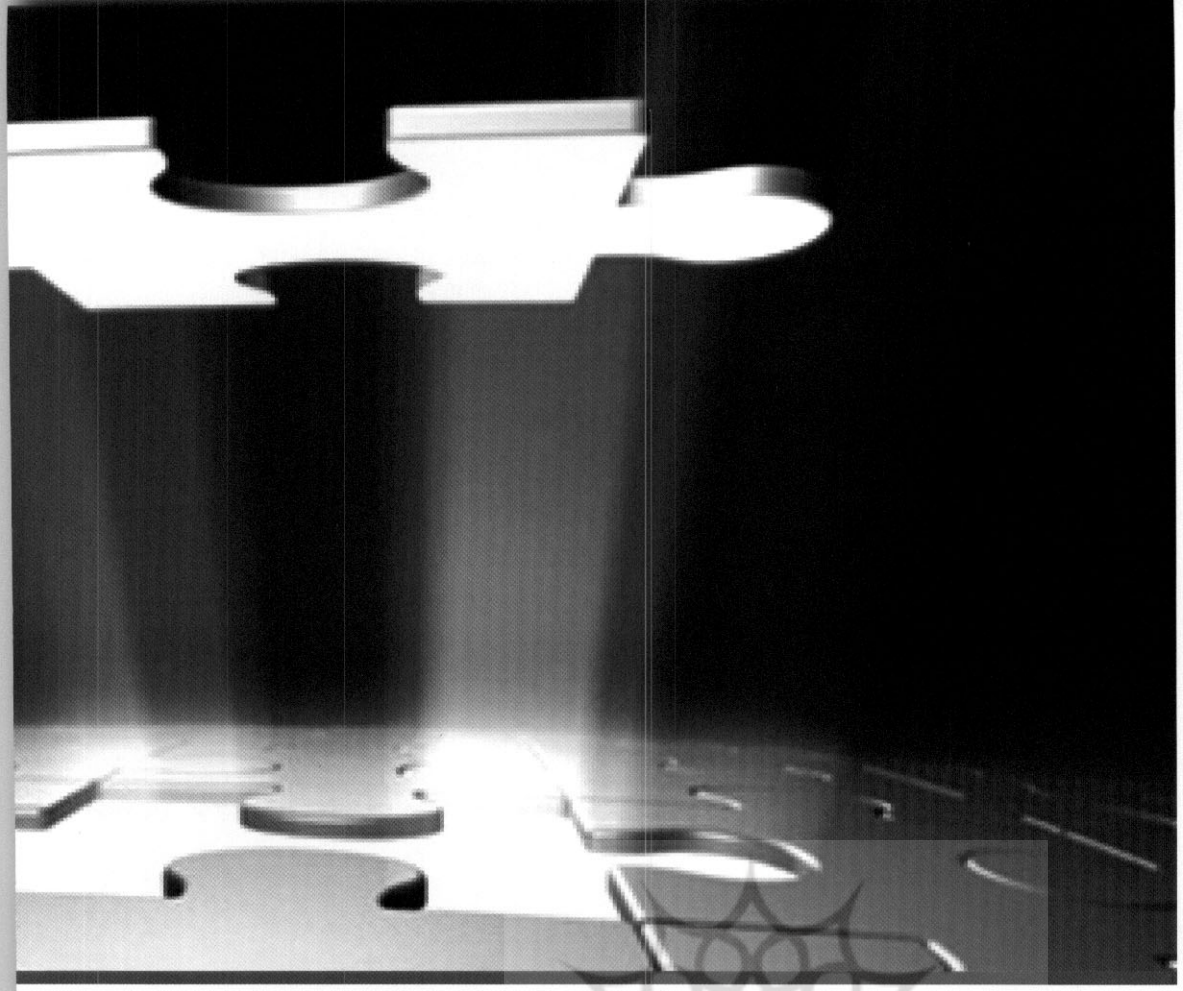
٤. الزامات امنیتی قراردادی (زیرساخت امنیتی اطلاعات):

- اتصال اینترنتی با دیگر سازمانها
- اکسترانت با شرکای خارجی
- اتصال از راه دور کارمندان خارج از شرکت

در بندهای ۵ و ٦ ISMS BSٔٔ۷۹۹-۲-۲۰۰۲ بر مسئولیت مدیریت ارشد سازمان در تایید، فراهم کردن امکانات لازم و بازبینی ISMS در مراحل مختلف تاکید شده است. در واقع حمایت مدیریت ارشد سازمان، یکی از شرایط لازم جهت پیاده‌سازی ISMS است. حمایت مدیریت ارشد، از بعد داخلی به معنی داشتن اهرم قدرت لازم جهت الزام کلیه واحدها به رعایت کنترل‌های استاندارد و حل اختلافات در مواقع لازم است. این امر از بعد خارجی و مسائل برون سازمانی نیز به معنای آشنایی مدیریت ارشد با الزامات قانونی و پذیرش مسوولیت آنهاست.

حال ببینیم چرا ISMS تاکنون در هیچ شرکت ایرانی پیاده سازی نشده است و مدیران سازمان‌ها و بنگاه‌ها در مورد این استاندارد اطلاعات کمی دارند. با نگاهی به موارد فوق به عنوان دلایل و اهداف استاندارد ISMS در می‌یابیم که اصولا انگیزه‌های لازم در شرکت‌های ایرانی برای پیاده‌سازی این سیستم وجود ندارد. اطلاعات در اغلب شرکت‌های ایرانی به عنوان یک دارایی (asset) مطرح نیست. بنابراین هدف اصلی ISMS که محافظت از اموال اطلاعاتی سازمان است اهمیت و ضرورت خود را به یکباره از دست می‌دهد.

در مورد دلایل حفاظت از دارایی‌های مهم



اطلاعات در اغلب شرکت‌های ایرانی به عنوان یک دارایی (asset) مطرح نیست. بنابراین هدف اصلی ISMS که محافظت از اموال اطلاعاتی سازمان است اهمیت و ضرورت خود را به یکباره از دست می‌دهد

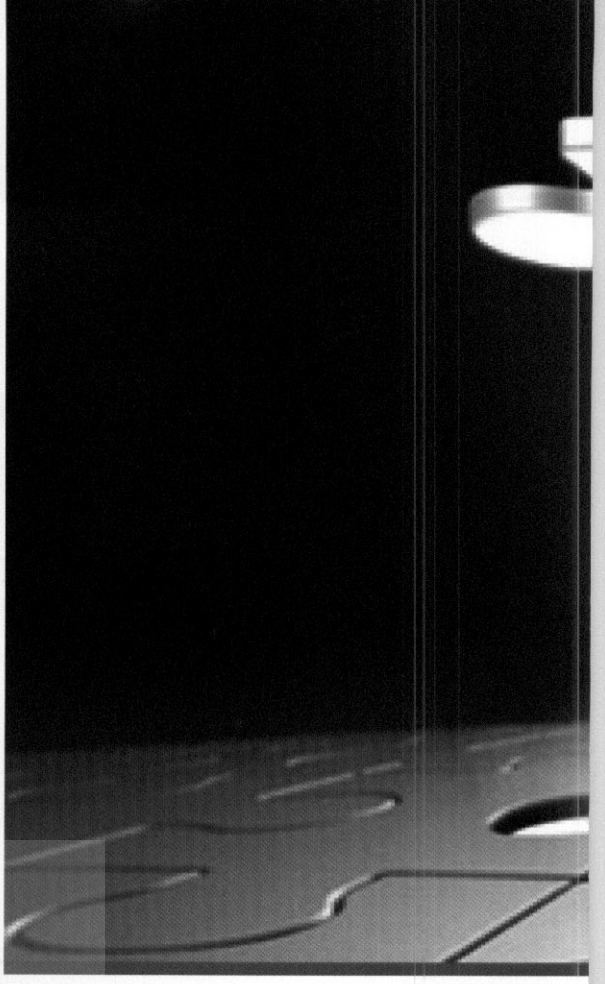
نیز موارد متعددی وجود دارد که هنوز در حیطه دغدغه‌های شرکت‌ها و بنگاه‌های ایرانی قرار نگرفته است. مثلا ارتباط با مشتریان/ سهامداران به صورت انتشار اطلاعات مربوط به مناقصه، اطلاعات سهام، قراردادها و... خیلی کم به صورت الکترونیکی انجام و در روش‌های متداول کنونی هم، از شگردهای سنتی و قدیمی‌در حفظ اطلاعات استفاده می‌شود.

در زمینه بازاریابی و به دست آوردن اعتماد مشتریان و شرکا نیز وضع به همین منوال است. اصولا اقتصاد ایران به دلیل ساختار و فرهنگ غالبا دولتی، نداشتن دانش نوین، نداشتن ارتباط با بازارهای آزاد و نداشتن رقیب در قلمرو انحصارزده و محدود خود، اهمیت چندانی به مدیریت ارتباط با مشتریان و جلب اعتماد مشتریان و شرکا نمی‌دهد. بنابراین چگونه می‌تواند به دنبال ارتقای کیفیت چیزی باشد که فاقد آن است؟

در زمینه در اختیار قرار دادن ابزار مدیریت داخلی، استاندارد ISMS می‌تواند مفید و موثر باشد. در حال حاضر به دلیل استفاده از شگردهای سنتی و غالبا دستی، امکان استخراج گزارشات دقیق و به روز در سازمان موجود نیست. سیستم‌های MIS و سیستم‌های یکپارچه موجود نیز بعضا به دلیل استفاده نادرست، دچار تناقض‌هایی در اطلاعات خروجی می‌شوند. با استفاده از ISMS می‌توان این ضعف را در سیستم‌های مکانیزه برطرف و آنها را قابل اطمینان کرد. یکی از مشکلات در راه استفاده از سیستم‌های موجود نبود دانش کافی نزد مدیران میانی و ارشد سازمان و عدم موفقیت در جلب حمایت و همکاری آنهاست.

در زمینه الزامات قانونی نیز ضعف فاحشی در سیستم قانونگذاری کشور مشاهده می‌شود. نداشتن قانون کپی رایت و تعریف نادرست از حق نشر، حق تالیف و مالکیت معنوی و نپیوستن به کنوانسیون‌های جهانی نقاط ضعفی است که باید برای بالا بردن استانداردها و متصل شدن به بازارهای جهانی آنها را برطرف کرد. هنوز در داخل کشور نمی‌توان تعریف دقیقی از سرقت اطلاعات، نرم‌افزار، جرم رایانه‌ای، مجرمان فضای مجازی (cybercriminals) و نظیر اینها ارائه داد. بنابراین در استاندارد ISMS نیز توانایی اجرای بندهای مرتبط استاندارد و اعمال کنترل‌های لازم وجود نخواهد داشت.

در زمینه الزامات امنیت قراردادی (زیرساخت) نیز وضعیت چندان مطلوب نیست. هر چند در سخت افزار فناوری و امنیت اطلاعات چندان از قافله عقب نیستیم. اما در زمینه مدیریت امنیت اطلاعات، کاربرد و نگهداری آن نقاط ضعفی مشاهده می‌شود. به عنوان مثال در زمینه نگهداری زیرساخت‌های کلان شبکه ملی **لایحه قانون صیانت از حریم مسیرهای شبکه کابل فیبر نوری** هنوز به تصویب مجلس شورای اسلامی نرسیده است. با توجه



به اظهارات وزیر ارتباطات و فناوری اطلاعات که در حال حاضر، مقررات کافی برای تسهیل در کابل‌کشی فیبر نوری، همکاری سازمان‌های دولتی و اخذ خسارت از اشخاص وجود ندارد، باید پرسید لایحه قانون صیانت از حریم مسیرهای شبکه کابل فیبر نوری در تاریخ ۸۴/۹/۱۵ به دولت ارسال و هم‌اکنون در مرحله نظرخواهی از دستگاه اجرایی قرار دارد...». ملاحظه می‌کنید که حدود دو سال از ارسال لایحه مذکور می‌گذرد و هنوز در مرحله نظرخواهی قرار دارد!

در همین مورد اطلاعات زیر که از سایت وزارت ارتباطات و فناوری اطلاعات استخراج شده جالب توجه است:

«در پی قطعی‌های مکرر شبکه فیبرنوری که به دلیل عدم وجود قانون صیانت از حریم مسیرهای فیبرنوری به وقوع می‌پیوندد، شرکت ارتباطات زیرساخت طی سال گذشته حداقل ۱۵۳ میلیارد و ۲۳۴ میلیون ریال خسارت مالی را متحمل شد.

۱۹۰ بار قطعی در برخی مسیرهای شبکه ملی فیبرنوری طی سال گذشته در مجموع ۷۰ هزار دقیقه قطعی در شبکه زیرساخت ایجاد کرد که عملا امکان برقراری ارتباطات در شبکه بین‌المللی و بین شهری کشور را به میزان ۹۵۷ میلیون و ۶۵۰ هزار کانال/ دقیقه از شرکت ارتباطات زیرساخت سلب کرد.

این در حالی است که طبق برآوردهای صورت گرفته، بازسازی یک مسیر قطع شده حدود ۲۰ تا ۳۰ میلیون ریال برای شرکت زیرساخت هزینه در بردارد که با توجه به ۱۹۰ قطعی به وقوع پیوسته در سال گذشته، این شرکت حدود ۴۰۰ میلیون تومان علاوه بر خسارت‌های قطعی شبکه برای بازسازی و ترمیم مسیرهای قطع شده فیبرنوری هزینه کرده است.»

در مجموع با توجه به اینکه در بیشتر بندهای فوق- که دلایل نیاز به داشتن یک استاندارد جامع و مانع در امنیت اطلاعات هستند- ضعف‌های آشکاری در کشور و واحدهای اقتصادی وجود دارد، انتظار دریافت گواهینامه ISMS و پیاده سازی این استاندارد نیز انتظاری بی مورد است. از آنجا که اطلاعات مدیران ارشد و میانی سازمان‌ها در زمینه فناوری اطلاعات و مدیریت آن زیاد نیست بنابراین، نسبت به آن رغبتی نشان نمی‌دهند. فقط تحصیلکردگان رشته فناوری اطلاعات و کارشناسان رایانه به دلیل ماهیت تخصص و حرفه خود با این مبحث آشنایی نسبی دارند. اما این دسته نیز یا دست تنهامی‌مانند یا به دلیل نداشتن زمینه‌های مدیریتی، خواسته و ناخواسته مدیریت امنیت اطلاعات را تا حد مهندسی امنیت شبکه‌های رایانه‌ای تنزل درجه می‌دهند و آن را به حاشیه می‌رانند.

در پایان پیشنهاد می‌شود برای آشنا کردن مدیران و تصمیم گیرندگان با این استاندارد و گسترش آن، شرکت‌هاو ممیزان و دست اندرکاران ارایه دهنده این استاندارد، جلسات اطلاع‌رسانی و تبلیغاتی برگزار کنند. ضمن اینکه در روند فعلی، مرور زمان نیز وابستگی سازمان‌ها را به سیستم‌های فناوری اطلاعات، مانند پایگاه‌های داده و ... افزایش می‌دهد. این موارد به علاوه الزامات الحاق به سازمان جهانی تجارت، بنگاه‌های اقتصادی و حتی سازمان‌های دولتی کشور را در آینده ای نزدیک به سمت به رسمیت شناختن فناوری اطلاعات و اتخاذ راهکارهای مدیریت آن مانند ISMS سوق خواهد داد.

نقاط ضعف

نداشتن قانون کپی رایت و تعریف نادرست از حق نشر، حق تالیف و مالکیت معنوی و نپیوستن به کنوانسیون‌های جهانی نقاط ضعفی است که باید برای بالا بردن استانداردها و متصل شدن به بازارهای جهانی آنها را برطرف کرد