فصلنامه رویکردهای پژوهشی نو در علوم مدیریت
Journal of New Research Approaches in Management Science
سال دوم. شماره دهم. زمستان ۱۳۹۷، صص۱۳۷-۱۱۵ Vol 2. No 10. 2019, p 115-137
شماره شاپا (۲۵۸۸-۵۵۶۱) ISSN: (2588-5561)

ضرورت سنجش عملکرد مدیریت امنیت اطلاعات در سازمان‌ها

شیدا شیرواندهی
کارشناسی ارشد کتابداری. کارشناس سازمان اسناد و کتابخانه ملی ایران
shirvandehi7@gmail.com

چکیده

امنیت اطلاعات شالوده‌ی هر نوع سیستمی می‌باشد و با حضور امنیت در سیستم‌ها خارج از نوع و هدف، می‌تواند برای مسئولان و مدیران آن سازمان اطمینان خاطر در برابر انواع آسیب‌ها، تهدیدات، ریسک‌ها را بدنبال داشته باشد، مدیریت امنیت اطلاعات بخشی از سیستم مدیریت کلی و سراسری در یک سازمان است که بر پایه رویکرد مخاطرات کسب‌وکار قرار داشته و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات است این نوع مدیریت مسأله‌ای است که در صورت پیاده‌سازی صحیح می‌تواند با کاهش ریسک‌های پیرامونی به عنوان یک عامل مهم، در تضمین سطح امنیتی تعریف شده، نقش بسزایی را ایفا نماید. استقرار سیستم مدیریت امنیت اطلاعات بعنوان سامانه‌ای جامع که همه ابعاد امنیت از جمله خط‌مشی امنیتی، سازماندهی امنیت اطلاعات، مدیریت دارایی‌ها، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی، استفاده، توسعه و نگهداری سامانه‌های اطلاعاتی، پشتیبانی حوادث، مدیریت تداوم کسب‌وکار، سازگاری با الزامات قانونی، حقوقی و قراردادی را در برگیرد، در سازمان‌ها امری ضروری است.

واژه‌های کلیدی: امنیت، مدیریت، اطلاعات، سازمان‌ها

[Downloaded from jnraims.ir on 2026-11-20]

مقدمه

رایج شدن فناوری اطلاعات و ارتباطات و گسترش روزافزون این فناوری، منجر به تشکیل جامعهٔ اطلاعاتی شده که بشر را به عصر اطلاعات وارد کرده است. ویژگی برجسته این فناوری‌ها، تأثیری است که بر تکامل ارتباطات راه دور گذاشته است. در راستای این دگرگونی و مدرن شدن ابزارهای نوین اطلاعات و ارتباطات، استفاده وسیع از پست الکترونیک و دستیابی به اطلاعات از طریق وب سایت‌های متعدد در اینترنت، نمونه‌هایی از این پیشرفت‌ها می‌باشد که جامعه امروزی را به طور پیچیده‌ای دگرگون ساخته است. از سوی دیگر، سهولت در دسترسی و جستجوی اطلاعات موجود در سیستم‌های رایانه‌ای، توأم با امکانات عملی نامحدود در مبادله و توزیع اطلاعات بدون توجه به فواصل جغرافیایی- منجر به رشد زیاد کسب اطلاعات موجود از این طریق شده است. این اطلاعات، موجب افزایش تغییرات اجتماعی و اقتصادی پیش‌بینی نشده‌ای، شده است. اما پیشرفت‌های مذکور جنبهٔ خطرناکی نیز دارد که پیدایش انواع تخلفات و جرایم و همچنین بهره‌برداری از فنآوری جدید در ارتکاب اعمال غیرقانونی و نامشروع، بخشی از آن به شمار می رود. موارد غیراصولی و مضر نامبرده، عمدتاً بر اثر بهره‌گیری غیرقانونی، نا به حق و غیرمشروع از اطلاعات و داده‌ها و سوءاستفاده از اطلاعات گسترده و بی‌انتهای مجازی است که در اقیانوس پهناور شبکه جهانی اینترنت و فضای وب و سایبر، غوطه ور می باشد.

با توجه به ویژگی‌های عصر امروزی که عصر اطلاعات نامیده شده مهم‌ترین سرمایه برای هر فرد و یا سازمان اطلاعات است. به همین جهت در این عصر، امنیت اطلاعات جزء یکی از مهم‌ترین مسائل امروزی است. امنیت اطلاعات در واقع محافظت از اطلاعات در برابر طیف وسیعی از تهدیدات شامل دسترسی، کاربرد، افشاء، قطع، تغییر یا انهدام غیرمجاز اطلاعات است که با هدف تضمین استمرار فعالیت‌های کاری، به حداقل رساندن ریسک‌های کاری و به حداکثر رساندن میزان بازده سرمایه‌گذاری‌ها و فرصت‌ها صورت می‌پذیرد. همچنین امنیت اطلاعات، کنترلی برای تضمین تداوم حفاظت از دارایی‌های سازمان از آسیب یا از دست دادن معنا شده است. به عبارت دیگر امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد. امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است (شیرازی، آل شیخ ۱۳۸۸).

امنیت داده‌ها و اطلاعات در کلیه شبکه‌های کامپیوتری در نهادها، موسسات و سازمان‌های متشکل از مجموعه‌ای از یارانه‌های به هم مرتبط، واجد اهمیت و توجه ویژه است. مسایل مهم مربوط به امنیت در سازمان‌ها می‌تواند شامل امنیت سخت‌افزارها، مرکز اطلاعات، جایگاه فیزیکی سرورها، امنیت تبادل اطلاعات، امنیت نرم افزاری کاربردی، امنیت نرم افزارهای ضدویروس باشد (حریری، ۱۳۹۱).

[Downloaded from jnraims.ir on 2026-11-20]

امنیت اطلاعات چیست؟

اطلاعات:[1] اطّلاع یا آگاهش، در کوتاه‌ترین تعریف، «داده‌های پردازش نشده» است. داده‌ها، مواد خام بالقوه معنی‌داری هستند که ما آنها را در راستای شناخت و فهم هر مفهوم مادی یا غیر مادی، به واسطه روش‌های پژوهشی، و با استفاده از ابزارهای شناختی به دست می‌آوریم. داده یک شرح مقدماتی از یک پدیده، اتفاق، فعالیت و یا تعاملات است که ثبت شده است، دسته‌بندی شده و ذخیره شده است؛ اما سازماندهی نشده و برای یک منظور مشخص آماده نشده است. داده‌ها عناصر اصلی اطلاعات هستند. داده‌ها در صورتی به اطلاعات تبدیل می‌شوند که افراد بخواهند برای درک بیشتر از آنها استفاده کنند. اطلاعات، داده‌های خلاصه‌ای هستند که گروه‌بندی، ذخیره، پالایش و سازماندهی شده‌اند تا بتوانند معنی‌دار شوند. اطلاعات زمانی ارزش پیدا می‌کنند که برای یک بُعد خاص، یک فرد خاص، یک هدف خاص و در زمان خاص گردآوری و آماده شوند، لذا اطلاعاتی که برای یک مدیر، جنبه اطلاعاتی دارد، برای مدیر دیگر ممکن است اصلاً ارزشی نداشته باشد. بدین ترتیب، اطلاعات، آگاهی‌های به دست آمده از عنصرها و رویدادهای جهان هستی است. به زبان محدود تکنیکی، مجموعه‌ای از نمادهای زبانی معنی‌دار و پیوسته درباره موجودات است. (استیوارت[2]، ۲۰۰۱)

امنیت: در واژه‌نامه وبستر[3] این گونه آمده است: "امنیت به معنای کیفیت یا حالت امن بودن، رهایی از خطر، ترس و احساس نگرانی و تشویش می‌باشد. امنیت به طور کلی عبارتست از حفاظت از آنچه برای ما ارزشمند است در برابر حملات عمدی و غیرعمدی توسط سرویس‌ها و اشخاص.

امنیت سازمانی: وجود یک حفره و یا مشکل امنیتی، می‌تواند یک سازمان را به روش‌های متفاوتی تحت تاثیر قرار خواهد داد. آشنائی با عواقب خطرناک یک حفره امنیتی در یک سازمان و شناسائی مهمترین تهدیدات امنیتی که می‌تواند حیات یک سازمان را با مشکل مواجه نماید، از جمله موارد ضروری به منظور طراحی و پیاده‌سازی یک مدل امنیتی در یک سازمان می‌باشد. وجود حفره‌های امنیتی در یک سازمان، می‌تواند پیامدهای منفی متعددی را برای یک سازمان به دنبال داشته باشد: کاهش درآمد و افزایش هزینه، خدشه به اعتبار و شهرت یک سازمان، از دست دادن، داده و اطلاعات مهم اختلال در فرآیندهای جاری یک سازمان پیامدهای قانونی به دلیل عدم ایجاد یک سیستم ایمن و تاثیر جانبی منفی بر فعالیت سایر سازمان‌ها (ترابی ۱۳۹۵)

امنیت اطلاعات: عبارت است از حفاظت اطلاعات و به حداقل‌رساندن دسترسی غیرمجاز به آنها (جعفری، (۱۳۹۰). همچنین پاسداری از حریم خصوصی افراد است که معادل اطلاعات خصوصی، مبادلات تجاری، مبادلات مالی، ارتباطات شخصی، اقامتگاه شخصی و وضعیت فیزیکی و جسمانی فرد

1- Information
2- Stewart
3- Webster

[Downloaded from jnraims.ir on 2026-11-20]

می‌باشد (راف[1] ۲۰۱۳ ص ۱۴-۱۸) و در تعریف دیگر امنیت اطلاعات حفاظت اطلاعات و به حداقل رساندن دسترسی غیرمجاز به آنها" است (عابدی جعفری؛ اسد نژاد رکنی؛ ایزدانی، ۱۳۹۰، صص ۶۹-۸۸). امنیت اطلاعات عبارت است از حفاظت اطلاعات و به حداقل رساندن دسترسی غیر مجاز به آنها (جراحی و عظیمی، ۱۳۸۷) همچنین علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر تغییرات غیرمجاز است (عامری، حسینی راد و باغبادی، ۱۳۹۳)، امنیت اطلاعات حفاظت از محرمانگی، تمامیت و دسترس پذیری اطلاعات است. علاوه بر اینها سایر ویژگی‌ها از قبیل اصالت، قابلیت جوابگویی، اعتبار، انکار ناپذیری و قابلیت اطمینان اطلاعات نیز می توانند مشمول این حفاظت باشند.

تاریخچه امنیت اطلاعات

مفهوم و اهمیت ایمنی و امنیت از همان آغاز زندگی بشر وجود داشت. بشر همیشه برای بقا و ادامه زندگی سعی نموده است که جهت حفاظت از خود و دارایی‌هایش، آگاهی‌ها و دانش خود را نسبت به محیط و خطرات اطراف خود افزایش دهد. ایمنی و امنیت یک مفهوم ذاتی است که با حفاظت از چیزهای ارزشمند ارتباط پیدا می‌کند؛ و به طور خلاصه، ایمنی به راه‌های ممکن که در آن سلامت یک سیستم بایستی تأمین و دفع نقایصی که در راه حصول به اهداف وجود دارد، تعریف می‌گردد. از زمانی که نوشتن و تبادل اطلاعات آغاز شد، همه انسان‌ها مخصوصاً سران حکومت‌ها و فرماندهان نظامی در پی راهکاری برای محافظت از محرمانه بودن مکاتبات و تشخیص دستکاری آنها بودند. ژولیوس سزار ۵۰ سال قبل از میلاد یک سیستم رمزنگاری مکاتبات ابداع کرد تا از خوانده شدن پیام‌های سری خود توسط دشمن جلوگیری کند حتی اگر پیام به دست دشمن بیفتد. جنگ جهانی دوم باعث پیشرفت چشمگیری در زمینه امنیت اطلاعات گردید و این آغاز کارهای حرفه‌ای در حوزه امنیت اطلاعات شد (کوآ[2] ۲۰۱۶). پایان قرن بیستم و سالهای اولیه قرن بیست و یکم شاهد پیشرفتهای سریع در ارتباطات راه دور، سخت‌افزار، نرم‌افزار و رمزگذاری داده‌ها بود. در دسترس بودن تجهیزات محاسباتی کوچکتر، قوی‌تر و ارزان‌تر پردازش الکترونیک داده‌ها باعث شد که شرکت‌های کوچک و کاربران خانگی دسترسی بیشتری به آنها داشته باشند. این تجهیزات به سرعت از طریق شبکه‌های رایانه مثل اینترنت به هم متصل شدند. با رشد سریع و استفاده گسترده از پردازش الکترونیک داده‌ها و کسب‌وکار الکترونیک از طریق اینترنت، همراه با ظهور بسیاری از خرابکاری‌های بین‌المللی، نیاز به روش‌های بهتر حفاظت از رایانه‌ها و اطلاعات آنها ملموس گردید. رشته‌های دانشگاهی از قبیل امنیت رایانه‌ای، امنیت اطلاعات و اطلاعات مطمئن همراه با سازمان‌های متعدد حرفه‌ای پدید آمدند. هدف مشترک این فعالیت‌ها و سازمان‌ها حصول اطمینان از امنیت و قابلیت اطمینان از سیستم‌های اطلاعاتی است (جرالد ۲۰۱۶، ص ۱۱۹-۱۲۹و۲۷۳-۲۸۱و ۱۳۱-۱۷۳).

1- Rafe
2- Coa

[Downloaded from jnraims.ir on 2026-11-20]

اما تاریخچه سیستم مدیریت امنیت از آنجا آغاز می‌شود که یک موسسه امنیتی در سال ۱۹۸۹ اقدام به انتشار کدهایی برای سنجش میزان امنیت کرد که به کد تمرینی کاربران[1]معروف شد. مدتی بعد کیفیت و کمیت این کدها از سوی مرکز محاسبات بین‌المللی[2]و یک کنسرسیوم از کاربران مورد بررسی قرار گرفت و درنهایت به صورت نخستین نسخه استاندارد امنیت با عنوان مستندات راهبری[3]پی دی ۳، در انگلستان منتشر شد. نسخه بازنگری شده این استاندارد در سال ۱۹۹۵ با عنوان استاندارد ایزو ثبت شد. با توجه به تجارب گذشته این گروه در گردآوری اسناد و قوانین و مستندات امنیتی استاندارد امنیتی بی اس ۷۷۹۹ توسط این گروه منتشر گردید و در فوریه ۱۹۹۸ قسمت دوم این استاندارد با عنوان سیستم مدیریت امنیت اطلاعات، منتشر شد. طی سال‌های ۱۹۹۹ تا ۲۰۰۲ بازنگری‌ها و تغییرات زیادی روی این استاندارد صورت گرفته و در سال ۲۰۰۰ با افزودن الحاقیه هایی به استاندارد بی‌اس ۷۷۹۹ که به عنوان یک استاندارد ایزو ثبت شده بود این استاندارد تحت عنوان استاندارد امنیتی ایزو[4]آی ای سی ۱۷۷۹۹به ثبت رسید. استاندارد بی‌اس ۷۷۹۹، حفاظت از اطلاعات را در سه مفهوم خاص یعنی قابل اطمینان بودن اطلاعات[5]؛ صحت اطلاعات[6]؛ در دسترس بودن اطلاعات[7]تعریف می کند. (ونکی ۱۳۹۶ص ۶۴-۶۵)

اهمیت و ضرورت امنیت اطلاعات

امنیت اطلاعات در عصر اطلاعات نه به صورت یک کالا و یا محصول بلکه باید به صورت یک فرآیند نگاه کرد و امنیت را در حد یک محصول خواه نرم‌افزاری و یا سخت‌افزاری تنزل ندهیم. عامل دیگر در اهمیت‌یافتن امنیت اطلاعات، شبکه‌های جهانی و تجارت جهانی است. با اشاعه اینترنت و جهانی‌شدن زندگی روزمره ما دچار تغییرات شده است و سازمان‌های مدرن از اینترنت برای عملیات کسب‌وکار خود استفاده نموده و در نتیجه به آن وابسته شده‌اند. این امر، تجارت الکترونیک را به دنبال داشته است که موجبات تغییر فرآیندهای کسب‌وکار را فراهم نموده است. این وابستگی به کسب‌وکار الکترونیک نیز ضرورت حفاظت از اطلاعات را مطرح نموده و رویکردهای گوناگونی را برای پیاده‌سازی امنیت اطلاعات به وجود آورده است. این رویکرد سعی در جلوگیری از آسیب رساندن به عملیات سازمان دارند و می‌توان بیان کرد که برای تداوم کسب‌وکار، امنیت اطلاعات سازمان اهمیت بسیار یافته است. امروزه حتی با ظهور سازمان‌های مجازی از نظر جغرافیایی، پراکنده و بدون مرز، تبادل اطلاعات اهمیت یافته است و حفظ ایمنی این اطلاعات اهمیتی حیاتی دارد و امنیت اطلاعات لازمه گسترش سازمان‌های مجازی است. در صورت هر گونه رخنه در محمل‌های اطلاعات، تبعات بسیار ناگواری برای سازمان به وجود می‌آورد که از

1- Users Code Of Practice
2- NCC
3- PD003
4- ISO/IEC17799
5- Confidentiality
6- Integrity
7- Availability

[Downloaded from jnraims.ir on 2026-11-20]

آن جمله می‌توان به خسارت‌های مالی، تصمیم‌گیری‌های اشتباه، از دست دادن اعتماد عمومی و ناتوانی در انجام وظایف حیاتی و هزینه‌های اضافی و رخنه در خدمات را ذکر نمود. همچنین از دست دادن داده‌های سازمان می‌تواند منجر به خدشه اعتبار سازمان و در نتیجه خسران کسب‌وکار، مشکلات قانونی، سقوط ارزش سهام و از بین رفتن اعتماد سرمایه‌گذاران کسب اطلاعات رقبا از دانش داخلی از دست دادن مشتریان و در نهایت ایجاد مشکل در استخدام آتی سازمان گردد. در هرحال دغدغه‌های سازمان‌ها بی‌جهت نمی‌باشد، زیرا بسیاری از آن‌ها با حوادث امنیتی مواجهه شده‌اند و ابزارها و سازوکارهای امنیتی، اثربخشی کمتری دارند زیرا امنیت اطلاعات در وهله اول مسئله انسانی و به همان میزان مسئله‌ای سازمانی یا مدیریتی می‌باشد. با توجه به این دیدگاه اهمیت امنیت اطلاعات به زمینه سازمانی برمی‌گردد که در آنجا وجود دارد. دلیل دیگر برای ضرورت تحقیق در زمینه امنیت اطلاعات این مورد است که دانش در زمینه امنیت اطلاعات با معنی و عمیق اما متنوع و گسترده است و نیازمند تحقیقات گسترده برای نحوه استفاده از آن است. دامنه امنیت اطلاعات در عصر رایانه به شدت تغییر کرده است (شیرازی، آل شیخ۱۳۸۸)

استانداردهای حوزه امنیت

منشاء اولین استاندارد در حوزه امنیت یعنی BS7799[1] به زمان تاسیس مرکز امنیت رایانه‌های بازرگانی[2]و شکل‌گیری بخش صنعت و تجارت انگلستان[3]در سال ۱۹۸۷م بر می‌گردد. این مرکز با هدف تعریف معیارهای بین‌المللی برای ارزیابی میزان امنیت تجهیزات تولید شده توسط سازندگان تجهیزات امنیتی تشکیل گردید تا از این طریق تاییده و گواهینامه‌های مربوطه و آموزش لازم را به کاربران ارایه نماید. مرکز انگلیسی CCSC در سال ۱۹۸۹م اقدام با انتشار شناسه‌هایی (کدهایی) با عنوان Code Of Practice Users برای سنجش میزان امنیت نمود. پس از آن اجرایی بودن شناسه‌ها از نگاه کاربران توسط مرکز محاسبات بین‌المللی[4]و کنسرسیومکاربران صنایع انگلستان مورد بررسی قرار گرفت. در سال ۱۹۸۵م این استاندارد یا عنوان BS7799 منتشر شد. قسمت دوم آن نیز در اوایل سال ۱۹۹۸م به آن اضافه گردید، این قسمت مفهوم سیستم مدیریت امنیت اطلاعات(ISMS[5]) را به وجود آورد. نسخه بازنگری شده ی این استاندارد در سال ۱۹۹۵م به عنوان استاندارد پذیرفته شده‌ی سازمان بین‌المللی استانداردؤ تحت عنوان ایزو ۲۷۰۰۱یا همان ISMS به ثبت رسید. در سال ۲۰۰۰ م با افزودن الحاقیه‌هایی به استاندارد BS7799 که به عنوان یک استاندارد ایزو ثبت شده بود، این استاندارد تحت عنوان استاندارد ایزو۱۷۷۹ به ثبت رسید. نسخه جدید و قسمت دوم این استاندارد در سال ۲۰۰۲م بمنظور ایجاد هماهنگی بین این

1- British Standard 7799
2- Commercial Computer Security Center (CCSC)
3- UK Department OF Trade and industry (DTI)
4- National Counting Center (NCC)
5- Information Security Management System (ISMS)
6- International Standard Organization (ISO)

[Downloaded from jnraims.ir on 2026-11-20]

استاندارد مدیریتی و سایر استانداردهای مدیریتی نظیر ایزو ۹۰۰۱ و ایزو ۱۴۰۰۱ تدوین گردید (برودریک، ۲۰۰۶، ۲۶-۳۱). این قسمت برای ارزیابی میزان موثر بودن سیستم ISMS در یک سازمان مدل (PDCA)[1]را همانگونه که در شکل ذیل نشان داده شده است، ارایه می‌نماید به عبارت دیگر با شکل‌گیری نگاه سیستمی به مقوله امنیت اطلاعات تامین امنیت اطلاعات در یک سازمان، به صورت آنی مقدور نبوده و لازم است این امر طی یک فرایند مداوم و در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح انجام گیرد. پس از آن مجموعه استانداردهای خانواده ایزو ۲۷۰۰۰ ازسال ۲۰۰۵م به بعد به صورت مستمر در حوزه‌ی مدیریت امنیت اطلاعات ارایه و منتشر گردید (دشتی، ۵۴:۱۳۸۴).

تعدادی از استانداردهای حوزه امنیت اطلاعات:

خانواده استانداردهای ایزو ۲۷۰۰۰[2]

ایده اساسی سری استانداردهای خانواده ۲۷۰۰۰ تهیه مدلی برای بنا نهادن و اجرای سیستمی مدیریتی است. این مدل همه جنبه‌هایی که خبرگان حوزه‌های مختلف فناوری بنا بر تحقیقات خود بدان رسیده‌اند، را به شکلی هنرمندانه و به عنوان سلسله‌ای از فعالیت‌های مدیریتی بیان کرده است. فعالیت‌های این گروه و گروه‌های همکار ایشان تحت عنوان استانداردهای خانواده مدیریت امنیت اطلاعات در جوامعه قومی مورد پذیرش و بحث قرار گرفته است. این سری از استانداردها کنترل‌هایی برای طراحی و پیاده سازی تا نگهداری و ارتقاء سیستم مدیریت امنیت اطلاعات فراهم می‌سازند. همچنین انعطاف بسیار زیادی برای تغییر مداوم و روبه پیشرفت برای استانداردهای ۲۷۰۰۰ تعبیه شده است به گونه‌ای که در مسیر حیات سازمان و برای ارتقاء سطح امنیت و تداوم کسب و کار متناسب با شرایط محیطی و محتاطی حاکم بر سازمان همواره تغییر و بهینه سازی‌های روبه جلو در همه مستندات به چشم می‌خورد (مدیری ۱۳۹۱: ۶۷).

استاندارد ایزو۱۵۴۴۳[3]

مستندی راهبردی است تا امکان ارائه روش‌های تست یا ارزیابی برای ضمانت محصولات فناوری اطلاعات ایجاد کنند و میزان تطابق محصولات با استانداردهای تهیه شده توسط سازمان ایزو بررسی کنند. هدف این استاندارد ارائه انواع مختلفی از متدهای تضمین است، و تهیه مستندات راهبردی که متخصصان امنیت فناوری اطلاعات در بخش‌های مورد نظر خود بتوانند روش‌های کاملا منطبق بر خواسته خود و برای دستیابی به سطح اطمینان مورد نظر خود که الزامات تضمین امنیت محصول مورد نظر این افراد ایجاب می‌کند را انتخاب کنند.

1- Plan-Do-check-Act
2- ISO/IEC 270002
3- ISO/IEC15443 part 1,2,3 information technology – security techniques-a framework for it security assurance

[Downloaded from jnraims.ir on 2026-11-20]

استاندارد ایزو ۱۵٤۰۸[1]

این استاندارد با توجه به نتایج ارزیابی امنیتی مجوز مقایسه را می‌دهد. برای این منظور مجموعه‌ای از نیازمندی‌ها را برای توابع امنیتی محصولات و سیستم‌های فناوری اطلاعات آماده کرده و استفاده از آنها را با توجه به ارزیابی امنیتی تضمین می‌کند. فرایند ارزیابی سطح محرمانگی، توابع امنیتی محصولات و سیستم‌ها و متریک‌های ضمانت، جهت بکارگیری این نیازمندی‌ها را مشخص می‌کند. این استاندارد می‌تواند به عنوان راهنما در جهت توسعه محصولات و یا سیستم‌های فناوری اطلاعات و نیز برای توسعه محصولات و سیستم‌های تجاری که نیازمند توابع امنیتی هستند مورد استفاده قرار گیرد.

استاندارد ایزو ۱۸۰٤۵[2]

این استاندارد را می‌توان به عنوان امتداد استانداردهای سری ایزو ۱۸۰۴۵ خصوصا بخش سوم این استاندارد با بخش‌های زیادی از استاندارد ذکر شده یکسان است. استاندارد حاضر به عنوان مستند کمکی برای ارزیابی ضوابط امنیت فناوری اطلاعات تعریف شده توسط استاندارد ۱۵۴۰۸ است و حداقل فعالیت‌های لازم که ارزیاب آن می‌بایست انجام دهند تا مطابق استاندارد ۱۵۴۰۸ ارزیابی‌ها انجام شود را بیان می‌کند. (ناصر مدیری۱۳۹۱: ۸۴).

استاندارد ایزو ۱۲۲۰۷[3]

استاندارد ایزو ۱۲۲۰۷ اولین بار در سال ۱۹۹۵ به شکل استاندارد جهانی تهیه شد که مشتمل بر مجموعه از فعالیت‌ها و وظایفی بود که در طول چرخه حیات نرم افزار (منظور نرم افزار مستقل، یا جزئی از یک سیستم بزرگتر) بوده است. در سال ۲۰۰۲ این استاندارد در استاندارد ایزو ۱۵۲۸۸ که فرایندهای چرخه حیات را معرفی می‌کرد ادامه یافت. استاندارد حاضر در سال ۲۰۰۸ به شکل نهایی و ارتقاء یافته با همه مفاهیم شناخته شده در صنعت نرم افزار ارائه گردید است.

استاندارد ایزو ۸-۲۳۸۲[4]

برای پرهیز از ابهام، و کج فهمی‌ها از مفاهیم به کار رفته توسط سازمان‌های مختلف در سراسر جهان، و همچنین برای تسهیل در هماهنگ‌سازی، و یکپارچه‌سازی تدوین اصطلاحات در میان همه کشورها، به شکلی غیرمبهم، غیرپیچیده، با توصیف متناسب هر اصطلاح با کاربرد آن اقدام به تهیه روشی ساختار یافته برای توصیف لغاتی که در گستره وسیع علوم فناوری اطلاعات و سیستم‌های به کار می‌رود، تدوین

1- ISO/IEC15408
2- ISO/IEC 18045
3- ISO/IEC 12207
4- ISO/IEC2382-8

[Downloaded from jnraims.ir on 2026-11-20]

استاندارد ایزو ۲۳۸۲ انجام شده است. این استاندارد شامل ۳۷ بخش عمده است که همه سرفصل‌های علوم را در بر می گیرد و بعنوان یک فرهنگ معارف علمی و مورد تایید جهانی مورد پذیرش صاحبنظران است. استاندارد (لغت نامه مهندسی نرم افزار):

ایزو ۲٤۷٦٥[1]

با پیشرفت روزافزون مهندسی نرم افزار و رشد و بلوغ یافتن آن در جوزه‌های مختلف، امروزه بسیاری از لغات و اصطلاحات جدید به وجود آمده‌اند و یا معناهای و مفهوم‌های جدیدی از لغات قبلی استنباط می‌شود. در این استاندارد همه این لغات و اصطلاحات جدید و قدیم با بازنگری جدید، با هدف هماهنگ‌سازی تعاریف و استاندارد سازی بیان محققین مختلف، تدوین شده است. همه اصطلاحاتی که در همه استانداردهای منتشر شده سازمان PMI, JEEE, ISO در حوزه فناوری اطلاعات، استفاده شده است. در این استاندارد گردآوری شده و محققین به راحتی می‌توانند همه معانی مختلف و مرتبط با اصطلاحات و لغات مهندسی نرم افزار و فناوری اطلاعات را در این استاندارد بیابند.

مدیریت امنیت اطلاعات در سازمان‌ها

در جهان امروز تکنولوژی اطلاعات امکان سودمندی و کارآمدی اطلاعات را ممکن ساخته است. بکارگیری تکنولوژی اطلاعات، تحول گسترده‌ای را در امور اداری و سیستم‌های اطلاعاتی باعث شده است، به طوریکه امکان انتقال الکترونیکی داده‌ها، مدارک، اسناد و مکاتبات مختلف از طریق کامپیوتر و خطوط ارتباطات مخابراتی فراهم‌شده است. مطالعات و تحقیقات نشان می‌دهد که بین سرمایه‌گذاری در فناوری اطلاعات و بازده موسسات و بهره‌وری نیروی انسانی ارتباط دو سویه مثبتی وجود دارد. همچنین تکنولوژی اطلاعات توانایی سازمان‌ها را افزایش می‌دهد و این در نتیجه افزایش تنوع محصولات و بهبود کیفیت و جلب رضایت مشتری است و نیز سبب تسهیل روند اداری و افزایش بازده نیروی انسانی و مدیریت می‌شود. یکی از نتایج عمده تکنولوژی اطلاعات تمرکز زدایی در عین تمرکزگرایی است. بدین معنی که می‌توان کارها را از راه دور انجام داد بدون آنکه لازم باشد تا در محل حضور فیزیکی و مستمر داشته باشیم که این ویژگی بر کوتاه شدن فواصل زمانی و مکانی به عنوان یک ابر شاهراه تاکید دارد. امروزه تکنولوژی اطلاعات دیگر سیستم‌های اطلاعاتی مدیریت از جمله CIS ، MIS، DSS AI، EIS، OA و ... را در اختیار گرفته و بدین ترتیب قطب اطلاعاتی مستقر در مرکز را قادر می‌سازد تا به افزایش کنترل خود بر مناطق و انجام عملیات تمرکزی اقدام نماید. بنابراین امکان افزایش سرعت و کیفیت تصمیم‌گیری و مدیریت را فراهم می‌نماید. تکنولوژی اطلاعات به عنوان یکی از مهمترین ابزار جهت مشارکت در بازار جهانی است. از ویژگیهای اساسی عصر حاضر، اطلاعات و تبدیل آن به دانش است.

1- ISO/IEC 24765

[Downloaded from jnraims.ir on 2026-11-20]

چنین ویژگی تاثیر زیادی روی نهادهای اجتماعی و اقتصادی جوامع خواهد گذاشت. نهادهای اجتماعی باید براساس آن تجدید بنا و تغییر ساختار دهند. پیشرفت‌های مذکور جنبهٔ خطرناکی نیز دارد که پیدایش انواع تخلفات و جرایم و همچنین بهره‌برداری از فنآوری جدید در ارتکاب اعمال غیرقانونی و نامشروع، بخشی از آن به شمار می رود که با مدیریت امنیت اطلاعات می توان تا حدودی آن را کنترل کرد. (ترابی ۱۳۹۵)

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را بر عهده دارد. همچنین مدیریت امنیت وظیفه پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته و در نهایت باید تلاش کند تا سیستم را همیشه روزآمد نگه دارد. هدف مدیریت امنیت اطلاعات در یک سازمان، حفظ سرمایه‌های نرم افزاری، سخت افزاری، اطلاعاتی و ارتباطی و نیروی انسانی سازمان در مقابل هر گونه تهدید است (دشتی، ۱۳۸۴: ۱۵۹). بورک[1] معتقد است برای رسیدن به این هدف نیاز به یک برنامه منسجم دارد. سیستم امنیت اطلاعات راهکاری برای رسیدن به این هدف می باشد. با توجه به گسترش استفاده از اینترنت، تبادلات اطلاعاتی و هزینه‌های صرف شده به منظور یکپارچگی اطلاعاتی، امروزه مبحث کنترل و مدیریت جابه‌جایی‌های اطلاعاتی و برخورداری از سامانهٔ جامعی برای مدیریت امنیت اطلاعات، بیش از پیش احساس می‌شود. امنیت اطلاعات مبحث بسیار مهمی است؛ زیرا هدف آن حفاظت کاربر در برابر تهدیدها و ریسک ها و دسترسی به اطلاعات امن، مطمئن و محرمانه است و برای اطمینان از امنیت آن، سازمان باید سیاست‌ها و خط‌مشی‌های امنیت اطلاعات را شناسایی و تبیین کند. با این حال، گاهی سازمان‌ها برای پیاده سازی سیاست‌های امنیت اطلاعات با شکست مواجه می‌شوند.

از آنجا که امنیت اطلاعات شالوده‌ی هر نوع سیستمی می‌باشد و با حضور امنیت در سیستم ها خارج از نوع و هدف، می‌تواند برای مسئولان و مدیران آن سازمان اطمینان خاطر در برابر انواع آسیب ها، تهدیدات، ریسک ها را بدنبال داشته باشد، و از طرفی، پیشرفت‌های شگرفی در فناوری رایانه حاصل شده است، در زمینه آگاهی استفاده‌کنندگان از آسیب‌پذیری داده‌ها و اطلاعات و نیز مخاطرات مربوط به تغییرات غیرمجاز، افشا و تخریب عمدی یا سهوی اطلاعات اقدام چندانی صورت نگرفته است. به‌طور معمول مسئله امنیت تا قبل از مرحله تعریف نیازمندی‌های عملیاتی، به طور جدی مدّنظر قرار نمی‌گیرد و نظام به طور مستقیم وارد مرحله پیاده‌سازی می‌شود. بدین ترتیب، دستیابی به یک سطح مناسب امنیتی برای سیستم در حال اجرا به ندرت امکان‌پذیر است. حتی در صورت عملی شدن چنین امنیتی، هزینه‌های ناشی از این امر در مقایسه با نظام‌هایی که از ابتدای طراحی، ملاحظات امنیتی را در نظر گرفته‌اند بسیار بالاتر خواهد بود. ذخیره‌سازی اطلاعات به صورت الکترونیکی، کاربرد وسیع رایانه‌ها در فعالیت‌های حرفه‌ای گوناگون را ناگزیر ساخته و استفاده از شبکه‌های رایانه‌ای و بویژه اینترنت، تغییرات اساسی در روند ارائه خدمات به

1- F. Bjorck.

[Downloaded from jnraims.ir on 2026-11-20]

وجود آورده است. این امکانات سبب شده حجم بسیار زیادی از اطلاعات تنها به اندازهٔ یک سرانگشت با کاربران فاصله داشته باشد. ناگفته پیداست، در این محیط پیچیده با این ارتباطات وسیع، مخاطرات گسترده‌ای سیستم‌های رایانه‌ای، سامانه‌های اطلاعاتی و فعالیت‌ها و زیرساخت‌های حیاتی وابسته به آنها را تهدید می‌کند (سادوسکای[1] ودیگران، ۱۳۸۴: ۹). این تهدید شامل دستکاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی هستند در چنین شرایطی، چنانچه عواملی که می‌توانند از مزایای سیستمها به شمار بروند اگر تحت کنترل نباشند، باعث بروز آسیب‌پذیری شده، سوء استفادهٔ افراد بد نیت از آنها به نفوذ و خرابکاری، کلاهبرداری بینجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‌ای رخ می‌دهد، درصورت نبود روش‌های صحیح برای حفاظت از اطلاعات، می‌تواند نتایج مخربی را به بار آورد. چنان که (کریدا[2] و دیگران، ۲۰۰۵) تأکید می‌کنند، حفاظت سیستم‌های اطلاعاتی از حملات امنیتی، یک چالش مستمر است که بسیاری از سازمانها با آن مواجه‌اند.

تدوین و اجرای تدابیر امنیتی در قبال این تهدیدهای گسترده، ضرورتی اجتناب ناپذیر برای سازمانهاست. اتخاذ تدابیر مناسب می‌تواند احتمال وقوع مخاطرات را به حداقل برساند و یا در صورت وقوع آنها، میزان خسارتهای وارده را در حد بسیار ناچیزی نگه دارد. این‌گونه تدابیر امنیتی، موجب افزایش قابلیت واکنش سریع و مؤثر می‌شود و به این ترتیب سازمان‌ها قادر خواهند بود برای ترمیم خسارت‌ها از فرایندهای از پیش تعیین‌شده استفاده کنند و بهره‌وری و ایمنی اطلاعات، افزایش یافته، کسب‌وکار به صورت مطمئن‌تری تداوم یابد (سادوسکای و دیگران، ۱۳۸۴: ۹).

از سوی دیگر امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود می باشیم. کافی است به اطراف خود نگاهی داشته باشیم تا به صحت گفته فوق بیشتر واقف شویم. همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه های کامپیوتری و به دنبال آن اینترنت، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است. استفاده‌کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فنآوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه‌های تاثیرگذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می‌باشند (فیلون[3] ۲۰۰۰).

امنیت اطلاعات و ایمن سازی شبکه‌های کامپیوتری از جمله این مولفه‌ها بوده که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران صرف‌نظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن سازی شبکه‌های کامپیوتری بوده و می بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد. وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران صرفنظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود

1- Sadowsky
2- Karyda.
3- G. Dhillon

[Downloaded from jnraims.ir on 2026-11-20]

دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملا" زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد (دینس[1] ۲۰۰۵).

سیستم امنیت اطلاعات

یکی از وظایف مدیریت امنیت اطلاعات بررسی و ایجاد یک سیستم امنیت اطلاعات است که متناسب با اهداف سازمان باشد. برای طراحی این سیستم باید عوامل مختلفی را در نظر گرفت. محاسبه ارزش اطلاعات از نظر اقتصادی، بررسی خطرات و محاسبه خسارتهای احتمالی و تخمین هزینه- سودمندی استفاده از سیستم امنیت اطلاعات، بررسی تهدیدات احتمالی و بررسی راهکارهای مختلف و انتخاب سودمندترین روش برای طراحی سیستم‌های امنیت اطلاعات ضروری بنظر می‌رسد. (پیپکین ۲۰۰۰)

مجموعه مراحلی که در طراحی یک سیستم امنیت اطلاعات در نظر گرفته می‌شود به شرح زیر می‌باشد:

آشنایی با منابع اطلاعاتی موجود در سازمان: مجموعه منابعی که یک سازمان در اختیار دارد شامل افرادی که در سازمان شاغل هستند، امکانات و سرمایه‌های مادی، اطلاعاتی و که حوضه‌های کاری را مشخص می‌کند و سازمان را از سایر سازمان‌ها جدا می‌کند، ساختارها یک سازمان مثل نیروی برق، ارتباطات و تبادلات اطلاعاتی و غیره ... می‌باشد. بعلاوه طراح سیستم باید با مجموعه الگوریتم‌ها و نرم‌افزارهای سیستم اطلاعاتی سازمان، امکانات موجود در سازمان و فرایند تولید و بازیابی اطلاعات و کاربران این اطلاعات آشنایی کامل داشته باشد. آشنایی با منابع مربوط به حوضه اطلاعات یک سازمان موجب درک وضعیت و میزان نیاز به امنیت و چگونگی اعمال راهکارهای امنیتی مناسب با آنها خواهد شد.

ارزیابی ارزش اطلاعات: قیمت گذاری اطلاعات به دو شکل قابل تخمین(محسوس) و غیر قابل تخمین (غیرمحسوس) قابل محاسبه است. اطلاعات موجود در سازمان مورد ارزیابی قرار گرفته و هزینه تولید آن به هر دو شکل باید محاسبه شود. علاوه بر این ضروری است ارزش هزینه تولید و هزینه تولید دوباره اطلاعات در صورت تهدید امنیتی و از بین رفتن اطلاعات محاسبه شود هزینه بازتولید اطلاعات شامل نیروی انسانی، ماشین، تجهیزات و زمانی است که صرف جمع‌آوری و ورود و هماهنگی اطلاعات خواهد و همچنین مقایسه آن با هزینه ایجاد امکانات حفظ اطلاعات مثل تهیه پشتیبان مناسب و بارگزاری به موقع اطلاعات و همچنین هزینه نرسیدن به موقع اطلاعات در هر یک از این مدل ها موجب می شود مدیریت امنیت اطلاعات سیستمی متناسب با ارزش اطلاعات سازمان طراحی کند. (پیپکین ۲۰۰۰)

1- S. Dynes

[Downloaded from jnraims.ir on 2026-11-20]

هزینه فاش شدن اطلاعات: مورد دیگری که باید بدقت مورد بررسی قرار گیرد هزینه فاش سازی اطلاعات است اینکه چه اطلاعاتی با فاش شدن صدمات بیشتری به سرمایه‌های سازمان وارد خواهد کرد و به این ترتیب تعیین سطوح مختلف ارزش اطلاعاتی و سازماندهی و طبقه‌بندی اطلاعاتی و هزینه افشاسازی هر یک از سطوح اطلاعاتی مسئله‌ای است که نباید در طراحی سیستم‌های اطلاعاتی مورد غفلت قرار گیرد. (پیپکین ۲۰۰۰)

تهدیدات سیستم اطلاعاتی: مجموعه تهدیداتی که متوجه سیستم اطلاعاتی می‌باشد به دو صورت کلی می‌باشد برخی به صورت عمدی ایست مثل کلاهبرداری های اینترنتی، حملات ویروس‌ها و هکرها، و یا به صورت غیرعمدی صورت می‌گیرد مثل اشتباهات انسانی، مشکل سخت‌افزاری و نرم‌افزاری و بلایای طبیعی.

تهدید کننده‌های امنیت اطلاعات

ویروس‌ها

ویروس‌های کامپیوتری، متداولترین نوع تهدیدات امنیتی در سالیان اخیر بوده که تاکنون مشکلات گسترده‌ای را ایجاد و همواره از خبرسازترین موضوعات در زمینه کامپیوتر و شبکه‌های کامپیوتری، بوده‌اند. ویروس‌ها، برنامه‌های کامپیوتری می‌باشند که توسط برنامه‌نویسان گمراه و در عین حال ماهر نوشته شده و بگونه‌ای طراحی می‌گردند که قادر به تکثیر خود و آلودگی کامپیوترها بر اثر وقوع یک رویداد خاص، باشند (گارود[1] ۲۰۰۷). مثلا "ویروس‌هایی که از آنان با نام ماکرو ویروس یاد می‌شود، خود را به فایل‌هائی شامل دستورالعمل‌های ماکرو ملحق نموده و در ادامه، همزمان با فعال شدن ماکرو، شرایط لازم به منظور اجرای آنان نیز فراهم می‌گردد. برخی از ویروس‌ها بی‌آزار بوده و صرفا" باعث بروز اختلالات موقت در روند انجام عملیات در کامپیوتر می‌شوند (نظیر نمایش یک پیام مضحک بر روی صفحه نمایشگر همزمان با فشردن یک کلید خاص توسط کاربر). برخی دیگر از ویروس‌ها دارای عملکردی مخرب‌تر بوده و می‌توانند مسائل و مشکلات بیشتری نظیر حذف فایل‌ها و یا کاهش سرعت سیستم را به دنبال داشته باشند. یک کامپیوتر صرفا "زمانی آلوده به یک ویروس می‌گردد که شرایط و امکان ورود ویروس از یک منبع خارجی (اغلب از طریق فایل ضمیمه یک نامه الکترونیکی و یا دریافت و نصب یک فایل و یا برنامه آلوده از اینترنت)، برای آن فراهم گردد. زمانی که یک کامپیوتر در شبکه‌ای آلوده گردید، سایر کامپیوترهای موجود در شبکه و یا سایر کامپیوترهای موجود در اینترنت، دارای استعدادی مناسب به منظور مشارکت و همکاری با ویروس، خواهند بود (گینن[3] ۲۰۰۰).

1- R. Garud, C. Hardy, S. 2007
2- Macro virus
3- D. Gefen, D. Straub, M. Boudreau.

[Downloaded from jnraims.ir on 2026-11-20]

برنامه‌های اسب تروا

برنامه‌های اسب تروا [1] به منزله ابزارهای برای توزیع کدهای مخرب می‌باشند. تروجان‌ها، می‌توانند بی‌آزار بوده و یا حتی نرم‌افزاری مفیدی نظیر بازی‌های کامپیوتری باشند که با تغییر قیافه و با لباسی مبدل و ظاهری مفید خود را عرضه می نمایند. تروجان ها، قادر به انجام عملیات متفاوتی نظیر حذف فایل‌ها، ارسال یک نسخه از خود به لیست آدرس‌های پست الکترونیکی، می‌باشند. این نوع از برنامه ها صرفا" می‌توانند از طریق تکثیر برنامه‌های اسب تروا به یک کامپیوتر، دریافت فایل از طریق اینترنت و یا باز نمودن یک فایل ضمیمه همراه یک نامه الکترونیکی، اقدام به آلودگی یک سیستم نمایند (گرنت[2]، ۲۰۰۵).

ویرانگران[3]

در وب سایت‌های متعددی از نرم افزارهائی نظیر اکتیوایکس[4]ها و یا اپلت‌های جاوا استفاده می گردد. این نوع برنامه‌ها به منظور ایجاد انیمیشن و سایر افکت‌های خاص مورد استفاده قرار گرفته و جذابیت و میزان تعامل با کاربر را افزایش می‌دهند. با توجه به دریافت و نصب آسان این نوع از برنامه‌ها توسط کاربران، برنامه‌های فوق به ابزاری مطئمن و آسان به منظور آسیب‌رسانی به سایر سیستم‌ها تبدیل شده‌اند. این نوع برنامه‌ها که به "ویرانگران" شهرت یافته‌اند، به شکل یک برنامه نرم‌افزاری و یا اپلت ارائه و در دسترس استفاده‌کنندگان قرار می‌گیرند. برنامه‌های فوق، قادر به ایجاد مشکلات متعددی برای کاربران می‌باشند (از بروز اشکال در یک فایل تا ایجاد اشکال در بخش اصلی یک سیستم کامپیوتری) (گرین وی[5]، ۲۰۰۵).

رهگیری داده [6](استراق سمع)

بر روی هر شبکه کامپیوتری روزانه اطلاعات متفاوتی جابجا می‌گردد و همین امر می‌تواند موضوعی مورد علاقه برای مهاجمان باشد. در این نوع حملات، مهاجمان اقدام به استراق سمع و یا حتی تغییر بسته‌های اطلاعاتی در شبکه می‌نمایند. مهاجمان به منظور نیل به اهداف مخرب خود از روش‌های متعددی به منظور شنود اطلاعات، استفاده می‌نمایند (جارویس[7]، ۲۰۰۳).

کلاهبرداری (ابتدا جلب اعتماد و سپس تهاجم)

کلاهبرداران از روش‌های متعددی به منظور اعمال شیادی خود استفاده می‌نمایند. با گسترش اینترنت این نوع افراد فضای مناسبی برای اعمال مخرب خود یافته‌اند. در برخی موارد شیادان با ارسال نامه‌های

1- Trojans
2- R. M. Grant
3- Wreckers
4- ActiveX
5- K. E. Greenaway, Y. E. 2005
6- Eavesdrop
7- C. B. Jarvis, S. B. MacKenzie, P. M. 2003

[Downloaded from jnraims.ir on 2026-11-20]

الکترونیکی وسوسه انگیز از خوانندگان می‌خواهند که اطلاعاتی خاص را برای آنان ارسال نموده و یا از یک سایت به عنوان طعمه در این رابطه استفاده می‌نمایند. به منظور پیشگیری از اینگونه اعمال، می بایست کاربران دقت لازم در خصوص درج نام، رمز عبور و سایر اطلاعات شخصی در سایت‌هائی که نسبت به هویت آنان شک و تردید وجود دارد را داشته باشند. با توجه به سهولت جعل آدرس‌های پست الکترونیکی؛ می‌بایست به این نکته توجه گردد که قبل از ارسال اطلاعات شخصی برای هر فرد، هویت وی شناسائی گردد. هرگز بر روی لینک‌ها و یا ضمائمی که از طریق یک نامه الکترونیکی برای شما ارسال شده است، کلیک نکرده و همواره می ایست به شرکت‌ها و موسساتی که به طور شفاف آدرس فیزیکی و شماره تلفن‌های خود را ذکر نمی نمایند، شک و تردید داشت (هاومن، ۱۹۹۳).

نامه‌های الکترونیکی ناخواسته

از واژه اسپم[1] در ارتباط با نامه‌های الکترونیکی ناخواسته و یا پیام‌های تبلیغاتی ناخواسته، استفاده می‌گردد. این نوع از نامه‌های الکترونیکی، عموما" بی‌ضرر بوده و صرفا" ممکن است مزاحمت و یا دردسر ما را بیشتر نمایند. دامنه این نوع مزاحمت‌ها می‌تواند از به هدر رفتن زمان کاربر تا هرز رفتن فضای ذخیره سازی بر روی کامپیوترهای کاربران را شامل می‌شود (پورمند، ۱۳۹۰).

ایمن‌سازی کامپیوترها

تمامی کامپیوترها از کامپیوترهای موجود در منازل تا کامپیوترهای موجود در سازمان‌ها و موسسات بزرگ، در معرض آسیب و تهدیدات امنیتی می‌باشند. با انجام تدابیر لازم و استفاده از برخی روش‌های ساده می‌توان پیشگیری لازم و اولیه‌ای را در خصوص ایمن‌سازی محیط کامپیوتری خود انجام داد. علیرغم تمامی مزایا و دستاوردهای اینترنت، این شبکه عظیم به همراه فنآوری‌های مربوطه، دریچه‌ای را در مقابل تعداد زیادی از تهدیدات امنیتی برای تمامی استفاده‌کنندگان (افراد، خانواده‌ها، سازمان‌ها، موسسات و. ..)، گشوده است (فیلون، ۲۰۰۹). با توجه به ماهیت حملات، می بایست در انتظار نتایج نامطلوب متفاوتی بود. در معرض آسیب قرارگرفتن داده‌ها و اطلاعات حساس، تجاوز به حریم خصوصی کاربران، استفاده از کامپیوتر کاربران برای تهاجم بر علیه سایر کامپیوترها، از جمله اهداف مهاجمانی است که با بهره‌گیری از آخرین فنآوری‌های موجود، حملات خود را سازماندهی و بالفعل می‌نمایند. بنابراین، می‌بایست به موضوع امنیت اطلاعات، ایمن‌سازی کامپیوترها و شبکه‌های کامپیوتری، توجه جدی شده و از فرآیندهای متفاوتی در جهت مقاوم سازی آنان، استفاده گردد (دیماگو[2] ۱۹۸۳).

1- Spam
2- P. J. DiMaggio, W. W. Powell. 1983

[Downloaded from jnraims.ir on 2026-11-20]

خطرهای تهدیدکننده امنیت اطلاعات، به دو دسته عمدی و غیرعمدی تقسیم می‌شود، خطرهای عمدی خطرهایی هستند که امنیت اطلاعات سیستم را با برنامه قبلی و هدفی خاص مورد حمله قرار می‌دهند، مثل خطر هکرها و خطرهای غیرعمدی، خطرهایی هستند که بر اثر اشتباهات انسان و نیروی کار به سیستم وارد می‌شود که این نوع خطر، بیشترین میزان خسارات را به سیستم اطلاعاتی وارد می‌کند، همچنین خطرهای ناشی از عوامل طبیعی مثل سیل، زلزله، طوفان و. . . جزء تهدیدات غیرعمدی به حساب می‌آید. برای اینکه در سیستم‌ها بتوانیم خطرهای موجود را رفع کنیم، قبل از هر چیز باید به فکر ایجاد امنیت شبکه‌های اطلاعاتی خود باشیم. این ایجاد امنیت، ابتدا باید شامل اتخاذ سیاست‌های امنیتی باشد. (دشتی، ۱۳۸۴)

پس از آشنائی با تهدیدات، می‌توان تمهیدات امنیتی لازم در خصوص پیشگیری و مقابله با آنان را انجام داد. بدین منظور می‌توان از فنآوری‌های متعددی نظیر آنتی ویروس‌ها و یا فایروال‌ها، استفاده بعمل آورد (پورمند، ۱۳۹۰).

نرم‌افزارهای آنتی ویروس[1]، نرم افزارهای آنتی ویروس قادر به شناسائی و برخورد مناسب با اکثر تهدیدات مربوط به ویروس‌ها می‌باشند نرم‌افزارهای آنتی ویروس در تعامل اطلاعاتی با شبکه‌ای گسترده از کاربران بوده و در صورت ضرورت پیام‌ها و هشدارهای لازم در خصوص ویروس‌های جدید را اعلام می‌نمایند. بدین ترتیب، پس از شناسائی یک ویروس جدید، ابزار مقابله با آن سریعا" پیاده‌سازی و در اختیار عموم کاربران قرار می‌گیرد. با توجه به طراحی و پیاده سازی ویروس‌های متعدد در سراسر جهان و گسترش سریع آنان از طریق اینترنت، می‌بایست بانک اطلاعاتی ویروس‌ها براساس فرآیندی مشخص و مستمر، بهنگام گردد (کینگ[2]، ۲۰۱۰). برای اینکه بتوانیم اطلاعات خود را ایمن کنیم نیاز به یک سری حفاظت‌ها[3]است که بایستی برای هر سطح از امنیت در نظر گرفته شود تا به هدف اصلی که CIA می‌باشد نزدیک شویم. اولین نکته حفاظتی برای اطلاعات احراز هویت[4]است. احراز هویت یعنی اینکه آیا شخص یا کاربر مورد نظر همان فردی است که ادعا می کند یا ادعای وب تقلبی است؟ در ساده‌ترین حالت ممکن شما در وب سایت itpro. ir هر شخص دارای یک نام کاربری و رمز عبور می‌باشد، این نام کاربری و رمز عبور وسیله احراز هویت شما در وب سایت انجمن می باشد، سیستم و سرویس‌هایی که در شبکه کار می‌کنند با استفاده از این نام کاربری و رمز عبور شما را شناسایی و احراز هویت می‌کنند. دومین نکته حفاظتی سطح اختیارات[5]است. سطح اختیارات بعد از عملیات احراز هویت اعلام می‌شود و به کاربر ما می‌گوید که حق انجام چه کاری را دارد. همه کاربران در وب سایت انجمن تخصصی فناوری اطلاعات ایران یاitpro. ir دارای نام کاربری و رمز عبور هستند اما فقط عده معدودی دارای دسترسی‌های مدیریتی هستند. سومین

1- Antivirus
2- B. G. King, T. Felin, D. A. Whetten. 2010
3- Protection
4- Authentication
5- Authorization

[Downloaded from jnraims.ir on 2026-11-20]

نکته حفاظتی حسابرسی[1] می‌باشد. کاربران چه فعالیت‌هایی در وب سایت انجام می‌دهند، بیشتر از چه منابعی استفاده می‌کنند و در هنگام بروز خطا در وب سایت در کجا بوده‌اند، این اطلاعات می‌تواند در بهبود سرویس‌دهی و همچنین جلوگیری از بوجود آمدن اختلال در وب سایت itpro. ir به مدیران وب سایت کمک کند (ماتا[2] ۱۹۹۵).

عوامل مهم در استقرار اثربخشی سیستم مدیریت امنیت اطلاعات

به منظور استقرار اثربخش سیستم مدیریت امنیت اطلاعات در سازمان بایست عوامل زیر را در نظر گرفت:

۱- تعهد مدیران به سازمان: درگیر شدن مستقیم مدیران ارشد در فرآیند استقرار سیستم مدیریت امنیت اطلاعات، کمک خواهد نمود که الزامات استاندارد در حوزه مدیریت منابع سیستم مدیریت امنیت اطلاعات برآورده شود.

۲- وجود یک متولی خاص بر ISMS : سیستم باید با هماهنگی واحدهای مختلف در سازمان شکل گیرد. اما واحد متولی اصلی می بایست مقبولیت عام داشته باشد.

۳- تعریف مناسب قلمروی پروژه ISMS در سازمان: اندازه قلمرو **(Scope)** پروژهISMS ، شفاف نمودن قلمرو فیزیکی پروژهISMS ، شفاف نمودن قلمرو فرایندی پروژهISMS ، شفاف نمودن قلمرو تکنولوژیکی پروژهISMS ، بلوغ واحدهای موجود در قلمروISMS تعریف مناسب قلمرو به ویژه در حوزه فناوری اطلاعات از اهمیت بالایی برخوردار است.

٤- پیاده‌سازی صحیح و کامل سیاست‌های امنیتی: تایید به موقع سیاست‌های امنیتی توسط مدیریت، نشر و اطلاع رسانی به موقع و مناسب سیاست‌های امنیتی بین پرسنل مشمول، اجرایی شدن سیاست‌های امنیتی تدوین شده در پایان پروژهISMS ، نظارت کار گروه ممیزی امنیت اطلاعات بر اجرای سیاست‌ها، تغییر به روز سیاست‌های امنیتی با تغییر تجهیزات پردازشی یا فرایندهای سازمان، آموزش سیاست‌های امنیتی به پرسنل مشمول و پرسنل جدیدالاستخدام

۵- تعامل با رویه‌های مدیریت خدمات فناوری اطلاعات (ITSM)**:** وجود و پیاده‌سازی مناسب فرایند مدیریت پیکره بندی در سازمان، وجود و پیاده‌سازی مناسب فرایند مدیریت تغییر در سازمان، وجود و پیاده‌سازی مناسب فرایند مدیریت بحران در سازمان، وجود و پیاده‌سازی مناسب فرایند مدیریت مشکل در سازمان، وجود و پیاده‌سازی مناسب فرایند مدیریت ترخیص در سازمان، وجود و پیاده‌سازی مناسب فرایند مدیریت درخواست سرویس در سازمان استقرار هم زمان سیستم مدیریت امنیت اطلاعات و سیستم مدیریت خدمات فناوری اطلاعات، سبب خواهد شد مجموعه فرآیندهای مشترک نظیر مدیریت حوادث

1- Accounting
2- F. J. Mata, W. L. Fuerst, J. B.

[Downloaded from jnraims.ir on 2026-11-20]

امنیت اطلاعات، مدیریت تغییرات، مدیریت مشکلات و ... با استفاده از بستر فناوری اطلاعات به شیوه‌ای اثربخش صورت پذیرد.

٦- بلوغ IT در سازمان: وجود یک مرکز داده مناسب و استاندارد در سازمان، ساختار یافته بودن شبکه سازمان، ساختار Active Directory سازمان، سیستم و سیاست پشتیبان‌گیری مناسب سازمان، و وجود سایت پشتیبان مناسب بدیهی است استقرار فنی مناسب بسیاری از کنترل‌ها، به بلوغ فناوری اطلاعات سازمان برمی گردد.

۷- رعایت ملاحظات مربوط به نیروی انسانی: فرهنگ‌سازی امنیت در سازمان، قرار دادن نکات امنیتی در تعاریف شغلی پرسنل، برگزاری دوره‌های آموزشی امنیتی برای پرسنل، رعایت ملاحظات امنیتی در ورود و خروج پرسنل از سازمان

۸- ممیزی دوره‌ای: مشخص بودن بازه‌های زمانی ممیزی داخلی، ممیزی دوره‌ای در بازه‌های زمانی مشخص، تغییر ممیزان در دوره‌های مختلف، برگزاری ممیزی خارجی در بازه‌های زمانی مشخص کنترل استقرار اثربخش سیستم مدیریت امنیت اطلاعات جز با ممیزی دوره‌ای امنیتی و ممیزی داخلی امکان‌پذیر نیست.

۹- پیاده‌سازی به موقع و مناسب طرح‌ها و مناقصات در پایان فاز طراحی: اعطای بودجه لازم برای برگزاری مناقصات و اجرای طرح‌ها، عدم تغییر مدیریت در بازه زمانی قبل از شروع پروژه تا زمان اجرا و برگزاری مناقصات، اجرای طرح‌ها طبق فازبندی و ترتیب مشخص شده در خروجی پروژهISMS ، عدم تأخیر در اجرای طرح‌ها و مناقصات خروجی پروژهISMS ، و استفاده از شرکت یا تیم طراح ISMS، به عنوان ناظر یا پیاده‌سازی طرح‌ها

۱۰- ارتباط با سازمان‌ها و نهادهای امنیتی: ارتباط با نهادهای ذیصلاح امنیتی، ارتباط با مجامع امنیتی متخصص و مؤسسات حرفه ای، رعایت ملاحظات امنیتی سازمان‌های بالاتر در تدوین سیاست‌های امنیتی، دریافت جدیدترین ابزارها و نرم افزارهای امنیتی از سایت‌های شرکت های مرتبط ارتباط با مراکز امنیتی

۱۱- امنیت شخص ثالث: رعایت نکات امنیتی در تفاهم نامه عدم افشا با پیمانکاران، مشاوران و سایر اشخاص ثالث؛ کنترل دسترسی اشخاص ثالث، بررسی عملکرد اشخاص ثالث از ابعاد امنیتی، درگیر نمودن پیمانکاران سازمان در پروژه ISMS

۱۲- مدیریت صحیح ریسک باقی‌مانده: کیفیت چهارچوب ارزیابی ریسک، ارزیابی ریسک دقیق، وجود معیاری مشخص برای تعیین سطح ریسک مورد پذیرش، پذیرش ریسک‌های باقی‌مانده از سوی مدیریت، انتقال مناسب ریسک‌هایی که باید انتقال داده شوند به سازمان‌های پیمانکار یا بیمه

۱۳- طراحی سیستم مواجهه با بحران مناسب: آموزش رویه‌های مواجهه با بحران به مدیران و کارکنان، آموزش رویه‌های مواجهه با بحران به پیمانکاران، مشاوران و اشخاص ثالث، پیاده‌سازی یک

[Downloaded from jnraims.ir on 2026-11-20]

سیستم Service Desk مناسب، کیفیت پایگاه اطلاعاتی تجربیات حاصل از بحران‌ها بسیاری از بحران‌های امنیتی چندین و چند بار در یک سازمان رخ می‌دهد. ولی درس‌های لازم از آن گرفته نمی‌شود. وجود یک سیستم Service Desk مناسب و پیگیری مناسب وقایع امنیتی، کمک خواهد نمود که هم میزان در دسترس نبودن سامانه‌ها کاهش یافته و هم پایگاه داده مناسبی به منظور بررسی وقایع و یادگیری از آنها شکل می گیرد. (خوانی، ۱۳۸۸)

وضعیت امنیت اطلاعات در ایران

در بعد داخلی، می‌توان گفت که تا قبل از سال ۱۳۸۰ تقریباً کاری جدی که در ارتباط با ارائه راهبرد، برنامه‌ریزی یا طرح‌ریزی منطقی در زمینه استقرار فضای سایبری و امنیت اطلاعات و یا حتی توسعه فناوری اطلاعات بوده باشد، وجود نداشته است. در سال ۱۳۸۰ فهرستی از خط‌مشی‌های کلان در رابطه با چگونگی توسعه و بهره‌برداری از شبکه‌های اطلاع‌رسانی رایانه‌ای توسط رهبری به دست اندرکاران در این زمینه ابلاغ گردید. در سال ۱۳۸۱ طرح توسعه و کاربری فناوری اطلاعات و ارتباطات کشور (تکفا) به عنوان اولین طرح در سطح ملی ارائه گردید. تجربه عمده‌ای که در ارتباط با فضای سایبری در کشور ما مورد استفاده قرار می گیرد، عمدتاً برگرفته از کشورهای فنلاند و ایالات متحده آمریکا است. سند راهبردی کشور فنلاند در سال ۲۰۰۲ و کشور آمریکا در سال ۲۰۰۳ به تصویب رسیده است. (شورای عالی اطلاعات رسانی دولت، ۱۳۸۲). یکی از الزامات اصلی در استفاده از فضای سایبری، داشتن پهنای باند بالا در شبکه‌های ملی و بین‌المللی است و این درحالی است که پهنای باند متوسط استفاده شده در کشور ما بسیار پایین‌تر از سایر کشورهاست که باعث عدم ارائه سرویس‌های لازم بر روی این فضا می‌شود.

نتیجه گیری

استقرار سیستم مدیریت امنیت اطلاعات بعنوان سامانه‌ای جامع که همه ابعاد امنیت از جمله خط مشی امنیتی، سازماندهی امنیت اطلاعات، مدیریت دارایی‌ها، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی، استفاده، توسعه و نگهداری سامانه‌های اطلاعاتی، پشتیبانی حوادث، مدیریت تداوم کسب و کار، سازگاری با الزامات قانونی، حقوقی و قراردادی را در برگیرد، در سازمان‌ها امری ضروری است. اعمال چنین سیستمی برا ی هر سازمان لازم بوده و بسته به سطح اطلاعات و ارزش اطلاعات سازمان گستردگی متنوعی خواهد داشت. در کل لازم است سازمان‌ها سه شرط زیر را در طراحی سیستم امنیت اطلاعاتی خود مد نظر داشته باشند:

۱. سلامت اطلاعات: اطمینان از سلامت اطلاعات چه در زمان ذخیره و چه به هنگام بازیابی و ایجاد امکان برای افرادی که مجاز به استفاده از اطلاعات هستند.

[Downloaded from jnraims.ir on 2026-11-20]

۲. دقت: اطلاعات چه از نظر منبع ارسالی و چه در هنگام ارسال و بازخوانی آن باید از دقت و صحت برخوردار باشد و ایجاد امکاناتی در جهت افزایش این دقت ضرورت خواهد داشت

۳. قابلیت دسترسی: اطلاعات برای افرادی که مجاز به استفاده از آن می‌باشند باید در دسترس بوده و امکان استفاده در موقع لزوم برای این افراد مقدور باشد.

[Downloaded from jnraims.ir on 2026-11-20]

فهرست منابع و مآخذ

ـ پورمند، علی، (۱۳۹۰) استانداردی برای امنیت اطلاعات www.imi.ir/tadbir

ـ ترابی میلاد. ۱۳۹۵ نقش امنیت اطلاعات در سازمان‌ها. منتشر شده در کنفرانس بین‌المللی پژوهش در علوم و مهندسی

ـ جراحی و عظیمی (۱۳۸۷)، پیاده‌سازی مدیریت امنیت اطلاعات، تهران، پنجمین کنفرانس بین‌المللی مدیریت فناوری اطلاعات و ارتباطات، ص ۹.

ـ جعفری، نیما، (۱۳۹۰) سیستم مدیریت امنیت اطلاعات از طرح تا اصلاح، ماهنامه تدبیر، شماره ۱۸۹

ـ حریری، نجلا؛ نظری، زهرا، (۱۳۹۱) امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران، فصلنامه کتابداری و اطلاع رسانی، شماره ۵۸

ـ خوانی، امیر، ۱۳۸۸ ارائه مدلی جهت شناسایی عوامل موثر بر اثربخشی سیستم مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران،

ـ سادوسکای، جورج و دیگران، (۱۳۸۴)، راهنمای امنیت فناوری اطلاعات، ترجمه مهدی میردامادی، زهرا شجاعی، محمدجواد صمدی، تهران، دبیرخانه شورای عالی اطلاع‌رسانی.

ـ شیرازی، حسین و روح الله آل شیخ. (۱۳۸۸) مدیریت امنیت ارتباطات و اطلاعات. دانشگاه صنعتی مالک اشتر. ۱۳۸۸. جلد اول و دوم

ـ دشتی، افسانه (۱۳۸۴). " استانداردهای امنیت" مجله شبکه، ش ۵۴، ۱۵۸.

ـ عابدی جعفری، حسن؛ اسد نژاد رکنی، مهدی؛ و حمیدرضایزدانی، (۱۳۹۰)، بررسی تأثیر استفاده از فناوری اطلاعات بر عملکرد عملیاتی و عملکرد راهبردی واحد مدیریت منابع انسانی در شرکت‌های خودرو ساز و قطعه ساز تهران. فصلنامه مدیریت فناوری اطلاعات، دوره ۳، شماره ۹، صص ۸۸-۶۹)

ـ عامری، حسینی‌راد و باغبادی (۱۳۹۳)، بررسی مدل‌های مدیریت امنیت سیستم‌های اطلاعاتی در سازمان‌ها، اولین همایش منطقه‌ای دستاوردهای نوین در مهندسی کامپیوتر، نطنز، معاونت پژوهشی دانشگاه آزاد اسلامی واحد نطنز.

ـ مدیری، ناصر. (۱۳۹۱)مهندسی امنیت سایت‌های کامپیوتری: مرجعی برای درس شبکه‌های کامپیوتری. مهرگان قلم

ـ ونکی مونا ۱۳۹۶ مدل پیاده‌سازی مدیریت امنیت فناوری اطلاعات در صنعت بانکداری ایران مونا ونکی پایان نامه دکتری دانشکده پردیس تحصیلات تکمیلی خودگردان علامه طباطبایی

__ B. G. King, T. Felin, D. A. Whetten,(2010) Finding the organization in organizational theory: a meta-theory of the organization as a social actor, Organ. Sci. 21 (1), pp. 290–305

[Downloaded from jnraims.ir on 2026-11-20]

__ Coa, J. , & Song, W. (2016). Risk assessment of co creating value with costumers: a rough group analytic network process approach. Expert system with applications , 55 (15), 145-156.

__ C. B. Jarvis, S. B. MacKenzie, P. M. Podsakoff,(2003) A critical review of construct indicators and measurement model misspecification in marketing and consumer research, J. Consum. Res. 30 (2), pp. 199–218

__ D. Gefen, D. Straub, M. Boudreau,(2000) Structural equation modeling and regression: guidelines for research practice, Commun. Assoc. Inf. Syst. 4 (7), pp. 1–77.

__ F. J. Mata, W. L. Fuerst, J. B. Barney,(1995) Information technology and sustainable competitive advantage: a resource-based view, MIS Q. 19 (4), pp. 487–504.

__ G. Dhillon, J. Backhouse,(2000) Information system security management in the new millennium, Commun. ACM 43 (7), pp. 125–128.

__ G. Dhillon, J. Backhouse,(2009) Current directions in IS security research: towards socioorganizational perspectives, Inf. Syst. J. 11 (2, pp. 127–153.

__ H. A. Haveman,(1993) Follow the leader—mimetic isomorphism and entry into new markets, Admin. Sci. Q. 38 (4), pp. 593–627.

__ Karyda, M. , Kiountouzis, E. & Kokolakis, S. (2005). Information systems security policies: a contextual perspective, Computers & Security, 24(3), 246-260.

__ Kovacich, Gerald L. (2016) Chapter 7 - The Cyber Security Program's Strategic, Tactical, & Annual Plans. The Information Systems Security Officer's Guide (Third Edition), P. P 119-129 ; P. P 273-281 ;P. P 131-173.

__ K. E. Greenaway, Y. E. Chan,(2005) Theoretical explanations for firms' information privacy behaviors, Commun. AIS 6 (6), pp. 171–198.

__ Pipkin, Donald. L. (2000). " Information security" new jersey: Prentice Hall.

__ P. J. DiMaggio, W. W. Powell,(1983) The iron cage revisitedinstitutional isomorphism and collective rationality in organizational fields, Am. Sociol. Rev. 48 (2), pp. 147–160

__ Pilling, Rafe. (2013) Global threats, cyber-security nightmares & how t-protect against them. Computer Fraud & Security, , Issue 9, September, P. P 14-18(.

__ R. Garud, C. Hardy, S. Maguire,(2007) Institutional entrepreneurship as embedded agency: an introduction to the special issue, Organ. Stud. 28 (7), pp. 957–969.

__ R. M. Grant,(2005) Contemporary Strategy Analysis, Blackwell Publishers, Boston, MA,

__ S. Dynes, H. Brechbuhl, M. E. Johnson,(2005) Information security in the extended enter- prise: some initial results from a field study of an industrial firm, in: Proceedings of the Workshop on Economics of

[Downloaded from jnraims.ir on 2026-11-20]

Information Security, Boston, MA, Stewart, Thomas, ,2001, Wealth of Knowledge. Doubleday, New York, NY, 379 -

[Downloaded from jnraims.ir on 2026-11-20]

[Downloaded from jnraims.ir on 2026-11-20]