نشریه علمی پدافند غیرعامل

سال سیزدهم، شماره ۴، زمستان ۱۴۰۱، (پیاپی ۵۲): صص ۳۸-۲۱

علمی-پژوهشی

مقایسه تطبیقی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات و احصای شاخص‌های امنیت سایبری مشترک

محمد اختری[۱]، محمدعلی کرامتی[۲*]، سیدعبداله امین موسوی[۳]

تاریخ دریافت:۱۴۰۰/۱۲/۲۲
تاریخ پذیرش: ۱۴۰۱/۰۷/۳۰

چکیده

با ورود جهان به عصر اطلاعات دیجیتال، نیازمندی دولت‌ها و شرکت‌ها به فناوری اطلاعات در راستای بهینه‌سازی عملکردها، هوشمندسازی فرایندهای کسب‌وکار و ارائه خدمات از راه دور افزایش پیدا کرده است. بدین ترتیب، فناوری اطلاعات و امنیت سایبری و اطلاعات نیز جایگاه ویژه‌ای در عرصه دیجیتال یافته است. بر همین اساس یکی از جدی‌ترین خطراتی که دولت‌ها با آن روبرو هستند که می‌تواند امنیت ملی را نیز مورد آسیب قرار دهد، حملات سایبری است. این حملات طیف گسترده‌ای از اهداف را در برمی‌گیرد که یکی از اصلی‌ترین اهداف، آسیب رساندن به زیرساخت‌های حیاتی است؛ بنابراین پایداری زیرساخت‌های حیاتی در مواجهه با چنین تهدیداتی بسیار حائز اهمیت است. این پژوهش با توجه به اینکه ایمن‌سازی زیرساخت‌های حیاتی یکی از مهم‌ترین عوامل تأمین امنیت ملی و پدافند غیرعامل محسوب می‌شود، به دنبال احصای شاخص‌های ایمن‌سازی زیرساخت‌های حیاتی از طریق روش مطالعه تطبیقی با استفاده از منابع کتابخانه‌ای است. در این پژوهش ۱۰ مدل از مهم‌ترین مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات مورد واکاوی قرار گرفته است که نتایج حاصل از این پژوهش بیانگر آن است که مدل‌های بررسی‌شده مجموعاً دارای ۹۳ شاخص هستند. مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات شباهت قابل‌توجهی به یکدیگر دارند؛ لذا برخی از شاخص‌های احصا شده دارای همپوشانی است. شاخص‌های دارای همپوشانی، شناسایی و در ۱۷ گروه دسته‌بندی شده‌اند. نتایج به‌دست‌آمده نشان می‌دهد که شاخص «مدیریت رخداد» با فراوانی ۱۱، موردتوجه‌ترین شاخص در ایمن‌سازی زیرساخت‌های حیاتی است، همچنین شاخص‌های امنیت فیزیکی، نظارت، کنترل دسترسی- هویت، سیاست‌های امنیتی و سایر شاخص‌ها در جایگاه بعدی قرار دارند.

کلیدواژه‌ها: زیرساخت‌های حیاتی، مدل بلوغ امنیت سایبری، مدل بلوغ امنیت اطلاعات، پدافند غیرعامل.

۱- دانشجوی دکتری گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
۲- دانشیار گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران - نویسنده مسئول (mohammadalikeramati@yahoo.com)
۳- استادیار گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

۱- مقدمه

با ورود جهان به عصر اطلاعات دیجیتال، نیازمندی دولت‌ها و شرکت‌ها به فناوری اطلاعات در راستای بهینه‌سازی عملکردها، هوشمندسازی فرایندهای کسب‌وکار و ارائه خدمات از راه دور افزایش پیدا کرده است. بدین ترتیب فناوری اطلاعات و امنیت سایبری نیز جایگاه ویژه‌ای در عرصه دیجیتال پیدا کرده است. مؤلفه‌های قدرت در دهه اخیر به دلیل توسعه فضای سایبری دستخوش تغییرات گسترده‌ای شده که زمینه‌ساز ایجاد مفاهیم جدید در سیاست شده است. امروزه توانایی نفوذ در فضای سایبر به‌عنوان یکی از مهم‌ترین منابع قدرت در قرن ۲۱ محسوب می‌شود؛ لذا بازیگران دولتی و غیردولتی برای دست یافتن به اهداف نظامی، ایدئولوژیک و اجتماعی در فضای سایبر یا فضای فیزیکی از این قدرت بهره می‌گیرند. حوزه سایبری دارای ویژگی‌های منحصربه‌فردی همچون گمنامی و نامتقارن بودن است که بر این اساس کشورها در عصر کنونی بر قدرت سایبری تمرکز کرده‌اند [۱].

نظریه‌پردازان مختلفی به تعریف این مفهوم پرداخته‌اند که بر اساس تعریف وایتمن [1] امنیت اطلاعات شامل محرمانه بودن، یکپارچگی و در دسترس بودن داده‌ها در هنگام ذخیره‌سازی، پردازش یا انتقال می‌شود که اختلال در هر کدام از مؤلفه‌های فوق می‌تواند تأثیر جدی بر عملکرد دولت‌ها، شرکت‌ها و جامعه داشته باشد [۲]. جرائم سایبری یک صنعت رو به رشد است که هزینه‌های آن برای اقتصاد جهانی بین ۳۷۵ تا ۵۷۵ میلیارد دلار برآورد شده است [۳].

در دنیای امروز فناوری اطلاعات، تحولات زیادی را تجربه کرده است. این تحولات در حوزه سایبری و امنیت آن اتفاق می‌افتد؛ در این حوزه روزانه ابزارهای مخرب [2] زیادی توسعه و تولید می‌شوند. در مقابل متخصصان امنیتی این حوزه سعی در شناسایی و جلوگیری ازاین‌گونه فعالیت‌ها دارند [۴]. برای جلوگیری از این جرائم سایبری، لازم است با استفاده از اقدامات امنیتی سایبری گسترده و به‌روز، از زیرساخت‌های حیاتی کشور برای به حداقل رساندن خطرات حملات سایبری محافظت کرد. امنیت سایبری و امنیت اطلاعات دارای نقاط مشترک بسیاری هستند اما این دو از یکدیگر متمایزند. بر طبق استاندارد ISO270032 امنیت اطلاعات به حفاظت از داده‌ها و امنیت سایبری بر پیشگیری و یا توقف حملات سایبری از طریق افزایش امنیت برنامه‌ها، امنیت شبکه و امنیت اینترنت تمرکز دارد. در تعریفی دیگر امنیت سایبری مجموعه‌ای از ابزارها، سیاست‌ها، مفاهیم امنیتی، دستورالعمل‌ها، رویکردهای مدیریت ریسک، اقدامات، آموزش، بهترین شیوه‌ها، تضمین‌ها و فناوری‌هایی است که می‌تواند برای حفاظت از محیط سایبری و دارایی‌های شرکت و کاربر استفاده شود [۵]. لازم به ذکر است درک رابطه بین این حوزه‌های امنیتی، جهت تأمین امنیت زیرساخت‌های حیاتی کشور امری ضروری می‌باشد که در شکل (۱) چگونگی این روابط مشخص شده است.

[1] Whitman
[2] Malicious

شکل (۱): رابطه بین امنیت سایبری و حوزه‌های مرتبط با آن [۶]

حملات سایبری می‌تواند پیامدهای ناگواری را در شبکه‌های نظامی و همچنین زیرساخت‌های شبکه‌ای غیرنظامی ایجاد کنند. با مدل‌سازی حملات سایبری، تحلیل‌گران این حوزه با دانستن انواع مختلف حملات و فنون به‌کاررفته به ارزیابی اثرات هر کدام از حملات پرداخته و خود را برای دفاع در مقابل آن‌ها آماده می‌کنند [۷].

زیرساخت‌های حیاتی از دارایی‌های مهم امنیت عمومی، رفاه اقتصادی و امنیت ملی کشورها محسوب می‌شوند. سیستم‌های سایبری به‌طور گسترده برای نظارت و کنترل زیرساخت‌های حیاتی استفاده می‌شوند، تعدادی از این زیرساخت‌ها بر بستر فناوری اطلاعات و اینترنت می‌باشند؛ بنابراین امنیت سایبری یکی از موارد مهم در دستور کار امنیت ملی هر کشور است.

اطمینان از حفاظت اطلاعات و محیط سایبری زیرساخت‌های حیاتی در برابر تهدیدات بالقوه برای دولت‌ها اهمیت زیادی دارد، چراکه زیرساخت‌های حیاتی وابسته به فناوری اطلاعات هستند. این وابستگی فزاینده به فناوری اطلاعات، موجب اقدام دولت‌ها در جهت کاهش خطرات ناشی از اختلال در سیستم‌های سایبری زیرساختی فناوری اطلاعات شده است. در صورت نادیده گرفتن این ریسک‌ها و وقوع فاجعه یا وقوع یک جنگ سایبری، ممکن است زیان‌های مالی هنگفتی متوجه آن کشور شود. برای جلوگیری از جرائم سایبری و حملات سایبری به زیرساخت‌های حیاتی، سرمایه‌گذاری مستمر در اقدامات امنیت سایبری، پژوهش‌های گسترده و به‌روزرسانی سیستم‌های پیچیده حفاظت از داده‌ها ضروری است. با توجه به اینکه در دهه اخیر تهدیدات سایبری رشد پیدا کرده‌اند، یکی از جدی‌ترین خطرات عملیاتی پیش روی دولت‌ها و سازمان‌ها، حملات و نفوذهای سایبری مکرر است که نیاز به بهبود امنیت سایبری را نمایان می‌سازد. امنیت ملی و شکوفایی اقتصادی به عملکرد قابل‌اعتماد زیرساخت‌های حیاتی و عملکرد پایدار سازمان‌ها از هر نوع در مواجهه با چنین تهدیداتی بستگی دارد [۸].

جایگاه راهبردی جمهوری اسلامی ایران در منطقه و سطوح بین‌المللی باعث شده تا همواره تهدیدهایی از سوی قدرت‌های بزرگ

نسبت به ایران اسلامی اعمال شود. مطابق فرمایش‌های رهبر فرزانه انقلاب اسلامی ایران، حضرت امام خامنه‌ای (مدظله‌العالی) تنها راه ایستادگی در مقابل استکبار جهانی و تهدیدهای آن، «مبارزه و آمادگی دفاعی» در همه زمینه‌ها است. معظم له همواره بر مسائل پدافند غیرعامل تأکید می‌نمایند [۹].

پنج هدف اصلی پدافند غیرعامل در سیاست ابلاغی از سوی مقام معظم رهبری، افزایش بازدارندگی، تداوم فعالیت ضروری، تسهیل مدیریت بحران، کاهش آسیب‌پذیری و ارتقاء پایداری ملی است [۱۰]. در این پژوهش هدف دوم یعنی تداوم فعالیت ضروری موردبررسی قرار گرفته است؛ بنابراین، نظر به اینکه فضای سایبری هیچ‌گونه حدومرزی ندارد و با کمترین هزینه و از هر نقطه جهان می‌توان هدف را موردحمله قرار داد، تهدیدات سایبری را می‌توان یکی از بزرگ‌ترین چالش‌های پیش‌روی حوزه امنیت زیرساخت‌های حیاتی قلمداد کرد. به همین جهت، فرایند طراحی سیاست‌های امنیت سایبری پایدار برای زیرساخت‌های حیاتی، در دستور کار بیشتر کشورهای جهان و همچنین سازمان پدافند غیرعامل کشور قرار گرفته است [۱۱]. ازاین‌رو، ضرورت آن می‌رود با توجه به اینکه در سال‌های اخیر حجم حملات سایبری به زیرساخت‌های حیاتی جمهوری اسلامی ایران، توسط دولت‌های متخاصم افزایش یافته است، ارائه یک مدل برای بالا بردن ضریب تاب‌آوری و امنیت سایبری زیرساخت‌های حیاتی موردنیاز است، برای رسیدن به یک مدل بلوغ امنیت سایبری، در گام اول می‌بایست شاخص‌های ایمن‌سازی زیرساخت‌ها احصا گردد و پس‌ازآن نسبت به تدوین مدل بلوغ امنیت سایبری برای این زیرساخت‌ها اقدام کرد.

۱-۱- اهمیت و اهداف پژوهش

۱-۱-۱- اهمیت

انجام این پژوهش از جنبه‌های ذیل دارای اهمیت است.

- مشخص شدن اجزا، شاخص‌ها و ویژگی‌های مدل بلوغ امنیت سایبری.
- کمک به ایمن‌سازی زیرساخت‌های حیاتی در حوزه سایبری و تصمیم‌گیری مدیران کشوری برای پیاده‌سازی مدل بلوغ امنیت سایبری در سطح ملی.
- کمک به بازنگری و ارزیابی وضعیت امنیت سایبری در زیرساخت‌های حیاتی کشور.
- پیش درآمدی برای تهیه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور.

۱-۱-۲- اهداف

انجام چنین تحقیقاتی موارد ذیل را به دنبال خواهد داشت.

- ایجاد مواضع فعالانه در برابر حملات سایبری.
- افزایش قدرت دفاع سایبری به دلیل پژوهش در حوزه زیرساخت امنیت سایبری.
- امکان برنامه‌ریزی هوشمندانه توسط حاکمیت در به‌کارگیری و توسعه مدل‌های بلوغ امنیت سایبری در زیرساخت‌های حیاتی کشور.

افزون بر آن افزایش استفاده از خدمات فناوری اطلاعات و ارائه برخی از زیرساخت‌های حیاتی کشور بر بستر فناوری اطلاعات و به‌موجب آن افزایش حملات سایبری، تضمین محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات امری بسیار مهم و حیاتی می‌باشد. در نتیجه همان‌طور که قبلاً بیان شده است، یکی از روش‌ها به‌منظور حفظ امنیت سایبری پایدار به‌کارگیری مدل بلوغ امنیت سایبری است که می تواند دولت‌ها و سازمان‌ها را در سطوح مختلف جهت ارزیابی و بهبود برنامه‌های امنیت سایبری و انعطاف‌پذیری عملیاتی راهنمایی و تقویت کند؛ ازاین‌رو در پژوهش حاضر، سعی بر آن شده است که انواع مدل‌های بلوغ امنیت سایبری موردبررسی و واکاوی قرار گیرد تا از این طریق بتوان شاخص‌های ایمن‌سازی زیرساخت‌های حیاتی را احصا نمود.

این پژوهش در چند بخش سازمان‌دهی شده است. بخش اول مقدمه و بیان مسئله را در برمی‌گیرد، بخش دوم روش تحقیق مورداستفاده در این پژوهش را معرفی می‌کند، بخش سوم به‌مرور ادبیات پرداخته است، در بخش چهارم مبانی نظری شرح داده شده است و در بخش پنجم مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات مورد واکاوی قرار گرفته است، در بخش ششم و هفتم نتایج به‌دست‌آمده، نتیجه‌گیری و پیشنهادهایی برای کارهای آتی بیان می‌شود و در انتها به پیوست برخی از داده‌های به‌دست‌آمده در این پژوهش آمده است.

۲- روش تحقیق

روش تحقیق مورداستفاده در این پژوهش روش مقایسه تطبیقی است، منظور از مطالعات تطبیقی شناخت یک پدیده در پرتو مقایسه است که با توصیف و تبیین نقاط مشترک و نقاط اختلاف انجام می‌پذیرد. در مطالعات تطبیقی صرف مقایسه کردن هدف نیست، بلکه از کشف موارد تشابه و اختلاف باید به ملاک تشابه یا اختلاف رسید و بر اساس آن مسئله را حل کرد [۱۲]؛ بنابراین می‌توان نتیجه گرفت روش تحقیق مطالعات تطبیقی مقایسه‌ای، راهبردی عقلایی جهت استفاده از تجارب دیگران است.

مطابق با فرایند یادشده و پس از تبیین مسئله، دامنه پژوهش «بررسی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات در سطح بین‌المللی» در نظر گرفته شد و با بررسی صورت گرفته و تجارب موجود، در عمل فرضیه اولیه‌ای توسط محققین پیشنهاد یا استنباط نشد. در ادامه با استفاده از روش جمع‌آوری اطلاعات

از طریق منابع کتابخانه‌ای و اینترنتی، مجموع اسناد و اطلاعات مرتبط با مدل‌های رایج بلوغ امنیت سایبری و امنیت اطلاعات، منتشرشده در سطوح جهانی موردبررسی جامعی قرار گرفت و جدیدترین و معتبرترین این شاخص‌ها در قالب ۱۰ مدل انتخاب و مورد واکاوی قرار گرفت. در ادامه این پژوهش، ۹۳ شاخص از مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات شناسایی شد؛ با توجه به تشابه بین شاخص‌های احصا شده، موارد مشابه به‌صورت گروه‌بندی در جدول (۱۴) جمع‌بندی و در نهایت شاخص‌های مهم بر اساس فراوانی در جدول (۱۱) ارائه شد.

این شاخص‌ها می‌تواند علاوه بر استفاده در تدوین اسناد بالادستی، معیاری برای ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور قرار گیرد، همچنین مدیران کشوری می‌توانند برای پیاده‌سازی مدل بلوغ امنیت سایبری در سطح ملی از این پژوهش بهره گرفته و نسبت به تدوین راهبردها و برنامه-های عملیاتی اقدام نمایند.

۳- مرور ادبیات

بررسی تحقیقات پیشین نشان می‌دهد که مدل بلوغ امنیت اطلاعات و مدل بلوغ امنیت سایبری از برخی جوانب موردبررسی قرار گرفته است ولی تحقیقات صورت گرفته در راستای احصای شاخص‌های ایمن‌سازی و ارائه مدل بلوغ امنیت سایبری زیرساخت‌های حیاتی کشور نبوده که پژوهش حاضر در امتداد انجام رساله دکتری تخصصی با عنوان ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور برای اولین بار نسبت به احصای این شاخص‌ها اقدام کرده است. برای نمونه در یکی از پژوهش‌های پیشین با عنوان «ارائه مدلی برای پایش بلوغ امنیت اطلاعات»، مدل‌های بلوغ امنیت اطلاعات موردبررسی قرارگرفته و با توجه به نظر خبرگان و یافته‌های پژوهش مدلی متشکل از پنج مرحله برای پایش امنیت اطلاعات ارائه گردیده است، این پژوهش در یکی از شرکت‌های زیرمجموعه صنعت نفت انجام شده است و پایه آن بر اساس الزامات استاندارد ISO27001 است [۱۳].

در پژوهشی دیگر با عنوان «بررسی انواع راه‌کارهای افزایش امنیت در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی»، دفاع در عمق را یکی از مهم‌ترین و پرکاربردترین راهبرد در ایمن‌سازی سیستم‌های کنترل صنعتی برشمرده است، همچنین در این پژوهش به بحث و توضیح این مسائل در قالب دو دسته پایه‌ای و ساختاری پرداخته شده است [۱۴].

به‌علاوه در پژوهشی دیگر با عنوان «مدل پرسشنامه‌ای برای ارزیابی بلوغ امنیت سایبری در زیرساخت‌های حیاتی» با استفاده از پرسشنامه و بررسی انواع مدل‌های بلوغ امنیت سایبری، یک مدل برای ارزیابی و بهبود امنیت سایبری برای ارائه‌دهندگان خدمات و مدیران زیرساخت‌های حیاتی ارائه شده است [۱۵].

همچنین در پژوهشی دیگر با عنوان «مدل بلوغ امنیت سایبری مبتنی بر آسیب‌پذیری برای اندازه‌گیری آمادگی حفاظت از زیرساخت‌های حیاتی ملی» یک مدل بلوغ امنیت سایبری مبتنی بر آسیب‌پذیری برای اندازه‌گیری زیرساخت‌های حیاتی در کشور ترکیه ارائه گردیده است [۱۶].

در یک کار پژوهشی دیگر با عنوان «مطالعه تطبیقی مدل‌های بلوغ قابلیت امنیت سایبری» نسبت به توصیف و مقایسه پرکاربردترین مدل‌های بلوغ قابلیت امنیت سایبری، در نتیجه یک بررسی سیستماتیک (SR) از مطالعات منتشرشده در بازه زمانی ۲۰۱۲ تا ۲۰۱۷ اقدام شده است [۱۷].

پژوهشی دیگر با عنوان «چارچوب جامع ارزیابی بلوغ امنیت سایبری برای مؤسسات آموزش عالی در انگلستان» یک مدل سبک و مبتنی بر وب را ارائه می‌کند که می‌تواند به‌عنوان ابزار ارزیابی امنیت سایبری برای مؤسسات آموزش عالی[1] (HEI) انگلستان استفاده شود. این پژوهش چارچوب جامع ارزیابی بلوغ امنیت سایبری شامل کلیه مقررات امنیتی، مقررات حفظ حریم خصوصی و بهترین شیوه‌هایی است که برای مؤسسات آموزش عالی باید با آن‌ها مطابقت داشته باشد و می‌تواند به‌عنوان خودارزیابی یا ابزار ممیزی امنیت سایبری مورداستفاده قرار گیرد را ارائه می‌دهد [۱۸].

در پژوهشی که در قالب یک رساله دکتری با عنوان «مدل بلوغ قابلیت امنیت سایبری برای زیرساخت‌های فناوری اطلاعات حیاتی در سازمان‌های مالی نیجریه» انجام شده است، مدل بلوغ قابلیت امنیت سایبری (C2M2[2]) برای سازمان‌های مالی نیجریه به‌عنوان یک مدل امنیتی برای تعیین سطح قدرت امنیت سایبری در سازمان‌های مالی نیجریه برگزیده شده است. این مدل توسعه‌ای پنج سطح بلوغ را ارائه کرده است. هدف این پژوهش ایجاد مدلی است که سطح قدرت امنیت سایبری در سازمان‌های مالی نیجریه را افزایش دهد. هفت سازمان شامل: گارانتی تراست بانک، یونایتد بانک آفریقا، یونیون بانک نیجریه، اولین بانک نیجریه، بانک Stanbic-IBTC، بانک وام مسکن فدرال و بانک پولاریس که همگی در منطقه داماتورو واقع شده‌اند، برای

[1] High Education Instituted
[2] Cybersecurity Capability Maturity Model

سنجش آمادگی امنیت سایبری خود با استفاده از این مدل توسعه انتخاب شده‌اند. همچنین در این پژوهش مصاحبه کاملاً ساختاریافته با مدیران فناوری اطلاعات انجام شده است. تجزیه‌وتحلیل نتایج نشان می‌دهد که تمامی سازمان‌ها در مطالعه موردی در سطح پیشرفته‌ای قرار دارند [۱۹].

به‌علاوه در پژوهشی دیگر با عنوان «ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی» به مطالعه و طبقه‌بندی تهدیدات سایبری پرداخته است، همچنین در این پژوهش با بررسی ادبیات موضوعی، شناسایی تهدیدات سایبری پرتکرار، اعتبارسنجی آن‌ها از منابع معتبر و استخراج مفاهیم مشترک مربوط به شناسایی تهدیدات سایبری، ابعاد و مؤلفه‌ها و شاخص‌های طبقه‌بندی تهدیدات سایبری زیرساخت-های حیاتی استخراج شده است [۲۰].

همچنین در پژوهشی دیگر که در قالب یک رساله دکتری با عنوان «مدل بلوغ امنیت اطلاعات برای سازمان‌های بهداشتی درمانی در ایالات متحده» با بررسی ادبیات موضوعی و مدل‌های مرجع نسبت به تبیین شاخص‌ها و مؤلفه‌های ارزیابی سازمان‌های بهداشتی پرداخته و درنهایت با معرفی یک مدل قابل‌تعمیم و سیستم اندازه‌گیری عملکرد امنیت اطلاعات در سازمان‌های بهداشتی درمانی کار خود را خاتمه داده است [۲۱].

در یک کار پژوهشی دیگر با عنوان «مدل بلوغ منطقه کانونی امنیت سایبری (CYSFAM[1])» با اتکا به نظر خبرگان و تهیه پرسشنامه، مدل بلوغ منطقه کانونی امنیت سایبری (CYSFAM) برای ارزیابی قابلیت‌های امنیت سایبری پیشنهاد شده است، همچنین در این تحقیق یک موسسه مالی مورد ارزیابی قرارگرفته است [۲۲].

لازم به توضیح است که تحقیقاتی که تاکنون صورت گرفته است جامع نبوده و هر کدام بخشی از امنیت سایبری و یا شاخص‌های آن را موردبررسی قرار داده است؛ لذا خلأ وجود شناسایی شاخص‌های بلوغ امنیت سایبری برای زیرساخت‌های حیاتی به چشم می‌خورد. ازاین‌رو در پژوهش پیش‌رو به‌منظور افزایش امنیت سایبری در حوزه زیرساخت‌های حیاتی کشور سعی شده است با واکاوی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات نسبت به شناسایی شاخص‌های حائز اهمیت اقدام نمود.

۴- مبانی نظری

۴-۱- زیرساخت‌های حیاتی

زیرساخت به مجموعه عناصر ساختاری به هم پیوسته‌ای اطلاق می‌شود که یک سیستم بزرگ را تشکیل داده و دارای ابعاد فنی و فناورانه گسترده‌ای است و در صورت عملکرد صحیح همه بخش‌های آن، می‌توان عرضه خدمات را به نحوه مطلوبی انتظار داشت. در یک تقسیم‌بندی کلی، می‌توان زیرساخت‌ها را به دو نوع حیاتی و غیرحیاتی طبقه‌بندی کرد. با این تقسیم‌بندی قائل به این هستیم که اهمیت برخی از زیرساخت‌ها نسبت به برخی دیگر بیشتر است. با توجه به این تفکیک به نظر می‌رسد زیرساخت‌های حیاتی را می‌توان به زیرساخت‌های مرتبط با امنیت ملی یک کشور مرتبط دانست [۲۳].

زیرساخت‌های حیاتی، ارائه‌دهنده خدمات اساسی و بنیادی است و ازاین‌رو چارچوب اصلی برای پشتیبانی از ساختارهای کلان امنیت ملی کشور و آحاد ملت می‌باشد. به همین جهت است که حفاظت از زیرساخت‌های حیاتی و دارایی‌های کلیدی از مهم‌ترین وظایف و مأموریت‌های هر دولتی محسوب می‌شود؛ چراکه تخریب یا وارد آمدن آسیب به آن‌ها، به‌راحتی می‌تواند تداوم حیات یک کشور را با مشکل مواجه سازد و امنیت آن را به لحاظ سیاسی، اقتصادی و دفاعی به شکل جدی به خطر اندازد [۲۴].

سازمان امنیت ملی ایالات متحده آمریکا، زیرساخت‌های حیاتی را شامل دارایی‌ها، سیستم‌ها و شبکه‌ها به‌صورت فیزیکی و مجازی تعریف می‌نماید، این زیرساخت‌ها از اهمیت بالایی برخوردار هستند، به‌گونه‌ای که آسیب و یا تخریب آن‌ها موجب تأثیر بر امنیت، پایداری اقتصادی، سلامت و ایمنی عمومی خواهد شد [۲۵].

زیرساخت‌های حیاتی اصطلاحی است که برای توصیف دارایی‌هایی استفاده می‌شود که برای عملکرد و امنیت یک جامعه اقتصادی در هر کشور ضروری است که در شکل (۲) نشان داده شده است [۲۶].

شکل (۲): زیرساخت‌های حیاتی [۲۷]

[1] The Cybersecurity Focus Area Maturity

۴-۲- مدل‌های بلوغ

مدل بلوغ مجموعه‌ای از ویژگی‌ها، شاخص‌ها یا الگوهایی است که نشان‌دهنده توانایی و پیشرفت در یک رشته خاص است. محتوای مدل‌های بلوغ معمولاً بهترین روش‌ها را با استفاده از استانداردها یا سایر دستورالعمل‌های مرتبط با یک حوزه مشخص را در برمی‌گیرد؛ بنابراین، یک مدل بلوغ معیاری را برای یک سازمان فراهم می‌کند که به‌وسیله آن می‌تواند سطح فعلی توانایی عملکردها، فرآیندها و روش‌های خود را ارزیابی کند و اهداف و اولویت‌هایی را برای بهبود مشخص نماید. همچنین، هنگامی‌که یک مدل به‌طور گسترده در یک صنعت خاص استفاده می‌شود و نتایج ارزیابی به‌صورت ناشناس به اشتراک گذاشته شده است، سازمان‌ها می‌توانند عملکرد خود را در برابر سایرین محک بزنند [۸].

مدل‌های بلوغ، روشی برای نمایش دانش خاص در حوزه‌ای مشخص است که به روشی ساختاریافته و به‌منظور ارائه فرآیند تکاملی برای ارزیابی و بهبود سازمان‌ها ارائه می‌شود که در جدول (۱) نشان داده شده است [۲۸].

جدول (۱): برخی از مدل‌های بلوغ در حوزه‌های مختلف [۲۸]

مدل بلوغ	سازمان / نویسندگان
مدل بلوغ شبکه هوشمند (SGMM)	CMMI Institute-SEI
مدل بلوغ فرایند کسب‌وکار	OMG
مدل بلوغ قابلیت افراد	CMMI Institute-SEI
ادغام مدل بلوغ ارزیابی (TMMi)	TMMi Foundation

۴-۳- مدل‌های بلوغ امنیت سایبری

مدل‌های بلوغ امنیت سایبری با درک طیف گسترده‌ای از امنیت تا ناامنی تعیین می‌شود، این مدل‌ها به‌عنوان یک ابزار سنجش برای اندازه‌گیری تفاوت بین وضعیت سطح امنیت فعلی و سطحی که قرار است سازمان به آن برسد به کار گرفته می‌شود. افزون بر آن و با توجه به وابستگی زیرساخت‌های حیاتی به بستر فناوری و فضای سایبر، تدوین دستورالعمل و ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌ها امری ضروری است که این موضوع مستلزم شناخت دقیق شاخص‌های موجود در مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات می‌باشد.

ارزش‌هایی که یک مدل بلوغ امنیت سایبری ارائه می‌دهد شامل موارد زیر است [۲۹]:

- اطلاعات مربوط به محیط امنیت سایبری را جمع‌آوری و تجسم آن را نسبتاً آسان می‌کند.
- ابزاری برای اندازه‌گیری پیشرفت وضعیت امنیت سایبری و سطح بلوغ آن فراهم می‌کند.
- به‌عنوان یک ابزار، به تجسم شکاف‌ها در وضعیت امنیت سایبری کمک می‌کند، مناطقی را که باید بهبود یابند شناسایی و سطح بلوغ امنیت سایبری را افزایش می‌دهد.
- فرصتی برای مقایسه وضعیت و سطوح امنیت سایبری با سایر ابزارها و معیارها فراهم می‌آورد.
- ارائه مستندات مربوط به سطح بلوغ امنیت سایبری، فرصتی برای توجیه سرمایه‌گذاری در حوزه‌های مختلف (افراد، فرایند، فناوری) و قانون‌گذاری برای مدیران و مسئولان به ارمغان می‌آورد.

تحقیقات صورت گرفته و بررسی پژوهش‌های پیشین بیانگر آن است که تاکنون مدل‌های مختلفی از بلوغ امنیت سایبری و بلوغ امنیت اطلاعات تدوین شده و توسعه یافته‌اند، بر این اساس به‌منظور احصای شاخص‌های ایمن‌سازی زیرساخت‌های حیاتی کشور مبتنی بر مدل‌های بلوغ امنیت سایبری و مدل‌های بلوغ امنیت اطلاعات مهم‌ترین مدل‌های موجود در این حوزه مورد واکاوی واقع شده است.

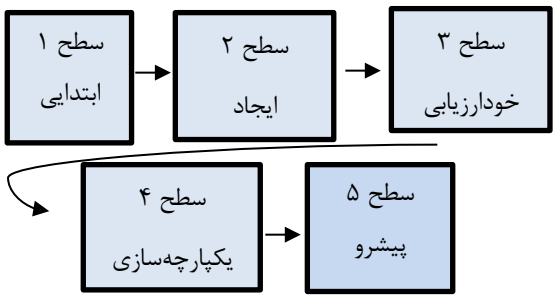
۵- انواع مدل‌های بلوغ امنیت سایبری

در این بخش مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات که در این پژوهش مورد واکاوی قرار گرفته‌اند، ارائه می‌شود، همچنین در جدول (۱۰) این مدل‌ها به‌صورت خلاصه بیان شده‌اند.

۵-۱- Maturity Model Community Cyber Security (CCSMM)

این مدل برای کمک به شرکت‌ها و جوامع مختلف برای ایجاد برنامه‌های امنیت سایبری و افزایش آگاهی در مورد خطرات سایبری توسعه یافته است. هدف این مدل ارائه ابزارهایی برای توسعه و بهبود امنیت سایبری می‌باشد. مدل بلوغ CCSMM یک معیار برای اندازه‌گیری وضعیت امنیت سایبری و سطح بلوغ

ارائه می‌کند (شکل ۳)، در نهایت یک نقشه راه برای بهبود وضعیت امنیت سایبری و همچنین یک نقطه مرجع و اصطلاحاتی مشترک برای استفاده‌کنندگان به ارمغان می‌آورد. این پروژه در بخش سایبری وزارت امنیت داخلی آمریکا در سال ۲۰۰۷ موردپژوهش قرار گرفته و در پنج ایالت پیاده‌سازی شده است [۳۰].



شکل (۳): مدل CCSMM [۳۰]

این مدل از پنج سطح بلوغ به شرح ذیل تشکیل شده است.

سطح یک، ابتدایی: این مرحله دارای حداقل آگاهی، همکاری و ارزیابی از امنیت سایبری است.

سطح دو، ایجاد: در این مرحله مدیران/مسئولان از مفاهیم و کلیات امنیت سایبری آگاه می‌باشند و برخی از همکاری‌ها، ارزیابی سیاست‌ها و رویه‌ها در این مرحله صورت می‌گیرد.

سطح سه، خودارزیابی: در این مرحله برنامه‌های مرتبط با آگاهی در خصوص امنیت سایبری از سوی مدیران و مسئولان حاکمیتی به افراد و شرکت‌های تابع اطلاع‌رسانی می‌شود. همچنین در این مرحله تمرین‌هایی در خصوص امنیت سایبری انجام شده و سیاست‌ها و رویه‌ها ارزیابی می‌گردند.

سطح چهار، یکپارچه‌سازی: در این مرحله برنامه‌هایی با محتوای امنیت سایبری از سوی مدیران و مسئولان حاکمیتی به افراد و شرکت‌های تابع ابلاغ می‌شود. همچنین مانورهای امنیت سایبری انجام شده و نتایج حاصل از آن ارزیابی و موردبررسی قرار می‌گیرد.

سطح پنج، پیشرو (نهایی): در این مرحله یک مرکز عملیات سایبری[1] ایجاد می‌شود که وظیفه این مرکز یکپارچه‌سازی واحدهای مختلف سایبری و پاسخگویی و راهنمایی سازمان‌های مختلف است.

مدل CCSMM در واقع ابزاری است که سازمان‌ها و شرکت‌ها می‌توانند از آن برای اندازه‌گیری و بهبود آمادگی خود در برابر حملات سایبری استفاده کنند، این امر با همکاری نهادهای مختلفی که در این حوزه نقش ایفا می‌کنند انجام می‌گردد. بارزترین ویژگی این مدل، اشتراک‌گذاری اطلاعات بین نهادهای مختلف، آگاهی بخشی به نیروی انسانی در حوزه امنیت سایبری و انجام رزمایش‌های سایبری است.

۲-۵- Information Security Maturity Model (ISMM)

هدف از ارائه مدل بلوغ ISMM این است که شرکت‌ها و سازمان‌ها بتوانند وضعیت پیاده‌سازی اقدامات انجام شده در خصوص امنیت اطلاعات را اندازه‌گیری نمایند. همان‌طور که در جدول (۲) مراحل این مدل ذکر شده است، این مدل در اوایل سال ۲۰۱۱ به‌عنوان فرآیندی برای مدیریت، اندازه‌گیری و کنترل شیوه‌های مدیریت امنیت اطلاعات انتشار یافت. اساس شکل‌گیری ISMM دقیقاً مشخص نمی‌باشد ولی ارائه‌دهنده این مدل با بهره‌گیری از چهارچوب COBIT[2] و TOGAF[3]، چهار دامنه برای آن ترسیم کرده است که این دامنه‌ها عبارت‌اند از: حاکمیت شرکتی، معماری سیستم، مدیریت خدمات و فرهنگ سازمانی [۳۱].

این مدل دارای پنج مرحله به شرح ذیل است.

سطح یک، عدم پذیرش: این بدان معناست که یک شرکت ممکن است فاقد سیاست‌ها و رویه‌های مرتبط با امنیت اطلاعات باشد.

سطح دو، پذیرش اولیه: در این مرحله شرکت‌ها از خطراتی که با آن مواجه هستند آگاه می‌شوند، اما این وضعیت شامل بی‌نظمی و تناقض است.

سطح سه، پذیرش ثانویه: رویه‌ها و فرآیندهای غیررسمی در این مرحله تعریف می‌شوند، همچنین فعالیت‌های اصلی کسب‌وکار و سیستم‌ها در این مرحله محافظت می‌شوند.

سطح چهار، قابل‌پذیرش: تمام پروتکل‌ها و سیاست‌های مدیریت امنیت اطلاعات به‌صورت متمرکز مدیریت می‌شوند.

سطح پنج، پذیرش کامل: یک شرکت از خطراتی که با آن مواجه است آگاه است و هر نیاز مرتبط با امنیت اطلاعات و تهدید کسب‌وکار را نظارت و بهبود می‌بخشد.

ISMM یک نمای کلی سطح پایین از امنیت اطلاعات است که اقدامات مختلفی را برای آن ارائه می‌کند.

[1] SOC (security operations center)

[2] Control Objectives for Information and Related Technologies
[3] The Open Group Architecture Framework

جدول (۲): سطوح مدل ISMM [۳۱]

سطوح انطباق	درجه (Stars)	ترکیب ارزیابی
عدم پذیرش	یک ستاره	۱٫۵-۰
پذیرش اولیه	دو ستاره	۲٫۵-۱٫۶
پذیرش ثانویه	سه ستاره	۳٫۵-۲٫۶
قابل‌پذیرش	چهار ستاره	۴٫۵-۳٫۶
پذیرش کامل	پنج ستاره	بیشتر از ۴٫۶

۳-۵- (E-Government) Information Security Maturity Model (ISMM)

مدل E-Government ISMM در اوایل سال ۲۰۱۱ برای اندازه‌گیری بلوغ حوزه‌های فنی و اجتماعی (غیر فنی) در شیوه‌های امنیت اطلاعات ایجاد شده است. این مدل برای شرکت‌هایی ایجاد شده است که خدمات دولتی ایمن ارائه می‌کنند. با استفاده از این مدل، شرکت‌ها می‌توانند میزان (بلوغ) اقدامات در حوزه امنیت اطلاعات خود را اندازه‌گیری کنند. استفاده‌کنندگان با استفاده از نتایج اندازه‌گیری، قادر به ایجاد طرح‌های مشخص برای بهبود اجرا و کنترل حوزه‌های فنی و اجتماعی هستند. برخلاف مدل‌های ISMM که قبلاً توسعه یافته است، این مدل هم کمیت و هم کیفیت خدمات دولتی را اندازه‌گیری می‌کند [۳۲].

این مدل حاصل پژوهشی است که به روش مطالعه مقایسه‌ای، تعدادی مدل بلوغ را مقایسه و بر اساس سه پارامتر (مدیریت، ارزیابی و آگاهی) دسته‌بندی کرده است که در نهایت منجر به ارائه این مدل شده است.

همان‌طور که در نمودار یک مشاهده می‌کنید، این مدل از پنج سطح بلوغ به شرح ذیل تشکیل شده است.

سطح یک، تعریف‌نشده: در این مرحله شرکت‌ها «اهداف امنیت اطلاعات[1]» پایینی دارند و در «محیط ریسک امنیتی[2]» پایین فعالیت می‌کنند. در این مرحله، اجرای تمام سیاست‌ها و فرایندها اجباری نیست و فقط برخی از فرایندهای کاهش ریسک و آگاهی الزامی است.

سطح دو، تعریف‌شده: شرکت‌ها در این مرحله، اهداف امنیت اطلاعات عادی دارند و همچنین در محیط ریسک امنیتی معمولی فعالیت می‌کنند. از دیگر مشخصات این مرحله می‌توان به عدم الزامی بودن انجام فرایندها، کاهش ریسک امنیتی و برقراری امنیت اطلاعات اشاره کرد.

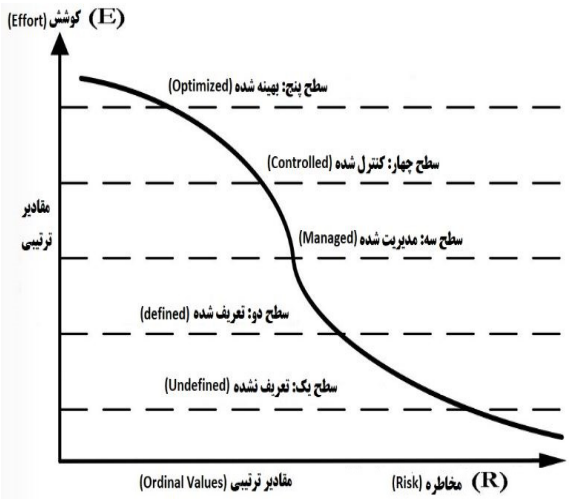
سطح سه، مدیریت‌شده: در این مرحله شرکت‌ها اهداف امنیت اطلاعات بالایی داشته و در محیط با ریسک بالای امنیتی کار می‌کنند، وجود سیاست امنیتی، کاهش ریسک‌های امنیتی و عدم الزامی بودن انجام فرایندها از دیگر مؤلفه‌های این مرحله است.

سطح چهار، کنترل‌شده: شرکت‌ها در این مرحله دارای اهداف امنیت اطلاعات بالایی می‌باشند و در محیط با ریسک بسیار بالا فعالیت می‌کنند، در این مرحله اجرای فرایندها الزامی بوده و کاهش ریسک به حد بالایی می‌رسد، همچنین امنیت اطلاعات، تعبیه شده و سیاست‌های امنیتی شکل می‌گیرند.

سطح پنج، بهینه‌شده: شرکت‌ها در این مرحله دارای اهداف امنیت اطلاعات بالاتری نسبت به مرحله قبل می‌باشند و در محیط با ریسک بسیار بالا فعالیت می‌کنند، در این مرحله اجرای فرایندها الزامی بوده و کاهش ریسک به بالاترین حد خود می‌رسد، همچنین امنیت اطلاعات، تعبیه شده و سیاست‌های امنیتی کامل شده‌اند.

این مدل در هفت دامنه فعالیت دارد، این دامنه‌ها عبارت‌اند از: راه‌حل‌های سخت‌افزاری، راه‌حل‌های نرم‌افزاری، اخلاقی و فرهنگی، حقوقی و قراردادی، اداری و مدیریتی، عملیاتی و رویه‌ای و آگاهی.

مهم‌ترین ویژگی این مدل متمرکز شدن اقدامات در سه گروه، مدیریت، ارزیابی و آگاهی است.



نمودار (۱): مدل E-Government ISMM [۳۲]

[1] IST (Information Security Targets)
[2] SRE (Security Risk Environment)

Five Stage To Information Security (5S2IS) -۴-۵

این مدل برای پیاده‌سازی مدیریت امنیت اطلاعات در شرکت‌های کوچک و متوسط [1] مورداستفاده قرار می‌گیرد. حتی شرکت‌هایی که قصد دریافت گواهینامه مرتبط با امنیت اطلاعات را ندارند می‌توانند از این مدل برای توسعه امنیت اطلاعات استفاده کرده و اقداماتی را جهت کاهش خطرات سایبری انجام دهند. این مدل در اواسط سال ۲۰۱۱ بر اساس استانداردهای ISO27001 و ISO27002 و مدل بلوغ قابلیت هامفری [2] استوار است [۳۳ و ۳۴].

این مدل از پنج سطح بلوغ به شرح ذیل تشکیل شده است.

سطح یک، تعهد: در این سطح شاخص‌های اصلی عملکرد [3] تعریف می‌شوند.

سطح دو، اصول: پروتکل‌ها و فرایندها برای انجام شاخص-های اصلی عملکردی که در مرحله قبل تعیین شده است، تعریف می‌شوند.

سطح سه، نظارت: در این مرحله خروجی‌های مرحله قبل (پروتکل‌ها و فرآیندها) با شاخص‌های اصلی عملکرد اندازه‌گیری می‌شوند.

سطح چهار، بهبودبخشی: در این مرحله، اندازه‌گیری شاخص‌های اصلی عملکرد برای شناسایی و بهبود کاستی‌ها در فرآیندها و پروتکل‌ها استفاده می‌شود.

سطح پنج، استقرار: در این مرحله، شرکت به‌طور مداوم بهبود می‌یابد و می‌تواند برای درخواست گواهینامه‌های رعایت امنیت اطلاعات/سایبری اقدام نماید. در مجموع این مدل دارای ۱۱ دامنه می‌باشد که برگرفته از استاندارد ISO27002: 2005 است و در جدول شماره (۳) به آن پرداخته شده است.

می‌توان استفاده از یک رویکرد گام‌به‌گام برای اجرای اقدامات مربوط به امنیت اطلاعات و راحتی پیاده‌سازی برای شرکت‌ها را از نقاط قوت این مدل برشمرد.

در پایان این مدل پیشنهاد می‌کند که شاخص‌های سیاست-های امنیتی، سازمان‌دهی امنیت اطلاعات، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی، مدیریت عملیات و ارتباطات، کنترل دسترسی، کسب سیستم اطلاعاتی، نگهداری و توسعه، مدیریت حوادث امنیت اطلاعات، مدیریت تداوم کسب‌وکار کار، انطباق در سطوح فوق موردبررسی قرار گیرند.

GAIA Maturity Level Information Security – ۵-۵ (GAIA-MLIS)

هدف مدل GAIA-MLIS افزایش بصیرت شرکت‌ها از سطح بلوغ آن‌ها در سیستم امنیت اطلاعات است. این امر با ارائه افزایش آگاهی از نقاط ضعف و قوت آن‌ها صورت می‌گیرد. این مدل بر اساس وضعیت شرکت، توصیه‌های مشخصی را در خصوص بهبود امنیت اطلاعات ارائه می‌دهد، هدف این مدل تعیین نقاط ضعف و کمک به بهبود و مدیریت در پنج حوزه، اطلاعات، سخت‌افزار، نرم‌افزار، خدمات، کارکنان می‌باشد (شکل ۴). مدل مذکور در اوایل سال ۲۰۱۴ انتشار یافت، این مدل برگرفته از استانداردهای COBIT5، 2005 :ISO27001، ISO27002: 2005 است [۳۵].

سطح صفر، بدون تضمین [4]: در این مرحله فرایندها و خط‌مشی‌ها تعریف نشده‌اند و اطلاع‌رسانی‌های لازم صورت نگرفته است، کنترل دسترسی و مدیریت دسترسی - هویت [5] وجود نداشته و داده‌ها فاقد رمزنگاری و طبقه‌بندی هستند، همچنین در این مرحله محیط فیزیکی فاقد امنیت لازم است و تجهیزات در برابر تهدیدات خارجی محافظت نمی‌شوند.

سطح یک، تضمین اولیه: در این گام برخی از فرایندها و خط‌مشی‌ها تعریف شده‌اند ولی همچنان آگاهی، کنترل دسترسی، رمزنگاری و طبقه‌بندی داده‌ها و امنیت فیزیکی وجود نداشته و فقط برخی از تجهیزات در برابر تهدیدات خارجی محافظت شده و مدیریت هویت و دسترسی در سطح پایینی صورت می‌گیرد.

سطح دو، تضمین معین: در این بخش فرایندها و خط‌مشی‌ها تعریف شده و آگاهی کمی حاصل شده است. مدیریت دسترسی - هویت و برخی از کنترل‌های دسترسی رعایت نمی‌شوند. امنیت فیزیکی، رمزنگاری و طبقه‌بندی اطلاعات همچنان نادیده گرفته شده و فقط برخی از تجهیزات در برابر تهدیدات خارجی محافظت می‌شوند.

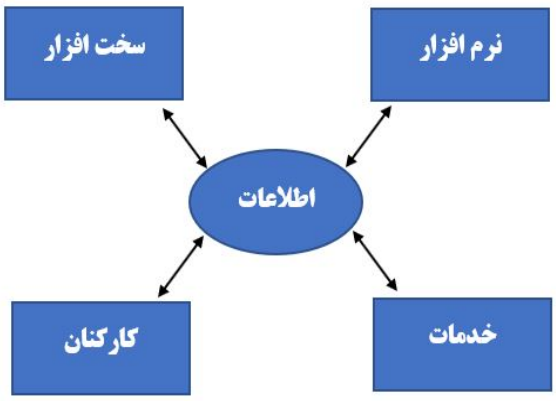
سطح سه، ایمنی نسبی: در این مرحله فرایندها و خط‌مشی‌ها تعریف شده‌اند و آگاهی به سطح نسبتاً مطلوبی رسیده است. مدیریت هویت و دسترسی، کنترل‌های دسترسی، امنیت فیزیکی، رمزنگاری و طبقه‌بندی داده‌ها صورت گرفته و فقط برخی از تجهیزات در برابر تهدیدات خارجی محافظت می‌گردند.

سطح چهار، تضمین کامل: در این گام فرایندها و خط‌مشی‌ها تعریف شده‌اند و آگاهی به سطح مطلوبی رسیده

[1] SME (Small and medium-sized enterprises)
[2] Humphrey
[3] KPIs (Key Performance Indicators)
[4] Insurance
[5] IAM (Identity and access management)

است. مدیریت هویت و دسترسی، کنترل‌های دسترسی، امنیت فیزیکی، رمزنگاری و طبقه‌بندی داده‌ها صورت گرفته و تمامی تجهیزات در برابر تهدیدات خارجی محافظت می‌گردند.

این مدل در پنج دامنه فعالیت دارد، این دامنه‌ها عبارت‌اند از سخت‌افزار، نرم‌افزار، خدمات و کارکنان. ابعادی که توسط این مدل موردتوجه قرار می‌گیرد، تمام وجوه یک شرکت را در برمی‌گیرد.



شکل (۴): مدل GAIA-MLIS [۳۵]

۵-۶- Information Security Focus Area Maturity Model (ISFAM)

مدل ISFAM در اوایل سال ۲۰۱۴ توسط اسپرویت و رولینگ[1] توسعه یافته است. این مدل بر حوزه امنیت اطلاعات متمرکز می‌باشد، همچنین قادر به تعیین سطح فعلی بلوغ امنیت اطلاعات است و می‌تواند برای بهبود تدریجی و ساختاری بلوغ امنیت اطلاعات در سازمان مورد بهره‌برداری قرار گیرد. این مدل از طریق چندین مطالعه موردی در بخش‌های مخابرات، آماد، مراقبت‌های بهداشتی و مالی با موفقیت ارزیابی شده است [۳۶].

مدل مذکور برگرفته از استانداردهای، ISO27002: 2005 سرفصل‌های دوره CISSP، استانداردهای منتشرشده در انجمن «تمرین خوب برای امنیت اطلاعات[2]»، چارچوب امنیت اطلاعات (ISO-light) و چارچوب IBM می‌باشد.

مدل ISFAM دارای ۱۲ سطح بلوغ است که به چهار مرحله بلوغ تقسیم می‌شود که در جدول (۴) نشان داده شده است.

مرحله یک، طراحی (شامل سطوح صفر الی چهار می‌باشد): در این مرحله سیاست‌ها توسعه یافته و شاخص‌های اصلی عملکرد[3] مشخص می‌شوند.

مرحله دو، پیاده‌سازی (شامل سطوح پنج و شش می‌باشد): نقش‌ها و مسئولیت‌ها در سازمان تعریف می‌شوند و فرآیندهای استاندارد توسعه می‌یابند.

مرحله سه، اثربخشی عملیاتی[4] (شامل سطوح هفت الی هشت می‌باشد): در این مرحله شرکت‌ها قادر به تضمین اجرای فرایندها و سیاست‌ها مطابق با طراحی صورت گرفته خواهند بود.

مرحله چهار، نظارت (شامل سطوح ۱۰ الی ۱۲ می‌باشد): این مرحله بر اجرای منظم سه مرحله اول نظارت می‌کند، سیاست‌ها، رویه‌ها و فرآیندها را بررسی و در صورت نیاز آن‌ها را به‌روزرسانی می‌نماید.

در واقع این ۱۲ سطح ترجمه‌شده از ۱۳ سطح موجود در استاندارد ISO27002:2005 می‌باشد که برخی از آن‌ها با سایر استانداردها همپوشانی دارد.

جدول (۴): مدل ISFAM [۳۶]

Focus Area:	Maturity Level:	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational														
1. Risk Management					A		B		C			D		
2. Policy Development				A		B						C		
3. Organizing Information Security			A			B					C		D	
4. Human Resource Security					A		B		C		D			
5. Compliance					A		B						C	
Technical														
6. Identity and access management						A		B		C		D		
7. Secure software development						A		B			C		D	
Organizational and Technical														
8. Incident management				A			B			C			D	
9. Business Continuity Management					A		B		C			D		E
10. Change Management					A		B		C		D			
Support														
11. Physical and environmental security							A		B		C			D
12. Asset Management				A				B			C		D	
13. Architecture					A		B			C		D		
		Design					Implementation		Operational Effectiveness			Monitoring		

[1] Spruit and Roeling
[2] Good Practice of the Information Security Forum
[3] KPIs (Key Performance Indicators)
[4] Operational Effectiveness

۵-۷- National Initiative for Cybersecurity Education – Capability Maturity Model (NICE)

مدل NICE برگرفته از مفهوم «ابتکار یکپارچه امنیت سایبری ملی[1]» و همچنین دستورالعمل‌های توسعه آموزش‌های سایبری ایجاد شده است. یکی از اهداف این مدل به‌کارگیری کارکنان با دانش فنی در امنیت سایبری می‌باشد. برای رسیدن به این اهداف، سه مؤلفه در این مدل دنبال می‌گردد، ۱) ایجاد ساختار امنیت سایبری کارکنان ۲) مدیریت استعدادها ۳) نقش برنامه‌ریزی کارکنان [۲۵].

مدل NICE دارای سه سطح بلوغ می‌باشد، این سطوح در جدول (۵) بررسی شده است.

جدول (۵): سطوح بلوغ مدل NICE [۲۵]

سطح	توصیف
سطح محدود	ابتدایی‌ترین سطح است که یک سازمان را با حوزه‌هایی از قابلیت برنامه‌ریزی نیروی کار امنیت سایبری به تصویر می‌کشد. می‌توان از ویژگی‌های این سطح به تلاش برای استقرار محدود فرآیندها، عدم آگاه‌سازی، فاقد داده‌های ساختاریافته و روش‌های تجزیه‌وتحلیل اشاره کرد.
سطح در حال پیشرفت	برخی از جنبه‌های برنامه‌ریزی نیروی کار امنیت سایبری را در سراسر سازمان توصیف می‌کند، در این سطح برای ایجاد زیرساخت‌های مناسب تلاش می‌شود.
سطح بهینه‌شده	حوزه‌های کلیدی قابلیت‌های برنامه‌ریزی نیروی کار در یک سازمان را به تصویر می‌کشد که به‌طور کامل توسعه یافته است و با سایر فرآیندهای تجاری یکپارچه شده‌اند، در نتیجه می‌توانند سطوح مختلف تحلیل نیروی کار و حجم کار را پشتیبانی کنند که نتایج آن دربرگیرنده تصمیم‌گیری کوتاه‌مدت و بلندمدت برای نیروی کار امنیت سایبری می‌باشد.

آخرین ویرایش این مدل مربوط به آگوست سال ۲۰۱۷ می‌باشد که فعالیت‌های کلیدی را در سه حوزه اصلی، به شرح ذیل تقسیم‌بندی می‌کند:

۱) تجزیه‌وتحلیل و فرایندها: این مرحله بیانگر آن دسته از فعالیت‌های مرتبط با مراحل واقعی سازمان می‌باشد که برای اجرای برنامه‌ریزی برای نیروی کار و نحوه ادغام این مراحل با سایر فرآیندهای مهم تجاری در سراسر سازمان است.

۲) حکمرانی یکپارچه[2]: نمایانگر آن دسته از فعالیت‌هایی است که با ایجاد ساختارهای حاکمیتی، توسعه و ارائه مشورت‌هایی جهت تصمیم‌گیری مرتبط هستند. این موارد برای راهبرد کلی برنامه‌ریزی برای نیروی کار و چشم‌انداز سازمان و همچنین تعیین مسئولیت، ارتقاء یکپارچگی و صدور دستورالعمل‌های برنامه‌ریزی است.

۳) آموزش متخصصین و به‌کارگیری فناوری: نشان‌دهنده فعالیت‌های مرتبط با ایجاد یک گروه حرفه‌ای از برنامه‌ریزان نیروی کار در یک سازمان است. به‌کارگیری فناوری، فعالیت‌های مربوط به دسترسی و استفاده از سیستم‌های داده را نشان می‌دهد.

۵-۸- Department Of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC)

گواهینامه مدل بلوغ امنیت سایبری (CMMC) در سال ۲۰۲۰ توسط وزارت دفاع ایالات متحده ایجاد شد. هدف ایجاد این مدل عدم اعتماد به ارزیابی مدل‌های بلوغ امنیت عنوان گردید. متقاضیان دریافت این گواهینامه شرکت‌های تجاری یا سازمان‌های دولتی هستند. این مدل بر پایه استانداردهای NIST SP 800-I7I, NIST SP 800- 53, ISO27001, ISO 27032, AIA NAS9933 می‌باشد. شاخص‌های مورد اهمیت در این مدل در جدول (۶) مشخص شده است [۳۷ و ۳۸].

جدول (۶): سطوح و دامنه مدل CMMC [۳۸]

سطح	دامنه/شاخص
سطح یک، اصول اولیه سایبری	کنترل دسترسی
	امنیت شخصی
	مدیریت دارایی
سطح دو، رعایت نسبی اصول سایبری	امنیت فیزیکی
	ممیزی و پاسخگویی
	بازیابی
	آگاهی و آموزش
سطح سه، رعایت اصول سایبری	مدیریت ریسک
	مدیریت پیکربندی
	مدیریت امنیت
سطح چهار، فعال	شناسایی و احراز هویت
	آگاهی موقعیتی
	پاسخ به رویدادها
	حفاظت از ارتباطات و سیستم‌ها
سطح پنج، پیشرفته	نگهداری
	یکپارچگی اطلاعات سیستم
	محافظت از رسانه

مدل CMMC دارای پنج سطح به شرح ذیل می‌باشد:

سطح یک، اصول اولیه سایبری[3]: در این گام کنترل دسترسی، امنیت فردی و مدیریت دارای موردتوجه قرار می‌گیرد.

سطح دو، رعایت نسبی اصول سایبری: در این مرحله امنیت فیزیکی، ممیزی و پاسخگویی[4]، بازیابی، آگاهی و آموزش موردتوجه قرار می‌گیرد.

سطح سه، رعایت اصول سایبری: در این گام مدیریت

[1] CNCI (Comprehensive National Cybersecurity Initiative)
[2] Integrated Governance
[3] Basic Cyber Hygiene
[4] Audit and Accountability

ریسک، مدیریت پیکربندی و مدیریت امنیت موردتوجه قرار می‌گیرد.

سطح چهار، فعال: در این مرحله شناسایی و احراز هویت، آگاهی موقعیتی، پاسخ به رویدادها و حفاظت از ارتباطات و سیستم‌ها موردتوجه قرار می‌گیرد.

سطح پنج، پیشرفته: در این مرحله نگهداری، یکپارچگی اطلاعات و سیستم و محافظت از رسانه[1] موردتوجه قرار می‌گیرد.

۵-۹- The Cybersecurity Focus Area Maturity (CYSFAM)

مدل CYSFAM توسط بیلگ یگیت اوزکان و دیگران[2] توسعه یافته است، این مدل برای ارزیابی قابلیت‌های امنیت سایبری و تعیین سطح فعلی بلوغ امنیت سایبری مورداستفاده قرار می‌گیرد. این مدل دارای یک ابزار ارزیابی متشکل از ۱۴۴ سؤال می‌باشد که بنا به ادعای توسعه‌دهندگان آن، می‌توان یک سازمان را در عرض چهار ساعت مورد ارزیابی قرار داد [۳۹].

مدل CYSFAM در اوایل سال ۲۰۲۱ انتشار یافت، این مدل دارای ۱۱ سطح بلوغ است که به دو مرحله بلوغ تقسیم می‌شود، این مراحل به دو دسته فنی و سازمانی برای تسهیل درک و مدیریت بهتر گروه‌بندی می‌شوند (جدول ۷).

مدل مذکور برگرفته از استانداردهای ISO/IEC 27032, ISO/IEC 27001, ISO/IEC 27033, ISO/IEC 27034, ISO/IEC 27035 است.

۴-۱۰- Cybersecurity Capability Maturity Model (C2M2)

مدل C2M2 توسط وزارت انرژی ایالات متحده توسعه یافته است. آخرین ویرایش این مدل نسخه (۲,۰) است که در جولای سال ۲۰۲۱ منتشر شده است.

این مدل در ۱۰ حوزه سازمان‌دهی شده است و هر دامنه یک گروه‌بندی منطقی از اقدامات امنیت سایبری است. تمرینات در هر حوزه به اهدافی سازمان‌دهی می‌شوند که نشان‌دهنده دستاوردهای درون دامنه هستند. دامنه‌ها و اهداف در جدول (۹) برشمرده شده‌اند. همچنین این مدل متشکل از چهار سطوح شاخص بلوغ[3] به شرح جدول (۸) است. محتوای این مدل در سطح بالایی از انتزاع ارائه شده است، به‌طوری‌که می‌تواند توسط سازمان‌ها در انواع، ساختارها و اندازه‌های مختلف مورداستفاده قرار گیرد [۸].

[1] Media
[2] B. Y. Ozkan and Others
[3] MIL (Maturity Indicator Levels)

جدول (۷): مدل CYSFAM [۳۸]

CYSFAM	Maturity Level												
Focus Area	0	1	2	3	4	5	6	7	8	9	10	11	12
Technical													
Server Protection					A					C	D		
End-user Controls					A		B		C			D	
Network Security				A		B		C			D		
Application Security					A		B		C			D	
Cryptography						A	B		C			D	
Mobile Security					A	B		C			D		
Vulnerability Management					A	B		C			D		
Organizational													
Social Engineering Controls				A		B		C			D		
Cybersecurity Incident Management				A			B		C			D	
Cybersecurity Awareness				A		B		C			D		E
Cybersecurity Governance		A	B					C	D				

جدول (۸): خلاصه ویژگی‌های سطوح شاخص بلوغ مدل C2M2 [۸]

سطح	ویژگی‌ها
MIL0	عدم انجام تمرین‌ها
MIL1	انجام اقدامات اولیه به‌صورت موردی
MIL2	**ویژگی‌های مدیریت:** -مستندسازی روش‌ها -فراهم آوردن منابع کافی برای پشتیبانی از فرایندها **ویژگی رویکرد:** -در این مرحله تمرینات کامل‌تر و پیشرفته‌تر از سطح MIL1 هستند.
MIL3	**ویژگی‌های مدیریت:** - فعالیت‌ها توسط خط مش‌ها هدایت می‌شوند. -کارکنانی که تمرینات را انجام می‌دهند، مهارت‌ها و دانش کافی دارند -مسئولیت، پاسخگویی و اختیار برای انجام اقدامات تعیین شده است -اثربخشی فعالیت‌ها ارزیابی و پیگیری می‌شود. **ویژگی رویکرد:** -تمرینات کامل‌تر و پیشرفته‌تر از سطح MIL2 هستند.

جدول (۹): شاخص‌ها و اهداف مدل C2M2 [۸]

شاخص	اهداف
مدیریت دارایی، تغییر و پیکربندی (Asset)	مدیریت موجودی دارایی، مدیریت پیکربندی دارایی، مدیریت تغییرات در دارایی‌ها
مدیریت تهدید و آسیب‌پذیری (Threat)	تهدیدها شناسایی شده و به آن‌ها پاسخ داده می‌شود، کاهش آسیب‌پذیری‌های امنیت سایبری
مدیریت ریسک (Risk)	ایجاد مدیریت ریسک امنیت سایبری، استراتژی
مدیریت هویت و دسترسی (Access)	ایجاد و حفظ هویت، کنترل دسترسی
آگاهی از موقعیت (Situation)	ثبت وقایع (Logging)، نظارت
پاسخ به حوادث و رویدادها، تداوم عملیات (Response)	شناسایی رویدادهای امنیت سایبری، واکنش به حوادث، تداوم برنامه‌ریزی
مدیریت ریسک شخص ثالث (Third-Parties)	ایجاد و حفظ کنترل‌ها برای مدیریت ریسک‌های سایبری ناشی از تأمین‌کنندگان و سایر اشخاص ثالث، متناسب با اهمیت زیرساخت‌های حیاتی و اهداف سازمانی.
مدیریت نیروی کار (Workforce)	تعیین مسئولیت‌های امنیت سایبری، کنترل چرخه حیات نیروی کار، توسعه نیروی کار امنیت سایبری، افزایش آگاهی نیروهای کار در حوزه امنیت سایبری
معماری امنیت سایبری (Architecture)	ایجاد و حفظ ساختار معماری امنیت سایبری سازمان، شامل کنترل‌ها، فرآیندها، فناوری‌ها و سایر عناصر، متناسب با اهمیت زیرساخت‌های حیاتی و اهداف سازمانی.
مدیریت برنامه‌های امنیت سایبری (Program)	ایجاد و حفظ یک برنامه امنیت سایبری سازمانی، تدوین برنامه‌ریزی راهبردی و حمایت مالی برای فعالیت‌های امنیت سایبری سازمان، به‌گونه‌ای که اهداف امنیت سایبری را هم با اهداف راهبردی سازمان و هم با اهمیت زیرساخت‌های حیاتی همسو می‌کند.

جدول (۱۰): مقایسه مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات، موردبررسی در این پژوهش [مؤلفین]

ردیف	نام مدل	شاخص‌های تدوین شده	سطوح/مراحل تعریف شده	سال انتشار/ آخرین ویرایش	پدید آورندگان
۱	CCSMM	شناسایی تهدیدات، اشتراک اطلاعات، تکنولوژی، آموزش، سنجش	سطح یک: ابتدایی / سطح دو: پیشرفته / سطح سه: خود ارزیابی/ سطح چهار: یکپارچه سازی/ سطح پنج: پیشرو	ژانویه ۲۰۰۷	وزارت امنیت داخلی آمریکا
۲	ISMM	نظارت بر سیستم‌ها، سیاست‌ها و روندها، امنیت انطباق، حوادث امنیتی، معماری امنیتی، کنترل پیشگیرانه و اصلاحی	سطح یک: عدم پذیرش/ سطح دو: پذیرش اولیه/ سطح سه: پذیرش ثانویه/ سطح چهار: قابل پذیرش/ سطح پنج: پذیرش کامل	ژانویه ۲۰۱۱	Dr. Malik F. Saleh
۳	E-Government ISMM	اهداف امنیت اطلاعات، محیط خطر امنیتی، فرایندها و سیاست‌های امنیتی، فرایندهای کاهش ریسک، آگاهی	سطح یک: تعریف نشده/ سطح دو: تعریف شده/ سطح سه: مدیریت شده/ سطح چهار: تحت نظارت / سطح پنج: بهینه شده	آگوست ۲۰۱۱	Geoffrey Karokola and Others
۴	5S2IS	سیاست‌های امنیتی، سازماندهی امنیت اطلاعات، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی، مدیریت عملیات وارتباطات، کنترل دسترسی، نگهداری و توسعه، کسب سیستم اطلاعاتی، مدیریت حوادث امنیتی اطلاعات، مدیریت تداوم کسب و کارانطباق	سطح یک: تعهد/ سطح دو: اصول/ سطح سه: نظارت/ سطح چهار: بهبود بخشی/ سطح پنج: استقرار	جان ۲۰۱۱	Alan Gillies
۵	GAIA-MLIS	سیاست‌ها و فرایندها، آگاهی، رخدادهای امنیتی، مدیریت دسترسی و هویت، کنترل دسترسی، امنیت فیزیکی، مدیریت شبکه، رمزنگاری داده، طبقه بندی داده	سطح صفر: بدون تضمین/ سطح یک: تضمین اولیه/ سطح دو: تضمین معین/ سطح سه: آیمتی نسبی/ سطح چهار: تضمین کامل	ژانویه ۲۰۱۴	Roger W. Coelho and Others
۶	ISFAM	مدیریت ریسک، توسعه سیاست‌ها، سازماندهی امنیت اطلاعات، امنیت منابع انسانی، انطباق، مدیریت دسترسی و هویت، توسعه امنیت نرم افزار، مدیریت حوادث، مدیریت تداوم کسب و کار، مدیریت تغییر، امنیت فیزیکی و محیطی، مدیریت دارایی، معماری	مرحله یک: طراحی/ مرحله دو: پیاده سازی/ مرحله سه: اثربخشی عملیاتی/ مرحله چهار: نظارت	ژانویه ۲۰۱۴	Marco Spruit and Martijn Röling
۷	NICE	برنامه ریزی نیروی کار، فرایند کسب و کار، مدیریت ریسک، ساختارهای حکمرانی، فعال سازی تکنولوژی	سطح محدود/ سطح در حال پیشرفت / سطح بهینه شده	آگوست ۲۰۱۷	یکشنبه امنیت ملی، توسط رئیس جمهور آمریکا جرج بوش (۲۰۰۸)
۸	CMMC	کنترل دسترسی، امنیت شخصی، مدیریت دارایی، امنیت فیزیکی، ممیزی و پاسخگویی، بازیابی، آگاهی و آموزش، مدیریت ریسک، مدیریت پیکربندی، مدیریت امنیت، شناسایی و احراز هویت، آگاهی از موقعیت، پاسخ به رویدادها، حفاظت از ارتباطات و سیستم‌ها، نگهداری، یکپارچگی اطلاعات سیستم، محافظت از رسانه	سطح یک، اصول اولیه سایبری/ سطح دو، رعایت نسبی اصول سایبری/ سطح سه، رعایت اصول سایبری/ سطح چهار، فعال/سطح پنج، پیشرفته	سپتامبر ۲۰۲۰	وزارت دفاع ایالات متحده
۹	CYSFAM	محافظت از سرور، کنترل‌های کاربر، امنیت شبکه، امنیت برنامه‌های کاربردی، رمزنگاری، امنیت تجهیزات قابل حمل، مدیریت آسیب پذیری، کنترل مهندسی اجتماعی، مدیریت حوادث امنیت سایبری، آگاهی امنیت سایبری، حکمرانی سایبری	سطح یک: فنی / سطح دو: سازمانی	فوریه ۲۰۲۱	Bilge Yigit Ozkan and Others
۱۰	C2M2	مدیریت دارایی، تغییر و پیگردی، مدیریت تهدید و آسیب پذیری، مدیریت ریسک، مدیریت هویت و دسترسی، آگاهی از موقعیت، پاسخ به حوادث و رویدادها، تداوم عملیات، مدیریت ریسک شخص ثالث، مدیریت نیروی کار، معماری امنیت سایبری، مدیریت برنامه‌های امنیت سایبری	سطح: MIL0/ سطح: MIL1 / سطح: MIL2/ سطح: MIL3	جولای ۲۰۲۱	وزارت انرژی ایالات متحده

۵- نتایج و بحث

پژوهش صورت گرفته نشان می‌دهد که مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات شباهت قابل‌توجهی به یکدیگر دارند؛ لذا با بررسی تطبیقی و مقایسه‌ای بین این مدل‌ها ۹۳ شاخص احصا گردید (این شاخص‌ها در جدول (۱۲) پیوست درج گردیده است).

بررسی این شاخص‌ها نشان می‌دهد برخی از شاخص‌های احصا شده دارای همپوشانی با سایر شاخص‌ها می‌باشند، بنابراین در این پژوهش شاخص‌های دارای همپوشانی در ۱۷ گروه دسته‌بندی شده (جدول ۱۴ در پیوست) و گروه‌های ایجاد شده در جدول (۱۱) ارائه شده است.

به‌علاوه در جدول (۱۰) مقایسه‌ای بین مدل‌های موردبررسی در این پژوهش صورت گرفته است. این مقایسه نشان می‌دهد مدل C2m2 به‌طور جامع شاخص‌های مرتبط با امنیت زیرساخت‌های حیاتی را در بردارد، همچنین شاخص‌های معرفی‌شده در این مدل ارتباط نزدیکی با یافته‌های این پژوهش دارد به‌نحوی‌که شاخص‌های معرفی‌شده در این مدل جزو ۱۰ شاخص برتر شناسایی شده (جدول ۱۲) در این پژوهش است.

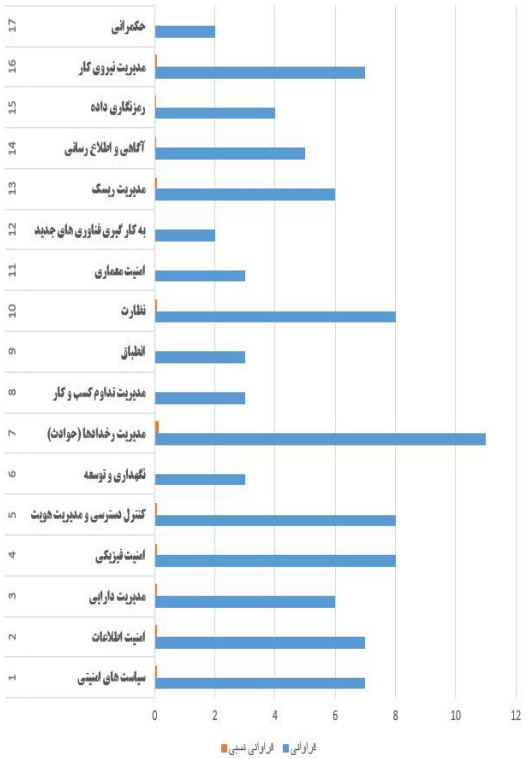
نتایج ذیل بر اساس جدول (۱۱)، به لحاظ فراوانی و اهمیت شاخص‌ها به دست آمده است:

- شاخص مدیریت رخدادها با فراوانی ۱۱، توانسته است جایگاه اول را به دست آورد ازاین‌رو، این شاخص موردتوجه‌ترین شاخص در ایمن‌سازی زیرساخت‌های حیاتی تلقی می‌گردد.
- شاخص‌های امنیت فیزیکی، نظارت و کنترل دسترسی و مدیریت هویت، به‌طور مشترک توانسته‌اند با فراوانی هشت، در جایگاه‌های بعدی قرار گیرند.
- سیاست‌های امنیتی، امنیت اطلاعات و مدیریت نیروی کار با فراوانی هفت، به‌طور مشترک در موضع بعدی قرار می‌گیرند.
- شاخص‌های مدیریت دارایی و مدیریت ریسک، به‌طور مشترک با فراوانی شش در مقام بعد قرار دارند.
- شاخص آگاهی و اطلاع‌رسانی با فراوانی پنج، در جایگاه بعد قرار دارد.
- شاخص رمزنگاری داده با فراوانی چهار در جایگاه بعدی قرار دارد.
- شاخص‌های نگهداری و توسعه، مدیریت تداوم کسب‌وکار، انطباق و امنیت معماری با فراوانی سه، در موضع بعدی قرار دارد.
- شاخص‌های به‌کارگیری فناوری‌های جدید و حکمرانی با فراوانی دو، در جایگاه آخر قرار دارند.

با توجه به نتایج به‌دست‌آمده و بر اساس جدول (۱۱)، در ادامه نمودار گروه‌بندی شاخص‌ها بر اساس فراوانی و فراوانی نسبی ارائه می‌شود.

جدول (۱۱): گروه‌بندی شاخص‌های دارای همپوشانی [مؤلفین]

ردیف	گروه‌بندی	فراوانی	فراوانی نسبی
۱	سیاست‌های امنیتی	۷	۰/۰۸
۲	امنیت اطلاعات	۷	۰/۰۸
۳	مدیریت دارایی	۶	۰/۰۶
۴	امنیت فیزیکی	۸	۰/۰۹
۵	کنترل دسترسی و مدیریت هویت	۸	۰/۰۹
۶	نگهداری و توسعه	۳	۰/۰۳
۷	مدیریت رخدادها (حوادث)	۱۱	۰/۱۲
۸	مدیریت تداوم کسب‌وکار	۳	۰/۰۳
۹	انطباق	۳	۰/۰۳
۱۰	نظارت	۸	۰/۰۹
۱۱	امنیت معماری	۳	۰/۰۳
۱۲	به‌کارگیری فناوری‌های جدید	۲	۰/۰۲
۱۳	مدیریت ریسک	۶	۰/۰۶
۱۴	آگاهی و اطلاع‌رسانی	۵	۰/۰۵
۱۵	رمزنگاری داده	۴	۰/۰۴
۱۶	مدیریت نیروی کار	۷	۰/۰۸
۱۷	حکمرانی	۲	۰/۰۲
جمع		۹۳	۱



نمودار (۳): گروه‌بندی شاخص‌ها بر اساس فراوانی و فراوانی نسبی [مؤلفین]

بر اساس اطلاعات به‌دست‌آمده در این پژوهش، مهم‌ترین شاخص‌های شناسایی شده به شرح جدول ذیل است:

جدول (۱۲): مهم‌ترین شاخص‌های احصا شده [مؤلفین]

ردیف	نام شاخص	درجه اهمیت
۱	مدیریت رخدادها (حوادث)	۱۱
۲	امنیت فیزیکی	۸
۳	کنترل دسترسی و مدیریت هویت	۸
۴	نظارت	۸
۵	سیاست‌های امنیتی	۷
۶	امنیت اطلاعات	۷
۷	مدیریت نیروی کار	۷
۸	مدیریت دارایی	۶
۹	مدیریت ریسک	۶
۱۰	آگاهی و اطلاع‌رسانی	۵
۱۱	رمزنگاری داده	۴
۱۲	نگهداری و توسعه	۳
۱۳	مدیریت تداوم کسب‌وکار	۳
۱۴	انطباق	۳
۱۵	امنیت معماری	۳
۱۶	به‌کارگیری فناوری‌های جدید	۲
۱۷	حکمرانی	۲

۶- نتیجه‌گیری

طی پیشرفت بشر در عصر اطلاعات، وابستگی به زیرساخت‌های ملی بیش از گذشته اهمیت یافته است. به خطر افتادن امنیت زیرساخت‌های حیاتی می‌تواند موجب اختلال در کارکرد بخش‌های گوناگون نظیر دولت، اقتصاد و مسیر عادی زندگی‌مان شوند. با ایجاد آسیب و اختلال در زیرساخت‌های ملی، ممکن است زیان‌های فاجعه‌باری در زمینه‌های تلفات انسانی، تخریب اموال، خسارت‌های اقتصادی و از دست دادن اعتماد عمومی ایجاد شود. در این پژوهش ۱۰ مورد از موردتوجه‌ترین مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات به همراه مهم‌ترین ویژگی‌ها و ابعاد ایمن‌سازی مورد واکاوی قرار گرفته است، در نهایت ۹۳ شاخص برای ایمن‌سازی سایبری زیرساخت‌های حیاتی کشور احصا گردید و شاخص‌های دارای همپوشانی و شباهت کارکردی در ۱۷ گروه دسته‌بندی و بر اساس فراوانی مهم‌ترین آن‌ها مشخص گردیدند (نمودار ۳). این نتایج می‌توانند علاوه بر استفاده در طراحی مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور، منجر به برنامه‌ریزی هوشمندانه توسط حاکمیت، افزایش قدرت سایبری و ایجاد مواضع فعالانه در برابر حملات سایبری گردد.

۶-۱- پیشنهادها

به جهت اهمیت زیرساخت‌های حیاتی و وابستگی این زیرساخت‌ها به فناوری اطلاعات، همواره تهدیدات سایبری در این حوزه وجود دارد؛ لذا پیشنهاد می‌شود زیرساخت‌های حیاتی بر اساس اهمیت اولویت‌بندی گردند و برای این زیرساخت‌ها دستورالعملی مشتمل بر شاخص‌های احصا شده در این پژوهش تدوین گردد، همچنین می‌توان با استفاده از روش‌های تجزیه‌وتحلیل خوشه‌ای[1]، نسبت به ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور اقدام نمود.

۷- مراجع

[1] J. Nye, & W. Jisi, "The Rise of China's Soft Power and Its Implications for the United States," in Richard Rosecrance and Gu Guoliang, Power and Restraint: A Shared Vision for the U.S.–China Relationship (New York: Public Affairs), pp. 28-30, 2006.

[2] M. Whitman, & H. Mattord "Roadmap to Information Security: For IT and Infosec Managers," Cengage Learning, 1st edition, 2011.

[3] Mcafee, 2014, "Mcafee-report-global-cost-cybercrime," https://www.csis.org/events/2014-mcafee-report-global-cost-cybercrime

[4] H.R. Javaheri & Others, "Improvement in the Ransomwares Detection Method with New API Calls Feature," In Journal of Electronical & Cyber Defence, Vol. 8, pp. 107-118, 2021.

[5] ITU "Corporate Annual Report 2008 ", https://www.itu.int/osg/csd/stratplan/AR2008_web.pdf

[6] ISO/IEC 27032:2012, "Information technology – Security techniques – Guidelines for cybersecurity", https://www.iso.org/standard/44375.html

[7] K. Shoushian and Others, "Probabilistic Modeling of Obfuscated Multi- Stage Cyber Attacks", In Journal of Electronical & Cyber Defence, Vol 8, 2020

[8] U.S Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response," CyberSecurity Capability Maturity Model (C2M2)" 2021

[9] H. Khazaei, "Passive defense from the point of view of the Supreme Leader and the Commander-in-Chief", vol 36, pp. 151-190, 2016 (In Persian)

[10] R. Shabaninezhad and Others, "The Strategic Study of Reducing the Vulnerability of power Systems Against Electromagnetic Pulses", In Journal of Passive Defence, vol 3, pp. 71-86, 2021 (In Persian)

[11] M. Miryousefi, R. Ghaffarpour "New Critical Infrastructure Protection Strategies", In Journal of Passive Defence, vol 3, pp. 1-14, 2021 (In Persian)

[1] Cluster Analysis

[12] A, Gharamaleki "Methodology of religious studies", Razavi University of Sciences Publisher, 2006 (In Persian)

[13] F. Akhavan, R. Radfar, "a model for monitoring information security maturity", In Journal of Technology growth, Vol 64, 2021 (In Persian)

[14] A. Afshar & Others, "Review of the Types of Strategies to Improve Security of Industrial Control Systems and Critical Infrastructure", In Journal of Passive Defence, Vol 2, 2018 (In Persian)

[15] Y. Bilge, S. Marco, "A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures", In Springer Nature Switzerland AG Conference paper, 2019

[16] K. Bilge and Others," A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness", In international journal of critical infrastructure protection, ScinceDirect, Elsevier, pp. 47 – 59 – 2019

[17] A. Marcelo and Others, "Comparative Study of Cybersecurity Capability Maturity Models" In Springer International Publishing AG – pp. 110-113 – 2017

[18] A. Aliyu and Others, "A Holistic Cybersecurity Maturity assessment framwork for higher education institution in United Kingdom" In Applied Sciences, 2020

[19] M. Ide, "cybersecurity capability maturity model for critical information technology infrastructure among nigeria financial organizations" PhD. Thesis, Teknologi Malaysia Univ, 2019

[20] M. Aghaei and Others, "a logical conceptual model for classifying critical infrastructure cyber threats" In Journal of National Security, Vol 2, 2019 (In Persian)

[21] J. Bridget, "Information Security Maturity Model for Healthcare Organizations in the United State", Ph.D. Thesis, Portland State Univ, 2021

[22] B. Yigit and Others, "The Cybersecurity Focus Area Maturity (CYSFAM) Model", In Journal Cybersecure Privacy, pp. 119-139, 2021

[23] A. Kavand, V. Hakimzadeh, "Identifying, evaluating and classifying high-risk infrastructures", Bostan Publisher, 2020 (In Persian)

[24] H. Zarghani, H. Azami, "Analysis of security considerations in planning and location of military centers and bases with emphasis on Khorasan Razavi province", In Journal of Planning and arranging space, Vol 15, pp. 112-127, 2016

[25] US Department of Homeland Security, "Cybersecurity Capability Maturity Model: Version 1.0. White paper, Department of Homeland Security", 2014.

[26] ITU "Guide to developing a national cybersecurity strategy 2end edition", https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf, 2021

[27] A. N. Singh, M.P. Gupta, A. Ojha, "Identifying critical infrastructure sectors and their dependencies: An Indian scenario", International Journal of Critical Infrastructure Protection, 7(2), pp.71–85.

[28] M.C Paulk and Others, "Capability Maturity Model version 1.1 IEEE Softw". In Los Alamitos Journal, Vol 10, pp. 18–27, 1993

[29] U.S, Department of Defence, "Cybersecurity Maturity Model Certification (CMMC)", DoD, 2020

[30] G.B, White, "The community cyber security maturity model". In IEEE International Conference on Technologies for Homeland Security, HST, pp.173–178, 2007

[31] M. Saleh, "Information Security Maturity Model", In International Journal of Computer Science and Security (5), pp.316-337, 2011

[32] G. Karokola, S. Kowalski & L. Yngström, "Towards an Information Security Maturity Model for Secure e-Government Services: A Stakeholders View", In Proceedings of the 5th HAISA2011, Conference, pp. 58–73, 2011

[33] A. Gillies, "Improving the quality of information security management systems with ISO27000", In the TQM Journal, 23(4), pp.367–376, 2011, http://doi.org/10.1108/17542731111139455

[34] S.W. Humphrey, "Managing the Software Process", In Omega International Journals of Management Science, Vol 16, 1989

[35] R.W. Coelho, G.F. Lemes, "GAIA-MLIS: A Maturity Model for Information Security". In SECURWARE Journal vol 61, pp.50–55, 2014

[36] M. Spruit and M. Roeling, "ISFAM: the information security focus area maturity model". In Proceedings of the European Conference on Information Systems (ECIS), 2014

[37] U.S, Department of Defence, "Cybersecurity Maturity Model Certification (CMMC)", DoD, 2020

[38] United States Agency for International Development (USAID), "understanding cybersecurity maturity models within the context of energy regulation", 2020

[39] B. Y. Ozkan, S. Lingen, M. Spruit, "The Cybersecurity Focus Area Maturity (CYSFAM) Model" In Journal of Cybersecurity and Privacy, Vol 1, pp. 119-139, 2021

[40] British Standards Institution, Moving from ISO 27001:2005 to ISO 27001:2013, BSI, London, 2013

[41] W. Zechariah, J. Shi, "Business Continuity Management System: A Complete Guide to Implementing ISO 22301 1st Edition", Kogan Page Publisher, 2014.

۸- پیوست

جدول (۱۲): شاخص‌های احصا شده از مدل‌های موردبررسی در این پژوهش [مؤلفین].

ردیف	شاخص	مدل مرجع
1	Security Policy	5S2IS
2	Organization information security	
3	Asset management	
4	Human resource security	
5	Physical security	
6	Communication and operation management	
7	Access control	
8	Development and maintenance	
9	Information system acquisition	
10	Information security incident management	
11	Business continuity management	
12	compliance	
13	monitoring the systems	ISMM
14	policies and procedures	
15	compliance security	
16	Security incidents	
17	security architecture	
18	preventive, detective and corrective control	
19	Threats addressed	CCSMM
20	Information sharing	
21	Technology	
22	training	
23	test	
24	Information Security Targets	E-Governance ISMM
25	security risk environment	
26	Security policies and process	E-Governance ISMM
27	risk reduction processes	
28	awareness	
29	processes and policies	GAIA-MLIS
30	awareness	
31	security incident	
32	IAM (identity and access management)	
33	access control	
34	Physical security	
35	Network management	
36	Data encryption	
37	Data classification	
38	Risk management	ISFAM
39	Policy development	
40	Organizing information security	
41	Human resource security	
42	Compliance	
43	IAM (identity and access management)	
44	Secure software development	
45	Incident management	
46	Business continuity management	
47	Change management	
48	Physical and environmental security	
49	Asset management	
50	architecture	
51	Asset, Change, and Configuration Management (ASSET)	C2M2
52	Threat and Vulnerability Management (THREAT)	
53	Risk Management (RISK)	
54	Identity and Access Management (ACCESS)	
55	Situational Awareness (SITUATION)	
56	Event and Incident Response, Continuity of Operations (RESPOND)	
57	Third-Party Risk Management (THIRD-PARTIES)	
58	Workforce Management (WORKFORCE)	
59	Cybersecurity Architecture (ARCHITECTURE)	
60	Cybersecurity Program Management (PROGRAM)	
61	Work force planning	NICE
62	Business process	
63	Risk management	
64	governance structures	
65	Enabling Technology	
66	Server protection	CYSFAM
67	End user's controls	
68	Network security	
69	Application security	
70	Cryptography	
71	Mobile security	
72	Vulnerability management	
73	Social engineering controls	
74	Cybersecurity incident management	
75	Cybersecurity awareness	
76	Cybersecurity governance	CYSFAM
77	Access control	CMMC
78	Personal security	
79	Asset Management	
80	Physical security	
81	Audit and Accountability	
82	Recovery	
83	Awareness and training	
84	Risk management	
85	Configuration management	
86	Security management	
87	Identification and authentication	
88	Situational awareness	
89	Incident response	
90	Systems and communications protection	
91	Maintenance	
92	System and information integrity	
93	Media protection	

جدول (۱۳): اهداف شاخص‌های گروه‌بندی‌شده [مؤلفین].

ردیف	گروه بندی شاخص ها	اهداف
۱۰	نظارت	ایجاد و حفظ برنامه‌ها، رویه‌ها و فناوری‌ها برای شناسایی، تجزیه و تحلیل آسیب پذیری ها مرتبط با زیرساخت های حیاتی[۸].
۱۱	امنیت معماری	ایجاد و حفظ ساختار و رفتار معماری امنیت سایبری سازمان، شامل کنترل‌ها، فرآیندها، فناوری‌ها و سایر عناصر[۸].
۱۲	به کار گیری فناوری های جدید	به کارگیری فناوری های جدید در صورتی اتفاق می افتد که این موارد در سطح یک سازمان وجود داشته باشد: *یک پورتال وب یا قابلیت مقایسه و دسترسی به طیف کاملی از سیستم های داده، ابزارهای تجزیه و تحلیل و مدل های مورد استفاده. *روش‌های خودکار برای ترکیب داده‌ها از سیستم‌های مختلف برای تجزیه و تحلیل و کاهش پردازش دستی وجود داشته باشد. *سیستم‌های داده معتبر، ابزارهای تحلیل و مدل‌ها در برنامه‌های مدرن و پایدار ساخته شده باشد که بتواند توسط طیف گسترده‌ای از کارکنان، صرف نظر از مهارت فنی، استفاده شوند[۲۴].
۱۳	مدیریت ریسک	راه اندازی و حفظ یک برنامه مدیریت ریسک سایبری سازمانی برای شناسایی، تجزیه و تحلیل و پاسخ به ریسک سایبری که سازمان در معرض آن است[۸]. این استراتژی باید رویکردی منسجم برای مدیریت ریسک تعریف کند تا به وسیله همه نهادهای دولتی و اپراتور های زیر ساخت های حیاتی داخلی دنبال شود. این رویکرد باید متجر به شناسایی دارایی های کلیدی و خدمات حیاتی برای کارکرد متناسب اقتصاد و جامعه، تهدیدات و ریسک های مرتبط با آن شود[۲۵].
۱۴	آگاهی و اطلاع رسانی	ایجاد و حفظ فعالیت‌ها و فناوری‌ها برای جمع آوری، نظارت، تجزیه و تحلیل، هشدار، گزارش، و استفاده از اطلاعات عملیاتی، امنیتی و تهدید، از جمله اطلاعات وضعیت و خلاصه از سایر حوزه‌های مدل، برای ایجاد آگاهی موقعیتی برای وضعیت عملیاتی سازمان و امنیت سایبری و همچنین اطلاع رسانی و آموزش های مرتبط با امنیت سایبری به کارمندان [۸].
۱۵	رمزنگاری داده	رمزگذاری و کنترل‌های رمزنگاری اغلب به‌عنوان یکی از مهمترین ابزار های امنیتی دیده می‌شوند. انتخاب نادرست فناوری‌ها و تکنیک‌های رمزنگاری یا مدیریت ضعیف مواد رمزنگاری (مانند کلیدها و گواهی‌ها) می‌تواند آسیب‌پذیری‌هایی را ایجاد کند[۳۹].
۱۶	مدیریت نیروی کار	برنامه‌ها، رویه‌ها، فن آوری‌ها و کنترل‌ها را برای ایجاد فرهنگ امنیت سایبری و اطمینان از شایستگی و پایش شایستگی مستمر پرسنل، متناسب با خطر زیرساخت‌های حیاتی و اهداف سازمانی[۸]. این استراتژی باید توسعه آموزش امنیت سایبری و طرح های توسعه مهارت را برای کارشناسان و افراد عادی در بخش های دولتی و خصوصی در نظر بگیرد[۲۵].امنیت. به خصوص زمانی که کارمندان و داده های تجاری اختصاصی شروع به ترکیب می کنند. همه چیز مربوط به هکرهای مخرب یا حملات باج افزار نیست. نکته اینجاست، و این چیزی است که ما تمایل داریم هنگام انجام روزهای کاری پرمشغله فراموش کنیم. کارکنان مستعد خطاهای انسانی هستند. بالاخره آنها انسان هستند، نه ماشین. قص داده ها به دلیل استفاده از گذرواژه های ضعیف، پیش فرض یا سرقت شده اتفاق می افتد. این ترسناک است، مهم نیست کسب و کار شما چقدر بزرگ یا کوچک است. همچنین شامل اشتباهات امنیتی «کارمند محور»، مانند ارسال اطلاعات حساس به شخص اشتباه، عدم دفع صحیح اطلاعات شرکت، پیکربندی نادرست سیستم‌های فناوری اطلاعات، لپ‌تاپ‌ها و دستگاه‌های تلفن همراه گم شده و دزدیده شده است[۳۹].
۱۷	حکمرانی	ایجاد و حفظ یک برنامه امنیت سایبری سازمانی که حکمرانی، برنامه‌ریزی استراتژیک و حمایت مالی را برای فعالیت‌های امنیت سایبری سازمان فراهم می‌کند به نحوی که اهداف امنیت سایبری را هم با اهداف استراتژیک سازمان و هم با خطر زیرساخت‌های حیاتی همسو می‌کند[۸] . این استراتژی باید خواستار توسعه یک طرح ملی اختصالی در مورد بحران های امنیت سایبری باشد [۸] .

ردیف	گروه بندی شاخص ها	اهداف
۱	سیاست های امنیتی	سیاست های امنیتی، سندی است که بیان می کند چگونه یک شرکت قصد دارد از دارایی های فیزیکی و فناوری اطلاعات (IT) خود محافظت کند. سیاست‌های امنیتی اسنادی هستند که با تغییر فناوری‌ها، آسیب‌پذیری‌ها و الزامات امنیتی به‌طور مداوم به‌روزرسانی شده و تغییر می‌کنند[۲۵].
۲	امنیت اطلاعات	سازماندهی امنیت اطلاعات در برگیرنده امنیت اطلاعات و اشتراک اطلاعات و به روزرسانی منظم آن ها می باشد[۳۵]. این استراتژی باید خواستار ایجاد مکانیز های اشتراک اطلاعات برای تبادل اطلاعات عملی و اطلاعات تهدید بین بخش های دولتی و خصوصی باشد. این استراتژی باید ایجاد سیاست های امنیت سایبری را برای نهادهای ملی مهم، مانند نهادهای دولتی و اپراتور های زیرساخت حیاتی، در میان دیگران ترغیب کند[۲۵]. اطمینان حاصل کنید که سیستم ها و حفاظت از یکپارچگی اطلاعات برای دارایی اطلاعاتی اختصاصی داده شده آنها وجود دارد[۳۹].
۳	مدیریت دارایی	مدیریت دارایی های IT و OT سازمان، از جمله سخت افزار و نرم افزار، و دارایی های اطلاعاتی [۸]. رویه‌های مدیریت تغییر برای کاهش خطر های ناشی از آسیب‌پذیری‌ها در زمان توسعه و طراحی می باشد که ممکن است به سیستم‌ها اجازه دهد پس از اعمال تغییرات در معرض خطر قرار گیرند[۳۹].
۴	امنیت فیزیکی	مناطق حساس باید توسط کنترل های ورودی مناسب محافظت شوند تا اطمینان حاصل شود که فقط پرسنل مجاز اجازه دسترسی دارند. این امر ممکن است با ابزار های بیومتریک و اسکن اثر انگشت کنترل شوند. کنترل بازدیدکنندگان نیز از اهمیت ویژه ای برخوردار خواهد بود و فرآیندهای مربوط به آن باید در نظر گرفته شود. باید توجه بیشتری به اعطای دسترسی به مناطقی که اطلاعات حساس یا طبقه بندی شده در آن ها پردازش یا ذخیره می شود، داده شود. در حالی که مناطقی که شامل تجهیزات کلیدی زیرساخت فناوری اطلاعات هستند به طور خاص باید تا حد زیادی محافظت شوند و دسترسی به آن‌هایی که واقعاً نیاز دارند محدود شود (از بعد فیزیکی)[۳۹].
۵	کنترل دسترسی و مدیریت هویت	ایجاد و مدیریت هویت برای اشخاصی که ممکن است به دارایی های سازمان دسترسی منطقی یا فیزیکی داشته باشند. کنترل دسترسی به دارایی های سازمان[۳۹].
۶	نگهداری و توسعه	سازمان ها باید محیط های توسعه ایمن را برای توسعه سیستم و تلاش های یکپارچه ایجاد کنند و به طور مناسب از آنها محافظت کنند که کل چرخه عمر توسعه سیستم را پوشش می دهد. محیط های توسعه باید محافظت شوند تا از توسعه و به روز رسانی مخرب یا تصادفی کد اطمینان حاصل شود که ممکن است آسیب پذیری ایجاد کند یا محرمانگی، یکپارچگی و در دسترس بودن را به خطر بیندازد. الزامات حفاظتی باید از ارزیابی ریسک، الزامات تجاری و سایر الزامات داخلی و خارجی از جمله قوانین، مقررات، قراردادهای قراردادی یا سیاست ها تعیین شود[۳۹].
۷	مدیریت رخدادها (حوادث)	برنامه‌ها، رویه‌ها و فن‌آوری‌ها را برای شناسایی، تجزیه و تحلیل، کاهش، پاسخ به و بازیابی رویدادها و حوادث امنیت سایبری و حفظ عملیات در طول حوادث امنیت سایبری، متناسب با خطر زیرساخت‌های حیاتی و اهداف سازمانی، ایجاد و ارائه می گردد[۸].
۸	مدیریت تداوم کسب و کار	مدیریت تداوم کسب‌وکار (BCMS) یک چارچوب مدیریتی است که سازمان را با توسعه استراتژی‌های تداوم کسب‌وکار برای انجام تعهدات تجاری و قانونی خود در طول یک حادثه آماده می‌کند. این در مورد بهینه سازی در دسترس بودن خدمات و حفظ عملکرد تجاری برای تضمین رشد آینده در بازار است[۴۰].
۹	انطباق	این استراتژی باید ایجاد مکانیزم های داخلی انطباق را ترویج کند. این مکانیزم ها باید برای جلوگیری، مقابله و کاهش اقدامات علیه محرمانگی، یکپارچگی و در دسترس بودن زیرساخت ها و دستگاه های ict و تهدید داده های کامپیوتری، مطابق با چارچوب حقوقی ذکر شده در بالا تنظیم شوند[۲۵].

جدول (۱۴): گروه‌بندی شاخص‌ها [مؤلفین]

row	Indicators	Fields	Abundance
1	Security Policy	Security Policy	7
2	Policy development		
3	processes and policies		
4	policies and procedures		
5	Security policies and process		
6	Media protection		
7	audit and accountability		
8	Organizing information security	Information Security	7
9	Information sharing		
10	Information Security Targets		
11	Organizing information security		
12	Social engineering controls		
13	System and information integrity		
14	Information system acquisition		
15	Asset management	Asset management	6
16	Asset, Change, and Configuration Management (ASSET)		
17	Configuration management		
18	Asset management		
19	Change management		
20	Asset management		
21	Physical security	Physical Security	8
22	Server Protection		
23	Physical and environmental security		
24	Physical security		
25	security risk environment		
26	Physical security		
27	Mobile security		
28	Physical security		
29	Access control	identity and access management	8
30	Network security		
31	access control		
32	IAM (identity and access management)		
33	Identity and Access Management (ACCESS)		
34	IAM (identity and access management)		
35	Access control		
36	Identification and authentication		
37	Development and maintenance	Development and maintenance	3
38	Secure software development		
39	Maintenance		
40	Information security incident management	Incident management	11
41	Cybersecurity incident management		
42	Event and Incident Response, Continuity of Operations		
43	Incident management		
44	security incident		
45	Security incidents		
46	Threats addressed		
47	Communication and operation management		
48	Incident response		
49	Systems and communications protection		
50	Recovery		
51	Business continuity management	Business continuity management	3
52	Business process		
53	Business continuity management		
54	Compliance	Compliance	3
55	Compliance		
56	compliance security		
57	monitoring the systems	Monitoring	8
58	End user's controls		
59	Threat and Vulnerability Management		
60	Network Management		
61	preventive, detective and corrective control		
62	Vulnerability management		
63	Test		
64	Security management		
65	Cybersecurity Architecture	Architecture	3
66	Security Architecture		
67	Architecture		
68	Technology	Enable Technology	2
69	Enable Technology		
70	risk reduction processes	Risk management	6
71	Risk management		
72	Risk Management		
73	Third-Party Risk Management		
74	Risk management		
75	Risk management		
76	Awareness	Awareness	5
77	Awareness		
78	Cybersecurity awareness		
79	Situational Awareness		
80	Situational awareness		
81	Data encryption	Data encryption	4
82	Data Classification		
83	Cryptography		
84	Application security		
85	Workforce Management	Workforce Management	7
86	Work force planning		
87	Personal security		
88	Training		
89	Awareness and training		
90	Human resource security		
91	Human resource security		
92	governance structures	governance	2
93	Cybersecurity Program Management		

Comparing Cyber Security Maturity and Information Security Maturity Models and Identifying Common Cyber Security Indicators

M. Akhtari, M. A. Keramati*, S. A. Amin Mousavi

Abstract

With the advent of the digital age, the need for governments and companies to use information technology to optimize performance, Business process smartening and provide remote services has increased. Thus, information technology and cyber security and information have also found a special place in the digital arena. Accordingly, one of the most serious dangers that governments face, which can also undermine national security, is cyber-attacks. These attacks cover a wide range of targets, one of the main of which is to damage critical infrastructure. Therefore, the sustainability of critical infrastructure in the face of such threats is crucial. This study, considering that the security of vital infrastructure is one of the most important factors in ensuring national security and passive defense, seeks to obtain the indicators of security of critical infrastructure through a comparative study method using library resources. In this study, 10 of the most important models of cyber security and information security maturity have been analyzed. The results of this study indicate that the studied models have a total of 93 indicators. Cyber security and information security maturity models are significantly similar; Therefore, some of the counted indicators overlap. Overlapping indicators were identified and classified into 17 groups. The results show that the "incident management" index with a frequency of 11 is the most important index in securing critical infrastructure, as well as physical security, monitoring, access-identity control, security policies and other indicators in They are next.

Key Words: *Critical Infrastructure, CyberSecurity Maturity Model, Information Security Maturity Model, Passive Defense*

* Associate Professor, Department of Industrial Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran (mohammadalikeramati@yahoo.com) - Writer-in-Charge