فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره ۲، بهار ۱۴۰۱
مقاله چهارم، از صفحات ۱۰۴-۸۱

مقاله پژوهشی:

بررسی و ارزیابی مدل‌های تاب‌آوری سایبری

موسی کاظمی[۱]، مهرداد کارگری[۲]

تاریخ دریافت: ۱۴۰۰/۰۳/۱۰ **تاریخ پذیرش: ۱۴۰۰/۰۸/۱۶**

چکیده

تاب‌آوری سایبری، توانایی سامانه برای برگشت به وضعیت اولیه بعد از یک رویداد غیرمنتظره است. در این مقاله محقق به دنبال پاسخ به این سؤالات است: تعریف تاب‌آوری سایبری چیست؟ چارچوب‌ها، مدل‌ها و موضوعات مرتبط با تاب‌آوری سایبری کدامند؟ چارچوب و مدل تاب‌آوری سایبری پیشنهادی کدام است؟ همچنین پس از تعریف تاب‌آوری سایبری بر اساس مراجع مختلف به چارچوب‌ها، مدل‌ها و موضوعات مرتبط با تاب‌آوری سایبری به شرح زیر پرداخته‌شده است: امنیت سایبری با راهبرد امن سازی، مراقبت و ارتجاع/ بازگشت، استاندارد ۲۷۰۰۱، تاب‌آوری زیرساخت، طرح اقدام شش‌گانه برای تاب‌آوری، چارچوب مهندسی تاب‌آوری سایبری، کلیدهای تاب‌آوری سایبری، بیانیه‌ای برای تاب‌آوری سایبری، مدل تاب‌آوری سایبری CERT، مدل تاب‌آوری عملیاتی، مدیریت امنیت اطلاعات و تاب‌آوری سایبری، حفاظت سازمان با تاب‌آوری سایبری، چارچوب امنیت سایبری NIST، مدلی برای تاب‌آوری سایبری.

در انتهای این مقاله، چارچوب مهندسی تاب‌آوری سایبری مؤسسهٔ MITRE و چارچوب تاب‌آوری سایبری مؤسسهٔ NIST با افزودن روش‌های ابتکاری و بومی برای به‌کارگیری و ایجاد تاب‌آوری سایبری سازمان پیشنهادشده است.

کلیدواژه‌ها: تاب‌آوری سایبری، انعطاف‌پذیری، جهندگی، مقاومت، حالت ارتجاعی

۱ دانشجوی مقطع دکتری دانشگاه عالی دفاع ملی (نویسنده مسئول) m.kazemi@sndu.ac.ir

۲ عضو هیئت علمی دانشگاه تربیت مدرس

مقدمه

تاب‌آوری در حوزه‌های مختلفی ازجمله پزشکی، روان‌شناسی، علوم انسانی، فنی و... مطرح است، معنی و مفهوم آن در حوزه‌های مختلف مشابه یکدیگر می‌باشد. اکثر مدل‌های تاب‌آوری بیشتر ناظر بر امور سلامت است.

کلمات مرتبط با تاب‌آوری در فرهنگ لغات به شرح ذیل است:

- Resilience & Resiliency: تاب‌آوری در نوشتار انگلیسی (خارج از آمریکا)، اغلب به‌صورت Resiliency و در نوشتار آمریکایی (در آمریکا) اغلب به‌صورت Resilience است؛ هر دو کلمه به‌صورت اسم به‌کاررفته و به معنی جهندگی، حالت ارتجاعی، قابلیت ارتجاع و بازگشت‌پذیری، فنریت، تاب‌آوری و انعطاف‌پذیری است؛ بنابراین عبارت‌های Cyber Resilience و Cyber Resiliency معادل یکدیگر و به معنای تاب‌آوری سایبری است؛
- Resilient: به‌صورت صفت به معنی یک شیء باقابلیت فنری یا جهنده است؛
- Resistant: به‌صورت صفت به معنی مقاوم، پایدار و مستحکم است؛
- Resist: به‌صورت اسم به معنی مقاومت، پایداری و استقامت است و به‌صورت فعل به معنی مقاومت کردن، پایداری کردن و استقامت کردن است.

تعریف‌های مختلفی از **تاب‌آوری سایبری** وجود دارد که به چند تعریف در زیر اشاره می‌شود:

- **تاب‌آوری سایبری**، «توانایی سامانه برای بازگشت به حالت اولیه[۱] بعد از یک رویداد غیرمنتظره[۲] است» (تعریف دیکشنری)؛
- **تاب‌آوری سایبری**، «توانایی یک سازمان برای مقاومت[۳]، پاسخ[٤] و بازیابی[٥] در برابر تهدیداتی که بر روی اطلاعات کسب‌وکار سازمان تأثیر می‌گذارد» (AXELOS، ۲۰۱۵)؛
- **تاب‌آوری سایبری**، «توانایی آمادگی[٦] و سازگاری[۷] برای تغییر شرایط، تحمل[۸] و بازیابی

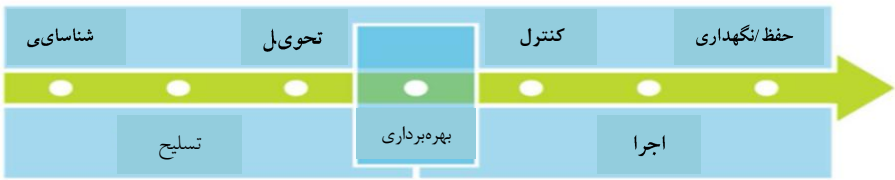
---

۱. original state
۲. an unexpected event
۳ Resist
٤. Respond
٥. Recover
٦. Prepare
۷. Adapt
۸. Withstand

سریع[۱] در برابر اختلال[۲] است؛ به‌عبارت‌دیگر، تاب‌آوری[۳] شامل توانایی تحمل[٤] و بازیابی[٥] در برابر حملات عمدی[٦]، سوانح[۷] یا تهدیدات طبیعی یا حوادث[۸] است» (ادارهٔ امنیت سایبری و ارتباطات وزارت امنیت داخلی آمریکا، ۲۰۱۳).

چارچوب‌ها، مدل‌ها و موضوعات مرتبط با تاب‌آوری سایبری

مأموریت‌ها و عملکردهای سازمان‌ها و کشورها در حوزهٔ کسب‌وکار به‌طور فزاینده‌ای به فضای سایبر وابسته هستند. در فضای سایبری، حملات تنها به رویدادهای گسستهٔ ساده‌ای مانند گسترش یک ویروس و یا کرم و یا یک حملهٔ انکار سرویس محدود نمی‌شود. حملات سایبری دارای تهدیدات مداوم پیشرفته است. در شکل (۱) چرخهٔ حیات حملهٔ سایبری نشان داده‌شده است (یک دفاع سایبری جدید و دفاع تهدید محور، ۲۰۱۳).



شکل (۱) چرخهٔ حیات حملهٔ سایبری

حملهٔ سایبری شامل فعالیت پنهان، مداوم و پیچیده برای ایجاد یک جای پا در سامانه‌های سازمانی، حفظ جای پا و گسترش آن در مجموعه‌ای از منابع کنترل دشمن و استخراج مخفیانهٔ اطلاعات حساس از منطقهٔ تحت کنترل دشمن و خراب کردن عملیات دشمن است (تاب‌آوری سایبری، ۲۰۱۵).

---

۱. Recover Rapidly
۲. Disruptions
۳. Resilience
٤. Withstand
٥. Recover
٦. Deliberate Attacks
۷. Accidents
۸. Incidents

جدول (۱) چارچوب‌ها، مدل‌ها و موضوعات مرتبط با تاب‌آوری سایبری

ردیف	چارچوب‌ها، مدل‌ها و موضوعات مرتبط با تاب‌آوری سایبری	ردیف	چارچوب‌ها، مدل‌ها و موضوعات مرتبط با تاب‌آوری سایبری
۱	امنیت سایبری با راهبرد امن سازی، مراقبت و ارتجاع/ بازگشت	۸	مدل تاب‌آوری سایبری CERT
۲	استاندارد ۲۷۰۰۱	۹	مدل تاب‌آوری عملیاتی
۳	تاب‌آوری زیرساخت	۱۰	مدیریت امنیت اطلاعات و تاب‌آوری سایبری
٤	طرح اقدام شش‌گانه برای تاب‌آوری	۱۱	حفاظت سازمان با تاب‌آوری سایبری
٥	چارچوب مهندسی تاب‌آوری سایبری	۱۲	چارچوب امنیت سایبری NIST
٦	کلیدهای تاب‌آوری سایبری	۱۳	مدلی برای تاب‌آوری سایبری
۷	بیانیه‌ای برای تاب‌آوری سایبری		

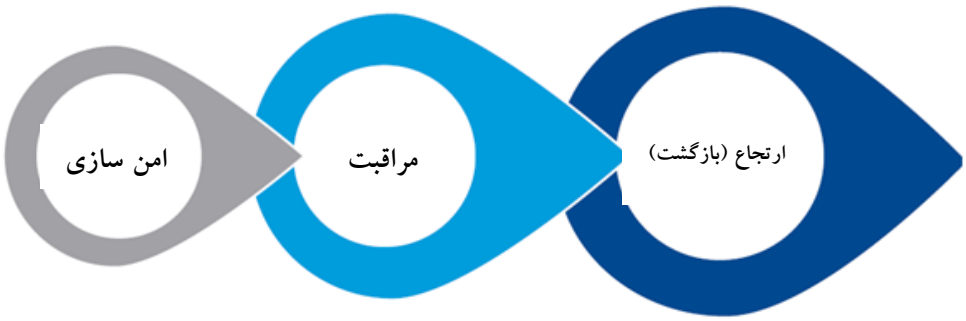
امنیت سایبری با راهبرد امن سازی، مراقبت و ارتجاع/بازگشت

بر اساس شکل (۲) – مدل مرکز تحلیل خدمات اقتصادی دِیلویت[۱] امنیت سایبری با راهبرد امن سازی، مراقبت و ارتجاع/بازگشت به شرح زیر است:

به‌صورت سنتی، تمرکز بر «امن سازی» بوده است اما تحول و گستردگی تهدیدات سایبری به رویکرد پویاتر و امنیت سایبری بهتری نیاز دارد.

- امن سازی: افزایش کنترل‌های اولویت‌بندی شدهٔ ریسک، برای حفاظت در برابر تهدیدات شناخته‌شده، مطابق با استانداردهای امنیت فضای سایبر صنعتی و قوانین موجود؛
- مراقبت: شناسایی تخلفات[۲] و ناهنجاری‌ها[۳] از طریق آگاهی موقعیتی بهتر[٤] در سراسر محیط سازمان؛
- ارتجاع/بازگشت: توانایی بازگشت سریع[٥] به عملکرد عادی[٦] و بازسازی خرابی[۷] برای انجام کسب‌وکار (مرکز تحلیل خدمات اقتصادی دِیلویت).

۱. (deloitte resilience, ۲۰۱٦)
۲. Violations
۳. Anomalies
٤. Better Situational Awareness
٥. quickly return
٦. Normal Operations
۷. Repair Damage



شکل (۲) امنیت سایبری با راهبرد امن سازی، مراقبت و ارتجاع/ بازگشت

استاندارد ۲۷۰۰۱

امنیت سایبری سنتی، رویکرد کافی برای رویارویی با چشم‌انداز تهدیدات سایبری مدرن را ندارد. امنیت سایبری سنتی، برای دفاع در مقابل هرگونه پتانسیل حملهٔ سایبری کافی نیست. شما باید بپذیرید که حمله به‌طورقطع اتفاق افتاده و موفق خواهد شد؛ بنابراین تاب‌آوری سازمان در شناسایی و پاسخ به نقض امنیتی، به یک ویژگی بقای حیاتی در آینده تبدیل خواهد شد.

تاب‌آوری سایبری تحت استاندارد ISO۲۷۰۰۱ است و مسائل گسترده‌تر استمرار کسب‌وکار توسط استاندارد ISO۲۷۰۳۱ پوشش داده می‌شود (تاب‌آوری سایبری، ۲۰۱۵).

مدل تاب‌آوری زیرساخت

مطابق شکل (۳) ابعاد تاب‌آوری زیرساخت عبارت است از:

- قابلیت اطمینان[۱]
- پاسخ و بازیابی[۲]
- افزونگی[۳]
- مقاومت[٤]

۱. Reliability
۲. Response and Recovery
۳. Redundancy
٤. Resistance

شکل (۳) تاب‌آوری زیرساخت

طرح اقدام شش‌گانه برای تاب‌آوری

تاب‌آوری سایبری، توانایی یک سامانه یا یک حوزه برای مقاومت و استقرار مجدد و سریع در برابر حملات یا خرابی‌ها است (مؤسسهٔ بین‌المللی مطالعات راهبردی، Nigel Inkster).

طرح اقدام[۱] شش‌گانه برای تاب‌آوری عبارت است از:

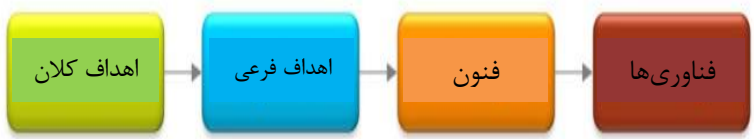
- آمادگی سازمانی[۲]؛
- آگاهی موقعیتی[۳]؛
- دفاع سایبری[۴]؛
- شناسایی[۵]؛
- کاهش و مهار[۶]؛
- بازیابی[۷] (MARM, ۲۰۱۵).

۱. Action plan
۲. Organizational Readiness
۳. Situational awareness
۴. Cyber defense
۵. Detection
۶. Mitigation and containment
۷. Recovery

چارچوب مهندسی تاب‌آوری سایبری

تعریف‌های مختلفی از تاب‌آوری[۱] وجود دارد، یکی از بهترین تعریف‌ها «قدرت یا توانایی بازگشت به شکل و موقعیت اولیه[۲] است.

حملات در فضای سایبر مانند گذشته به رویدادهای سادهٔ گسسته مانند گسترش ویروس و یا حملهٔ انکار سرویس محدود نمی‌شود. حملات سایبری با تهدیدات مداوم پیشرفته[۳] دارای قابلیت‌ها، منابع و تداوم نفوذ به زیرساخت‌های فناوری اطلاعات هستند؛ بنابراین سامانه‌های امروزی باید در برابر تهدیدات مداوم پیشرفته انعطاف‌پذیر باشند. مؤسسهٔ MITRE، چارچوب مهندسی تاب‌آوری سایبری[٤] با عنوان «راهنمای تاب‌آوری سایبری» را برای پشتیبانی از توسعهٔ ساخت‌یافته و سازگار ایجاد نموده است؛ این چارچوب مهندسی تاب‌آوری سایبری شامل اهداف کلان، اهداف فرعی و فنون است. (Deb Bodeau Richard Graubart, September ۲۰۱۳)

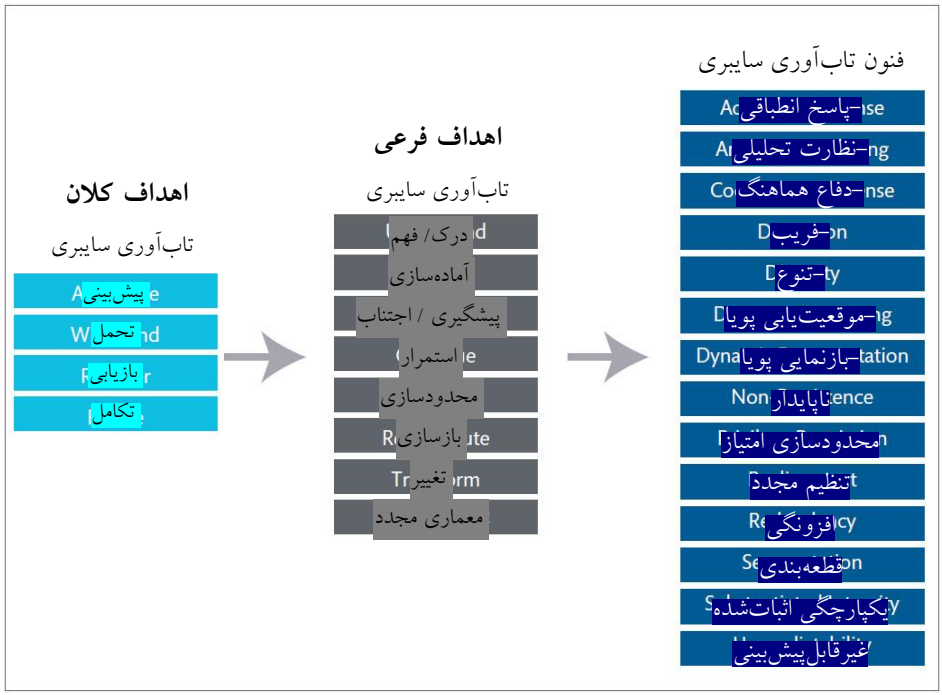


شکل (٤) ابعاد، مؤلفه‌ها، شاخص‌ها و متغیرهای چارچوب مهندسی تاب‌آوری سایبری

بر اساس شکل (٤) برای تحقق تاب‌آوری سایبری اهداف کلی تعریف می‌شود؛ برای تحقق هر هدف کلی نیاز است که اهداف فرعی در نظر گرفته شود؛ برای تحقق هر هدف فرعی از چند فن استفاده می‌شود. برای تحقق هر فن از چند فناوری استفاده می‌شود.

---

۱. Resiliency
۲. original
۳. Advanced Persistent Threat (APT)
٤. Cyber Resilience Engineering Framework (CREF)



شکل (۵) چارچوب مهندسی تاب‌آوری سایبری

اهداف کلان چارچوب مهندسی تاب‌آوری سایبری به‌صورت زیر تعریف می‌شود:

جدول (۲) تعریف اهداف کلان چارچوب مهندسی تاب‌آوری سایبری

هدف کلان[۱]	تعریف
پیش‌بینی[۲]	حفظ حالت آمادگی آگاهانه به‌منظور پیشگیری از به خطر انداختن عملکرد[۳] مأموریت در شرایط ناگوار
تحمل[۴]	تداوم اجرای[۵] مأموریت ضروری[۶] با وجود شرایط نامطلوب[۷]
بازیابی[۸]	بازگشت به عملکرد مطلوب مأموریت در طول و بعد از شرایط نامطلوب
تکامل[۱]	تغییر عملکردهای مأموریت و یا پشتیبانی از قابلیت‌ها تا زمانی که عوارض نامطلوب حاصل از

۱ Goal
۲ Anticipate
۳ function
۴ Withstand
۵ functions
۶ essential
۷ adverse
۸ Recover

هدف کلان[۱]	تعریف
	شرایط نامطلوب واقعی یا پیش‌بینی‌شده به حداقل برسد.

اهداف فرعی چارچوب مهندسی تاب‌آوری سایبری به‌صورت زیر تعریف می‌شود:

جدول (۳) تعریف اهداف فرعی چارچوب مهندسی تاب‌آوری سایبری

هدف فرعی[۲]	تعریف
درک[۳]	حفظ بازنمایی‌های[٤] مفید وابستگی مأموریت و وضعیت منابع با توجه به ناملایمات ممکن[٥]
آماده‌سازی[٦]	حفظ مجموعه‌ای از دوره‌های واقع‌گرایانه[۷] عملی که به پیش‌بینی[۸] یا پیش‌بینی ناملایمات[۹] اشاره دارد.
پیشگیری/ اجتناب[۱۰]	ممانعت از اجرای موفقیت‌آمیز حمله و یا جلوگیری از تحقق[۱۱] شرایط نامطلوب
استمرار[۱۲]	به حداکثر رساندن طول عمر[۱۳] عملکردهای ضروری مأموریت در شرایط نامطلوب
محدودسازی[۱٤]	محدود نمودن خسارت حاصل از شرایط نامطلوب
بازسازی[۱٥]	آرایش[۱٦] منابع برای رقابت[۱۷] برای مجموعه‌ای از عملکردهای مأموریت که ممکن است پس‌ازآن به شرایط نامطلوب دچار شوند.
تغییر[۱۸]	تغییر رفتار سازمانی در پاسخ به شرایط نامطلوب قبل[۱۹]، حین[۲۰] و یا آینده‌نگر[۲۱] و یا حمله

۱. Evolve
۲. Objective
۳. Understand
٤. representations
٥. possible adversity
٦. Prepare
۷. realistic
۸. predicted
۹. anticipated adversity
۱۰. Prevent / Avoid
۱۱. realization
۱۲. Continue
۱۳. viability
۱٤. Constrain
۱٥. Reconstitute
۱٦. Redeploy
۱۷. compete
۱۸. Transform
۱۹. prior
۲۰. current
۲۱. prospective

هدف فرعی[۲]	تعریف
معماری مجدد[۱]	اصلاح معماری برای بهبود تاب‌آوری

فنون چارچوب مهندسی تاب‌آوری سایبری به‌صورت زیر تعریف می‌شود:

جدول (٤) تعریف فنون چارچوب مهندسی تاب‌آوری سایبری

فن[۲]	تعریف
پاسخ انطباقی[۳]	پاسخ مناسب و پویا به شرایط[٤] خاص با استفاده از احتمالات[٥] عملیاتی جایگزین[٦] و چابک برای حفظ حداقل قابلیت‌های عملیاتی به‌منظور محدود کردن پیامد[۷] و اجتناب[۸] از بی‌ثباتی[۹] و اقدام پیشگیرانهٔ[۱۰] مناسب
نظارت تحلیلی[۱۱]	جمع‌آوری، ترکیب و تجزیه‌وتحلیل داده‌ها به‌طور مستمر برای استفاده از اطلاعات[۱۲] تهدید، شناسایی آسیب‌پذیری‌ها، پیدا کردن نشانه‌های[۱۳] شرایط نامطلوب بالقوه و شناسایی آسیب[۱٤] بالقوه یا واقعی
دفاع هماهنگ[۱٥]	هماهنگی متعدد[۱٦]، مکانیسم‌های متمایز[۱۷] (دفاع در عمق[۱۸]) برای حفاظت از منابع حیاتی در سراسر زیرسامانه‌ها، لایه‌ها، سامانه‌ها و سازمان
فریب[۱۹]	گیج کردن[۲۰]، فریب[۲۱] و گمراه کردن[۲۲] دشمن
تنوع[۱]	استفاده از مجموعهٔ فناوری‌های ناهمگن، منابع داده‌ها، مکان‌های پردازش و مسیرهای ارتباطی

۱. Re-architect
۲. Technique
۳. Adaptive Response
٤. situations
٥. contingencies
٦. alternative
۷. consequences
۸. avoid
۹. destabilization
۱۰. preemptive
۱۱. Analytic Monitoring
۱۲. intelligence
۱۳. indications
۱٤. damage
۱٥. Coordinated Defense
۱٦. multiple
۱۷. distinct
۱۸. defense-in-depth
۱۹. Deception
۲۰. Confuse
۲۱. deceive
۲۲. mislead

فن[۲]	تعریف
	برای به حداقل رساندن خرابی‌های عمومی[۲] (ازجمله حملات بهره‌برداری از آسیب‌پذیری‌های عمومی)
موقعیت‌یابی پویا[۳]	توزیع و جابه‌جایی وظایف[٤] و دارایی‌ها[٥] به‌صورت پویا
بازنمایی پویا[٦]	پشتیبانی از آگاهی موقعیتی[۷] مأموریت و واکنش[۸] با استفاده از بازنمایی[۹] پویای قطعات، سامانه‌ها، خدمات، فعالیت‌های دشمن و دیگر شرایط نامطلوب و اثرات دوره‌های جایگزین عملی[۱۰]
مدت‌زمان ناپایداری[۱۱]	نگه‌داشتن[۱۲] اطلاعات، خدمات و اتصال برای مدت‌زمان محدود و درنتیجه[۱۳] کاهش در معرض خرابی[۱٤]، تغییر[۱٥] یا مورد غصب[۱٦] قرار گرفتن
محدودسازی دسترسی[۱۷]	طراحی برای محدود کردن دسترسی‌های داده‌شده[۱۸] به کاربران و نهادهای سایبری و به مجموعهٔ درخواست‌های دسترسی به منابع بر اساس حساسیت[۱۹]
تنظیم مجدد[۲۰]	همسو کردن[۲۱] منابع با عملکردهای مأموریت اصلی و درنتیجه کاهش سطح حملهٔ بالقوه برای پیامدهای ناخواسته[۲۲] و کاهش پتانسیل خرابی‌های آبشاری[۲۳]
افزونگی[۲٤]	تهیهٔ چندین نمونهٔ[۱] حفاظت‌شده از اطلاعات حیاتی و منابع به‌منظور کاهش پیامدهای از دست

---

۱. Diversity
۲. common
۳. Dynamic Positioning
٤. functionality
٥. assets
٦. Dynamic Representation
۷. situation awareness
۸. response
۹. representations
۱۰. alternative courses of action
۱۱. Non-Persistence
۱۲. Retain
۱۳. thereby
۱٤. corruption
۱٥. modification
۱٦. usurpation
۱۷. Privilege Restriction
۱۸. privileges assigned
۱۹. criticality
۲۰. Realignment
۲۱. aligned
۲۲. unintended
۲۳. cascading failures
۲٤. Redundancy

فن[۲]	تعریف
	دادن اطلاعات
قطعه‌بندی/ جداسازی[۲]	جداسازی منطقی یا فیزیکی اجزا بر اساس حساسیت و اعتماد[۳] به‌منظور محدود کردن گسترش[٤] آسیب[٥]
یکپارچگی اثبات‌شده[٦]	ایجاد مکانیسم‌هایی برای اطمینان[۷] از اینکه آیا خدمات حیاتی، مخازن اطلاعات، جریان اطلاعات و اجزا خراب[۸] است یا نه؟
غیرقابل‌پیش‌بینی[۹]	ایجاد تغییرات به‌طور مکرر و تصادفی برای اینکه سطح حمله غیرقابل‌پیش‌بینی است.

نگاشت اهداف فرعی با فنون تاب‌آوری سایبری در چارچوب مهندسی تاب‌آوری سایبری به‌صورت زیر است:

جدول (۵) نگاشت اهداف فرعی به فنون تاب‌آوری سایبری در چارچوب مهندسی تاب‌آوری سایبری

فنون تاب‌آوری سایبری	اهداف فرعی							
	درک	آمادسازی	جلوگیری	محدودسازی	استمرار	بازسازی	تغییر	معماری مجدد
واکنش انطباقی				X	X	X		
نظارت تحلیلی	X	X		X		X		
دفاع هماهنگ		X	X	X	X	X		
فریب	X		X		X			
تنوع			X		X			X
موقعیت پویا	X		X		X			X
بازنمایی پویا	X	X					X	
ناپایداری			X	X	X			X
محدودسازی			X	X				

۱. instances
۲. Segmentation / Separation
۳. trustworthiness
٤. spread
٥. damage
٦. Substantiated Integrity
۷. ascertain
۸. corrupted
۹. Unpredictability

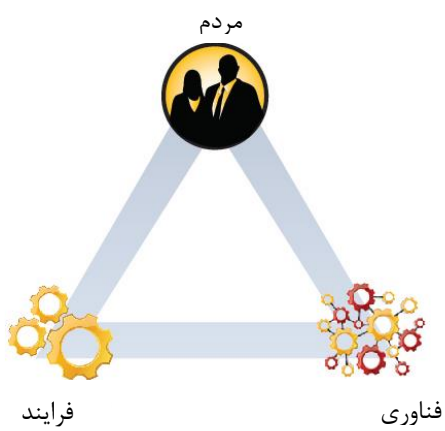
فنون تاب‌آوری سایبری	اهداف فرعی							
	درک	آماده‌سازی	جلوگیری	محدودسازی	استمرار	بازسازی	تغییر	معماری مجدد
امتیاز								
تنظیم مجدد				X			X	
افزونگی					X	X		
تقسیم‌بندی / جدایی			X	X				
یکپارچگی اثبات‌شده	X			X	X	X		
غیرقابل‌پیش‌بینی	X		X		X			

کلیدهای تاب‌آوری سایبری

مطابق شکل (٦) کلیدهای تاب‌آوری سایبری عبارت‌اند از: مردم؛ فناوری؛ فرآیند.

برای تاب‌آوری سایبری سازمان باید به تاب‌آوری حوزه‌های انسانی، فناوری مورداستفاده و فرآیندهای انجام مأموریت توجه داشت.

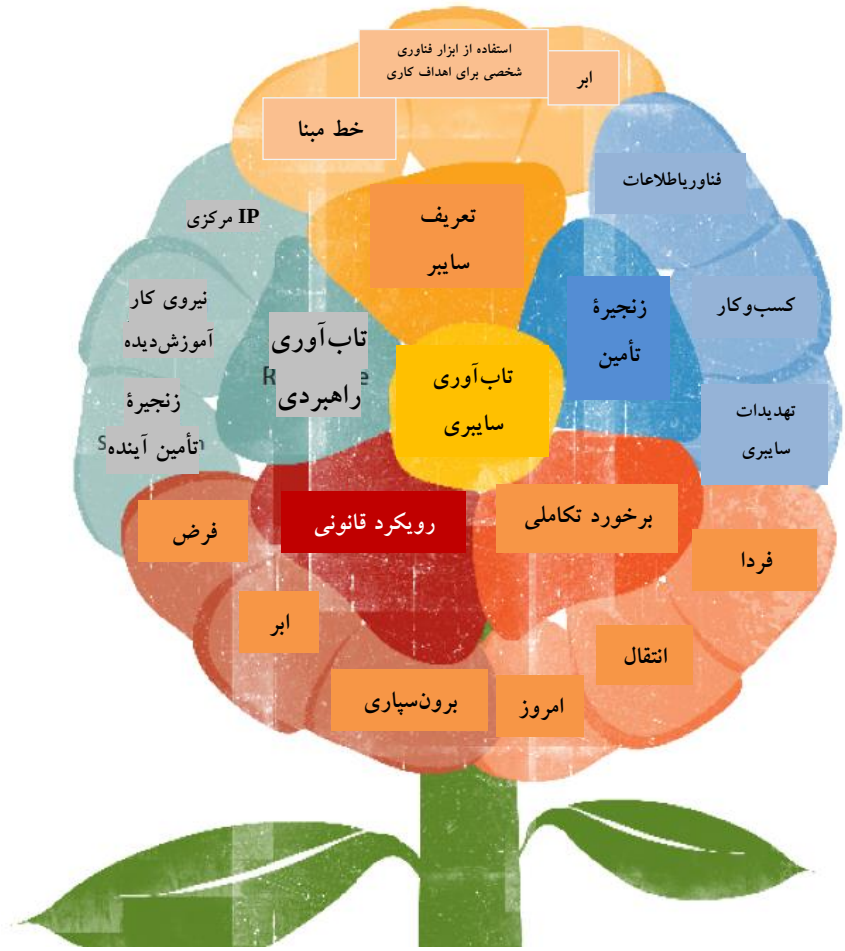
(The Cyber-Resilient Enterprise: Harnessing Your Security Intelligence)



شکل (٦) کلیدهای تاب‌آوری سایبری

بیانیه‌ای برای تاب‌آوری سایبری

شرکت Symantec ابعاد و مؤلفه‌های تاب‌آوری سایبری را در بیانیه‌ای به‌صورت زیر ارائه نموده است:



شکل (۷) بیانیه‌ای[۱] برای تاب‌آوری سایبری

(Symantec, ۲۰۱۵)

۱. Manifesto

مدل تاب‌آوری سایبری CERT

مؤلفه‌های تاب‌آوری سایبری CERT آمریکا به‌صورت زیر است:

- مدیریت دارایی[۱]؛
- مدیریت کنترل‌ها[۲]؛
- مدیریت پیکربندی و تغییرات[۳]؛
- مدیریت آسیب‌پذیری[٤]؛
- مدیریت حادثه[٥]؛
- مدیریت استمرار خدمات[٦]؛
- مدیریت ریسک[۷]؛
- مدیریت وابستگی خارجی[۸]؛
- آموزش و آگاهی[۹]؛
- آگاهی موقعیتی[۱۰].

(CYBER RESILIENCE REVIEW & CYBER SECURITY EVALUATION TOOL, ۲۰۱٥)

مدل تاب‌آوری عملیاتی

بر اساس شکل (۸) مؤلفه‌های تاب‌آوری عملیاتی به‌صورت زیر است:

---

۱. Asset Management

۲. Controls Management

۳. Configuration and Change Management

٤. Vulnerability Management

٥. Incident Management

٦. Service Continuity Management

۷. Risk Management

۸. External Dependency Management

۹. Training and Awareness

۱۰. Situational Awareness

جدول (٦) مؤلفه‌های تاب‌آوری عملیاتی

ردیف	مؤلفه‌های تاب‌آوری عملیاتی	ردیف	مؤلفه‌های تاب‌آوری عملیاتی
١	امنیت اطلاعات	٦	استمرار کسب‌وکار
٢	عملیات فناوری اطلاعات	٧	بازیابی فاجعهٔ فناوری اطلاعات
٣	تداوم زنجیرهٔ تأمین	٨	ارتباطات موقع بحران
٤	مدیریت ریسک	٩	مدیریت اضطرار
٥	استمرار نیروی کار	١٠	مدیریت موقع بحران

شکل (٨) مدل تاب‌آوری عملیاتی

مدیریت امنیت اطلاعات و تاب‌آوری سایبری

بر اساس شکل (۹) توصیه‌های مدیریت امنیت اطلاعات و تاب‌آوری سایبری به شرح زیر است:

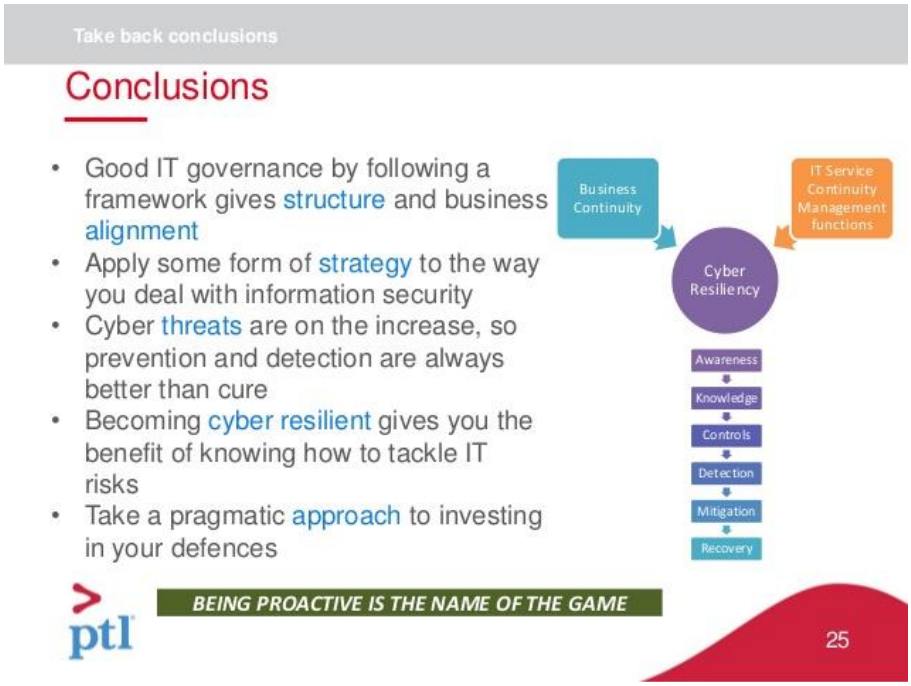
- ادارهٔ فناوری اطلاعات با پیروی از یک چارچوب مناسب، ساختار و هم‌ترازی[۱] کسب‌وکار را به ارمغان[۲] می‌آورد؛
- در این مسیر تعدادی از راهبردها[۳] را اجرا کنید؛ به امنیت اطلاعات رسیدگی[٤] کنید؛
- تهدیدات سایبری رو به افزایش است، بنابراین پیشگیری[٥] و تشخیص[٦] همیشه بهتر از درمان[۷] است؛
- داشتن تاب‌آوری سایبری[۸] به شما چگونگی مقابله با خطر فناوری اطلاعات را هدیه می‌کند؛
- رویکرد واقع‌گرایانه[۹] به سرمایه‌گذاری در دفاع از خود داشته باشید.

همچنین برای استمرار کسب‌وکار و عملکردهای مدیریت مستمر سرویس فناوری اطلاعات، باید به دنبال تاب‌آوری سایبری در سازمان بود. برای تحقق تاب‌آوری سایبری باید مؤلفه‌های آن محقق شود.

در این مدل مؤلفه‌های تاب‌آوری سایبری عبارت‌اند از: آگاهی موقعیتی[۱۰]؛ دانش[۱۱]؛ کنترل‌ها[۱۲]؛ تشخیص[۱۳]؛ کاهش[۱٤]؛ بازیابی[۱٥].

---

۱. alignment
۲. give
۳. some form of strategy
٤. deal
٥. prevention
٦. detection
۷. cure
۸. cyber resilient
۹. pragmatic approach
۱۰. Awareness
۱۱. Knowledge
۱۲. Controls
۱۳. Detection
۱٤. Mitigation
۱٥. Recovery



شکل (۹) مدیریت امنیت اطلاعات و تاب‌آوری سایبری

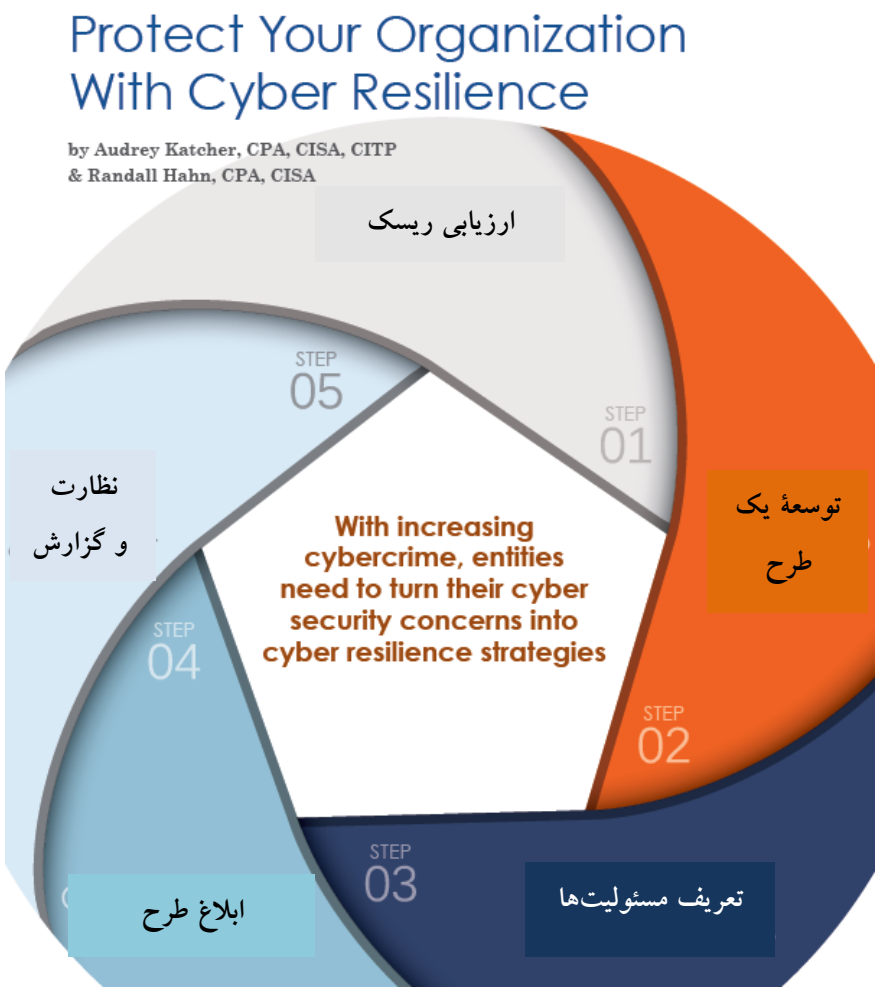
حفاظت سازمان با تاب‌آوری سایبری

بر اساس شکل (۱۰) سازمان‌ها نیاز دارند با افزایش جرم سایبری، نگرانی‌های امنیت سایبری خود را به راهبردهای تاب‌آوری سایبری تبدیل کنند؛ بر اساس این مدل مؤلفه‌های تاب‌آوری سایبری عبارت است از:

ارزیابی خطر[۱]؛ توسعهٔ یک طرح[۲]؛ تعریف مسئولیت‌ها[۳]؛ ابلاغ طرح[۴]؛ نظارت و گزارش[۵].

Protect Your Organization with Cyber Resilience, ۲۰۱۵, online

۱. Assess the Risk
۲. Develop a plan
۳. Define Responsibilities
٤. Communicate the Plan
٥. Monitoring & Report



شکل (۱۰) حفاظت سازمان با تاب‌آوری سایبری

چارچوب امنیت سایبری NIST

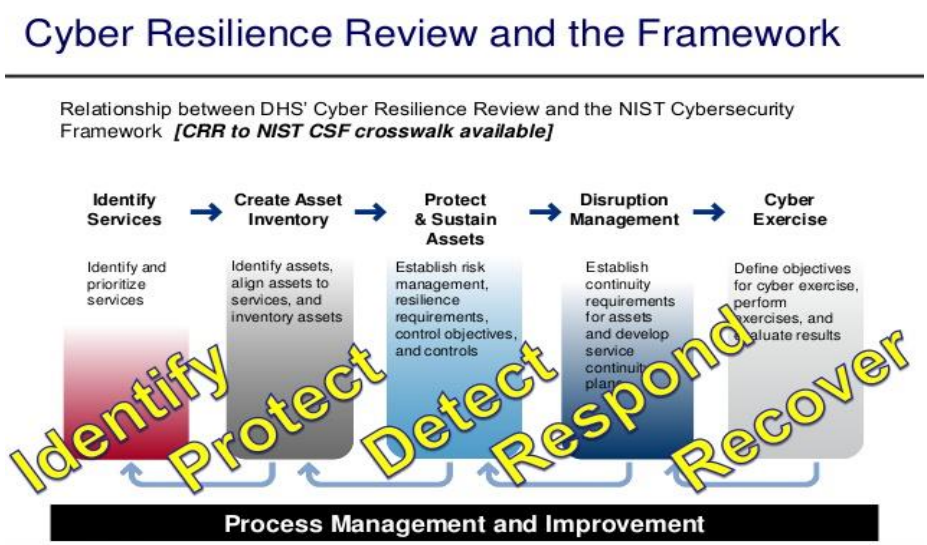
سازمان‌ها به‌طور فزاینده‌ای تشخیص می‌دهند که مأموریت‌ها، عملکردهای کسب‌وکار، سامانه‌ها، زیرسامانه‌ها و بخش‌های مأموریتی در برابر تهدیدات مداوم پیشرفته[۱] به تاب‌آوری نیاز دارند. بسیاری از سازمان‌ها برای مدیریت ریسک شرح داده‌شده در ویژه‌نامهٔ NIST SP ۸۰۰-

۱. APT

۳۹[۱]، رویکرد چندلایه‌ای و رویکرد چرخهٔ حیات امنیتی برای مدیریت ریسک تعریف‌شده توسط چارچوب مدیریت ریسک در NIST SP ۸۰۰-۳۷[۲] را اتخاذ نموده‌اند؛ برای آن دسته از سازمان‌هایی که با استفاده از استاندارد NIST به دنبال برقراری مدیریت ریسک در سازمان خود هستند، این سؤال مطرح می‌شود: چگونه باید کنترل‌های امنیتی در NIST SP ۸۰۰-۵۳R٤[۳] را انتخاب، طراحی و برای بهبود تاب‌آوری سایبری اجرا نمود؟ (تاب‌آوری سایبری، ۲۰۱۵)

در چارچوب مدیریت ریسک تعریف‌شده توسط NIST SP ۸۰۰-۳۷، فنون تاب‌آوری سایبری را می‌توان به‌عنوان مجموعه‌ای از خدمات به اشتراک گذاشته و یا زیرساخت مشترک یا انتخابی[٤]، سفارشی[٥] و اجرای کنترل‌های امنیتی را به یک سامانه اعمال نمود؛ همچنین این سند از تاب‌آوری سایبری سند NIST SP ۸۰۰-۵۳R٤ حمایت می‌کند.

(Deborah J. Bodeau, Richard Graubart, December ۲۰۱۳)



شکل (۱۱) تاب‌آوری سایبری و چارچوب امنیت سایبری NIST

۱. مدیریت ریسک امنیت اطلاعات، ۲۰۱۱

۲. راهنمای اجرای چارچوب مدیریت ریسک سامانه‌های اطلاعاتی فدرال، ۲۰۱۰

۳. کنترل‌های امنیتی و حریم خصوصی سازمان‌ها و سامانه‌های اطلاعاتی فدرال، ۲۰۱۳

٤. Selecting

٥. Tailoring

مطابق شکل (۱۱) چارچوب تاب‌آوری سایبری NIST دارای مؤلفه‌های زیر است:

شناسایی[۱]؛ حفاظت[۲]؛ تشخیص[۳]؛ پاسخ[٤]؛ بازیابی[٥].

مدلی برای تاب‌آوری سایبری

بر اساس شکل (۱۲) مؤلفه‌های تاب‌آوری سایبری عبارت‌اند از:

جمع‌آوری بلادرنگ[٦]؛ تشخیص پیشرفته و رفتار[۷]؛ تهدید، شناسایی و تحلیل خودکـار[۸]؛ امنیـت بلادرنگ و نمایش انطباق با استاندارد[۹]؛ راهکار یکپارچگی و کاهش[۱۰].

شکل (۱۲) تاب‌آوری سایبری

۱. Identify
۲. Protect
۳. Detect
٤. Respond
٥. Recover
٦. Real-time collection
۷. Advanced detection and behavior
۸. Threat identification and automated analysis
۹. Real-time security and compliance display
۱۰. Integrated Resolution and Remediation

روش‌شناسی

نوع تحقیق بر اساس هدف کاربردی و بر اساس ماهیت داده‌ها توصیفی است؛ گردآوری داده‌ها به‌صورت کتابخانه‌ای دربارهٔ موضوع تحقیق انجام‌شده است.

نتیجه‌گیری

هر یک از چارچوب‌ها و مدل‌های تاب‌آوری سایبری دارای مؤلفه‌های متفاوتی هستند. برای تاب‌آوری سازمان در برابر حملات و تهدیدات مداوم پیشرفتهٔ سایبری، لازم است یک یا ترکیبی از چارچوب‌ها و مدل‌های تاب‌آوری سایبری انتخاب و در سطح سازمان به‌کارگیری شوند.

در این میان چارچوب مهندسی تاب‌آوری سایبری مؤسسهٔ MITRE و چارچوب تاب‌آوری سایبری مؤسسهٔ NIST به ابعاد و مؤلفه‌های بیشتر و جامع‌تری پرداخته‌اند؛ بنابراین برای ایجاد تاب‌آوری سایبری در سازمان، اجرا و پیاده‌سازی چارچوب‌ها و مدل‌های تاب‌آوری سایبری مذکور پیشنهاد می‌شود.

علاوه بر به‌کار بستن چارچوب‌ها و مدل‌های تاب‌آوری سایبری این مؤسسات، با افزودن روش‌های ابتکاری و بومی به آن‌ها می‌توان به تاب‌آوری سایبری با ضریب امنیت بیشتری دست‌یافت.

فهرست منابع و مآخذ

منابع لاتین

- Bodeau., D. J. (۲۰۱٤). Cyber Resiliency Engineering. ۸۷٤.
- Cyber Resilience. (۲۰۱٥). Retrieved from itgovernance.co.uk: http://www.itgovernance.co.uk/cyber-resilience.aspx#.VBxpblf٤J٤s
- Deb Bodeau Richard Graubart. (۲۰۱۳, September). Cyber Resiliency and NIST Special Publication ۸۰۰-٥۳ Rev.٤ Controls. Retrieved from NIST.
- deloitte resilience. (۲۰۱٦). Retrieved from deloitte.com: https://www۲.deloitte.com
- Explore AXELOS Best Practice. (۲۰۱٦). Retrieved from axelos.com: https://www.axelos.com/
- Joint Task Force Transformation Initiative. (۲۰۱۰, February). Guide for Applying the Risk Management Framework to Federal. Retrieved from dx.doi.org: http://dx.doi.org/۱۰,٦۰۲۸/NIST.SP.۸۰۰-۳۷r۱
- Joint Task Force Transformation Initiative. (۲۰۱۱). NIST SP ۸۰۰-۳۹, Managing Information Security Risk: Organization, Mission, and Information System View. Retrieved from csrc.nist.gov: dx.doi.org/۱۰,٦۰۲۸/NIST.SP.۸۰۰-۳۹
- JOINT TASK FORCE TRANSFORMATION INITIATIVE. (۲۰۱۳, April). Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP ۸۰۰-٥۳ R٤). Retrieved from dx.doi.org: http://dx.doi.org/۱۰,٦۰۲۸/NIST.SP.۸۰۰-٥۳r٤
- Malta Association of Risk Management (MARM). (۲۰۱۳). Cyber Resilience. Retrieved from marm.org.mt: http://www.slideshare.net/ianstaf/cyber-resilience-donald-tabone
- Protect Your Organization with Cyber Resilience. (۲۰۱٥). Retrieved from itgovernance.co.uk: http://www.itgovernance.co.uk/find-out-more-about-cyber-resilience.aspx#.VYsrGlJ۱xpk
- symantec. (۲۰۱٥). The Cyber-Resilient Enterprise: Harnessing Your Security Intelligence. Retrieved from symantec.com: https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilient-enterprise-wp-۲۱۳۳۲٤۷۱-en-us.pdf
- The Department of Homeland Security's (DHS). (۲۰۱٥). CYBER RESILIENCE REVIEW & CYBER SECURITY EVALUATION TOOL. Retrieved from ics-cert.us-cert.gov: https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CRR_CSET_S٥۰۸C.pdf
- Threat-Based Defense: A New Cyber Defense Playbook. (۲۰۱۲). Retrieved from mitre.org: https://www.mitre.org/sites/default/files/pdf/cyber_defense_playbook.pdf