



مخاطره امنیت اطلاعات؛ روش‌های ارزیابی و مدیریت

پدیدآوران

حمیدرضا خدمتگزار

استادیار پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

ساناز قربانلو

پژوهشگر پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

APK
توسعه فناوری و مهندسی
امن پردازان کوپر


وزارت علوم، تحقیقات و فناوری
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

سرشناسه	: خدمتگزار، حمیدرضا، ۱۳۶۳-
عنوان و نام پدیدآور	: مخاطره امنیت اطلاعات: روش های ارزیابی و مدیریت/ پدیدآوران حمیدرضا خدمتگزار، ساناز قربانلو؛ ویراستار بهروز رسولی.
مشخصات نشر	: تهران: پژوهشگاه علوم و فناوری اطلاعات ایران، ۱۴۰۰.
مشخصات ظاهری	: ۱۸۰ ص.: مصور(رنگی)، جدول (رنگی)، نمودار (رنگی)؛ ۲۹×۲۲ س.م.
شابک	: 978-622-98708-0-8
وضعیت فهرست نویسی	: فیبا
یادداشت	: پشت جلد به انگلیسی: Hamid Reza Khedmatgozar, Sanaz Ghorbanloo, Information Security Risk: Assessment and Management Methods
یادداشت	: کتاب حاضر با پشتیبانی شرکت فنی و مهندسی امن پردازان کویر منتشر شده است.
یادداشت	: کتابنامه: ص. ۱۷۳-۱۸۰.
موضوع	: کامپیوترها -- کنترل دستیابی
موضوع	: Computers -- Access control
موضوع	: کامپیوترها -- ایمنی اطلاعات
موضوع	: Computer security
موضوع	: تکنولوژی اطلاعات -- مدیریت
موضوع	: Information technology -- Management
موضوع	: شبکه های کامپیوتری -- تدابیر ایمنی
موضوع	: Computer networks -- Security measures
شناسه افزوده	: قربانلو، ساناز، ۱۳۶۶-
شناسه افزوده	: پژوهشگاه علوم و فناوری اطلاعات ایران
شناسه افزوده	: شرکت فنی و مهندسی امن پردازان کویر
رده بندی کنگره	: QA۷۶/۹
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۸۴۶۰۴۲۰
وضعیت رکورد	: فیبا

مخاطره امنیت اطلاعات: روش های ارزیابی و مدیریت

APK



انلود فنی و مهندسی
امن پردازان کویر

وزارت علوم، تحقیقات و فناوری
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

حمیدرضا خدمتگزار - استادیار پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

ساناز قربانلو - پژوهشگر پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)

ویراستار: بهروز رسولی

ویرایش فنی و صفحه آرایی: حمیدرضا خدمتگزار

طراح جلد: رضا عبدالحسینی

چاپ نخست: ۱۴۰۰

شمارگان: ۵۰۰۰

شابک: ۹۷۸-۶۲۲-۹۸۷۰۸-۰-۸ ISBN: 978-622-98708-0-8

حق هرگونه چاپ و انتشار محفوظ است.

قیمت: ۷۵۰۰۰ تومان

تهران: ۴-۶۶۴۹۴۹۸۰ و ۹-۶۶۹۵۱۴۳۰ (۰۲۱)

تهران- خیابان انقلاب اسلامی- خیابان فلسطین جنوبی.

خیابان خواجه نصیر. شماره ۱۱

پیشگفتار بدید آوران

یکی از کارکردهای مهم حاکمیت مدیریت فناوری اطلاعات، مدیریت مخاطره (ریسک) است که هدف آن ایجاد یک محیط امن برای کسب و کارهای الکترونیکی و تجارت الکترونیکی است. در حمایت از این کارکرد، سازمان‌های گوناگون علاقمند به پیاده‌سازی استانداردهایی هستند که روش‌های گوناگون مدیریت مخاطره را منتشر کرده‌اند. این روش‌ها، در قالب دستورالعمل‌ها/راهنماها، استانداردها و چارچوب‌های ملی و بین‌المللی از خاستگاه‌های گوناگون کاربردی و پژوهشی و به منظور ارزیابی مخاطره امنیت اطلاعات طراحی، و به منظور شناسایی، تحلیل و کاهش مخاطره‌های مرتبط با فناوری اطلاعات از سوی سازمان‌ها مورد استفاده قرار می‌گیرد. در حوزه امنیت اطلاعات، ارزیابی مخاطره امنیت اطلاعات به شکل کلی، یک روش نظام‌مند به منظور دستیابی به یک دید جامع در خصوص شناسایی (یافتن، تشخیص و تشریح)، تحلیل (درک ماهیت و تعیین سطح) و سنجش (مقایسه سطح با معیارها) مخاطره‌های امنیت اطلاعات در یک سازمان را فراهم می‌آورد. در حال حاضر تعداد زیادی از انواع روش‌های ارزیابی مخاطره امنیت اطلاعات وجود دارد که توسط نهادهای ملی و بین‌المللی، سازمان‌های حرفه‌ای و طرح‌های پژوهشی منتشر شده است. هر یک از این روش‌ها برای برآورده ساختن نیازهای خاصی طراحی شده‌اند و از این‌رو اهداف، مراحل، ساختار و سطح کاربرد متفاوتی دارند. هدف مشترک این روش‌ها برآورد و اولویت‌بندی ارزش مخاطره و پیشنهاد بهترین برنامه کاهش مخاطره برای رفع یا به حداقل رساندن این مخاطره‌ها به یک سطح قابل قبول است.

به رغم تعداد روزافزون روش‌های ارزیابی و مدیریت مخاطره، گزارش‌های گوناگون، نظرسنجی‌ها و ادبیات این حوزه نشان می‌دهد که گسترش کاربرد این روش‌ها در حال حاضر در سازمان‌ها به دلیل کمبود آگاهی، هزینه‌های بالا، نیاز به تخصص و فرآیند طولانی بسیار محدود است. افزون بر این، «اعتماد به این روش‌ها به علت نتایج ضعیف، گزارش‌های اشتباه و محدوده فناورانه بسیار کم است. افزون بر این، تعداد بسیار زیاد و گنج‌کننده روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات مشکلی را برای سازمان‌هایی که تمایل به پذیرش و بهره‌برداری از این روش‌ها دارند ایجاد کرده است و کمبود و عدم توافق در معیارهای مرجع توافق شده یا چارچوبی برای مقایسه این روش‌ها، کاربرد علمی آن را در ارزیابی مخاطره‌های امنیتی اطلاعات سازمان‌ها محدود می‌کند. در این حوزه علی‌رغم اینکه تعدادی مطالعه در مقایسه این روش‌ها انجام شده است، اما هم از نظر جامعیت روش‌های مورد بررسی و هم معیارهای طراحی شده در چارچوب پایه مقایسه محدودیت‌های فراوانی دارند. ضمن آنکه پیچیدگی موجود این ارزیابی‌ها در شکل ارائه نیز استفاده گسترده و سریع از آنها را در حوزه کاربرد دچار خدشه کرده است. از سوی دیگر در حوزه کاربرد در ایران شاهد آن هستیم که علی‌رغم وجود تنوع زیاد روش‌های ارزیابی مخاطره امنیت اطلاعات، هم از سوی مشاوران و هم از سوی بهره‌برداران دانش و آگاهی کافی در خصوص این روش‌ها وجود ندارد و تنها تعداد محدودی از آنها مورد استفاده قرار می‌گیرد. همچنین چارچوبی که بتوان مبتنی بر آن نسبت به شناخت و مقایسه این روش‌ها در موقعیت‌های گوناگون کاربردی اقدام کرد، یافت نشد.

در مجموع این محدودیت‌های پژوهشی و کاربردی، لزوم طراحی چارچوب مقایسه روش‌های ارزیابی و مدیریت مخاطره امنیت اطلاعات و سپس مصورسازی آنها را به منظور ایجاد امکان استفاده گسترده در حوزه کاربرد بیشتر نمایان می‌کند. با این توضیحات، هدف این کتاب را می‌توان مقایسه جامع و مصورسازی روش‌های ارزیابی و مدیریت مخاطره امنیت اطلاعات معرفی کرد.

این کتاب با توجه به رویکرد خود می‌تواند برای استفاده کاربردی، پژوهشی و دانشگاهی در حوزه‌های تخصصی مرتبط با مدیریت و مهندسی امنیت اطلاعات مد نظر قرار گیرد. از همه صاحب‌نظرانی که انتقاد و پیشنهادی برای ارتقاء اثر حاضر دارند، تقاضا داریم هرگونه نظر خود را درباره کتاب حاضر با پست الکترونیکی به آدرس khedmatgozar@irandoc.ac.ir ارائه فرمایند.

با سپاس

حمیدرضا خدمتگزار

ساناز قربانلو

پیشگفتار پشتیبان کتاب

توسعه روزافزون به کارگیری فناوری اطلاعات در فرآیندهای کسب و کار موجب شده است که اطلاعات و دارایی های اطلاعاتی به یکی از منابع حیاتی سازمان ها تبدیل شود. استفاده مناسب از این اطلاعات و دارایی های اطلاعاتی به یکی از نیازهای اساسی برای دستیابی به اهداف سازمانی تبدیل شده است و حفظ محرمانگی، صحت و دسترس پذیری اطلاعات از مشخصه های مهم برای حفظ حیات و تداوم کسب و کار تلقی می شود.

پیشرفت سیستم های رایانه ای، رایانش ابری، خدمات شبکه های اجتماعی و وابستگی کسب و کارها به فناوری اطلاعات، آنها را در معرض خطرات زیادی از جمله سرقت، از بین رفتن و یا تخریب اطلاعات قرار داده است. از این منظر باید گفت تأمین امنیت اطلاعات مهمترین دغدغه و چالش این دوران است. از مهمترین موضوع ها در حوزه امنیت اطلاعات، شناسایی و مدیریت مخاطرات است که می توان آن را به عنوان سنگ بنای تصمیم های مدیران و متخصصان امنیتی دانست. مدیریت مخاطره یک فرآیند نظام مند است که به سازمان ها در درک اینکه مخاطره چیست، چه کسانی در معرض مخاطره قرار دارند و اینکه کنترل های فعلی برای این مخاطره ها و قضاوت های موجود در خصوص کفایت این کنترل ها مناسب هستند یا خیر، کمک می کند. در صورتی که این کنترل های موجود مناسب و کافی نباشند، برای ارتقای کنترل و مدیریت سطح مخاطره به یک سطح قابل قبول و معقول، بایستی اقدام هایی انجام شود. امروزه پیاده سازی یک سیستم مدیریت امنیت اطلاعات مبتنی بر مدیریت مخاطره مناسب در سازمان ها، به خصوص سازمان های بزرگ، بیش از هرگونه تعهد اخلاقی برای محافظت از کارکنان، به یک الزام قانونی تبدیل شده است که توصیه می شود قبل از هرگونه اقدامی از تجارب شرکت های دارای سابقه در این حوزه بهره جست.

تجربیات گسترده «شرکت فنی و مهندسی امن پردازان کویر» یا به اختصار (APK) در زمینه خدمات و محصولات مدیریت مخاطرات امنیت اطلاعات، طی سالیان متمادی، آن را به شرکتی قابل اعتماد و پیشرو تبدیل کرده که می تواند همراه مطمئنی برای سازمان ها در مسیر مشاوره، پیاده سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات باشد.

ما معتقدیم "ارزیابی مخاطره امنیت اطلاعات" و راهکارهای فنی مبتنی بر آن، باید همواره به عنوان سنگ بنای پیاده سازی استانداردهای "سیستم مدیریت امنیت اطلاعات" مورد توجه سازمان ها و کسب و کارها قرار گیرد؛ اگرچه، هم اکنون تنوع روش های ارزیابی و مدیریت مخاطره امنیت اطلاعات، همچنین عدم توافق در معیارهای مرجع مورد تأیید و نبود چارچوب مقایسه ای برای ارزیابی آنها، سازمان ها را در فرآیند انتخاب و بهره برداری از این روش ها با چالش هایی جدی مواجه کرده است.

در همین راستا امیدواریم این اثر برای مدیران اجرایی، ممیزان، مشاوران و سران تیم های امنیتی در استفاده بهینه از یک چارچوب ارزیابی مقایسه ای، با هدف به کارگیری مناسب روش های ارزیابی و مدیریت مخاطره امنیت اطلاعات مفید بوده و با کاهش چالش های سازمان ها در این حوزه، به ذینفعان این اطمینان خاطر را دهد که مخاطره ها به صورت بهینه مدیریت می شوند.

با سپاس

شرکت فنی و مهندسی

امن پردازان کویر

www.apk-group.net

فهرست نوشته‌ها

۱۳	۱. فصل نخست: مفاهیم پایه مدیریت مخاطره امنیت اطلاعات
۱۵	۱-۱. مقدمه
۱۵	۱-۲. نگاهی اجمالی به مفهوم امنیت
۱۷	۱-۳. امنیت اطلاعات و ارکان اصلی آن
۱۸	۱-۴. جایگاه امنیت اطلاعاتی سازمانی
۱۹	۱-۵. اهمیت و ضرورت توجه به امنیت اطلاعات
۱۹	۱-۵-۱. موج نخست: فنی
۱۹	۱-۵-۲. موج دوم: مدیریتی
۲۰	۱-۵-۳. موج سوم- نهادینه‌سازی
۲۲	۱-۵-۴. موج چهارم- حاکمیت امنیت اطلاعات
۲۳	۱-۶. روند شکل‌گیری و توسعه امنیت اطلاعات
۲۴	۱-۷. مدیریت امنیت اطلاعات
۲۵	۱-۸. مخاطره
۲۵	۱-۹. مدیریت مخاطره
۲۶	۱-۱۰. مدیریت مخاطره امنیت اطلاعات
۲۷	۱-۱۱. چالش‌های مطرح در فرایند مدیریت امنیت اطلاعات
۲۸	۱-۱۱-۱. چالش نخست: فهرست سیاهه دارایی و اقدامات متقابل
۲۹	۱-۱۱-۲. چالش دوم: تخصیص ارزش دارایی
۲۹	۱-۱۱-۳. چالش سوم: پیش‌بینی‌های شکست خورده از مخاطره
۳۰	۱-۱۱-۴. چالش چهارم: اثر اطمینان بیش از حد
۳۰	۱-۱۱-۵. چالش پنجم: اشتراک دانش
۳۰	۱-۱۱-۶. چالش ششم: مخاطره در مقابل هزینه‌های تجاری
۳۱	۱-۱۲. گزیده فصل
۳۳	۲. فصل دوم: روش‌های ارزیابی مخاطره
۳۵	۲-۱. مقدمه
۳۵	۲-۲. روش‌های ارزیابی مخاطره
۳۶	۲-۲-۱. روش ارزیابی مخاطره آنالوگ (ARA)
۳۷	۲-۲-۲. چارچوب اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط با آن (COBIT)
۳۹	۲-۲-۳. روش تجزیه و تحلیل درخت خطا (FTA)
۴۰	۲-۲-۴. چارچوب مدیریت مخاطره سازمانی کوزو (COSO ERM)
۴۲	۲-۲-۵. روش مطالعه مخاطرات و راهبری عملیات (Hazop)
۴۴	۲-۲-۶. روش ارزیابی امنیتی دلفی (Delphi)
۴۶	۲-۲-۷. روش تجزیه و تحلیل حالات و اثرات شکست (FMEA)
۴۹	۲-۲-۸. روش تجزیه و تحلیل بحرانی حالات و اثرات شکست (FMECA)

۵۰	۹-۲-۲. روش سنتی تحلیل مخاطره امنیت اطلاعات
۵۲	۳-۲. گزیده فصل
۵۵	۳. فصل سوم: روش‌های ارزیابی مخاطره امنیت اطلاعات
۵۷	۱-۳. مقدمه
۵۸	۲-۳. روش‌های ارزیابی مخاطره امنیت اطلاعات
۶۲	۱-۲-۳. استانداردهای ملی و بین‌المللی مدیریت و ارزیابی مخاطره امنیت اطلاعات
۶۳	۱-۱-۲-۳. استاندارد سری ISO 27000
۶۸	۲-۱-۲-۳. استاندارد سری ISO 31000
۷۲	۳-۱-۲-۳. استاندارد سری NIST 800
۷۹	۴-۱-۲-۳. استاندارد سری BSI
۸۳	۵-۱-۲-۳. استاندارد ETSI TVRA
۸۷	۲-۲-۳. چارچوب‌ها و راهنماهای عمومی مدیریت و ارزیابی مخاطره امنیت اطلاعات
۸۷	۱-۲-۲-۳. راهنمای Austrian IT Security Handbook
۹۰	۲-۲-۲-۳. راهنمای MAGERIT
۹۳	۳-۲-۲-۳. راهنمای Microsoft's Security Risk Management
۹۶	۴-۲-۲-۳. چارچوب‌های ISACA
۱۰۸	۳-۲-۳. روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات
۱۰۸	۱-۳-۲-۳. روش CORAS
۱۱۲	۲-۳-۲-۳. روش CRAMM
۱۱۵	۳-۳-۲-۳. روش EBIOS
۱۱۸	۴-۳-۲-۳. روش FAIR
۱۲۱	۵-۳-۲-۳. روش FRAAP
۱۲۳	۶-۳-۲-۳. روش MEHARI
۱۲۶	۷-۳-۲-۳. روش OCTAVE
۱۲۹	۸-۳-۲-۳. روش IRAM
۱۳۳	۳-۳. گزیده فصل
۱۳۵	۴. فصل چهارم: مقایسه روش‌های مدیریت و ارزیابی مخاطره امنیت اطلاعات
۱۳۷	۱-۴. مقدمه
۱۳۸	۲-۴. روش پژوهش
۱۴۱	۳-۴. مقایسه اسناد پایه مدیریت و ارزیابی مخاطره
۱۴۱	۱-۳-۴. نوع سند پایه ارزیابی مخاطره
۱۴۲	۲-۳-۴. ماهیت سند پایه ارزیابی مخاطره
۱۴۳	۳-۳-۴. سازمان ارائه‌دهنده سند پایه ارزیابی مخاطره
۱۴۴	۴-۳-۴. اندازه سازمان هدف سند پایه ارزیابی مخاطره
۱۴۵	۵-۳-۴. سطح کاربری سند پایه ارزیابی مخاطره
۱۴۶	۶-۳-۴. سطح تخصص/مهارت مورد نیاز سند پایه ارزیابی مخاطره
۱۴۷	۷-۳-۴. فرآیند تطبیق مراحل مدیریت و ارزیابی مخاطره امنیت اطلاعات بر اساس استاندارد ISO/IEC 27005

۱۴۸	۱-۷-۳-۴. پشتیبانی از مراحل مدیریت مخاطره.....
۱۵۰	۲-۷-۳-۴. پشتیبانی از مراحل ارزیابی مخاطره.....
۱۵۱	۸-۳-۴. رویکردهای تخمین مخاطره.....
۱۵۳	۹-۳-۴. شیوه ارزیابی مخاطره.....
۱۵۴	۱۰-۳-۴. پشتیبانی ابزارها.....
۱۵۵	۱۱-۳-۴. پشتیبانی از زبان‌های رایج.....
۱۵۶	۱۲-۳-۴. میزان سازگاری با استانداردها و مستندات پایه.....
۱۵۶	۱۳-۳-۴. پوشش تعاریف و اصطلاحات (واژه‌نامه).....
۱۵۷	۱۴-۳-۴. نوع دسترسی سند پایه ارزیابی مخاطره.....
۱۵۸	۱۵-۳-۴. کارایی سند پایه ارزیابی مخاطره.....
۱۵۹	۴-۴. مصورسازی روش‌های مدیریت و ارزیابی مخاطره.....
۱۵۹	۵-۴. گزیده فصل.....
۱۶۳	فهرست واژگان و علائم اختصاری انگلیسی به فارسی.....
۱۶۸	فهرست واژگان و علائم اختصاری فارسی به انگلیسی.....
۱۷۳	فهرست منابع.....